ISSN 1728-5445

SERIES

STUDIES AND PERSPECTIVES | 94

ECLAC SUBREGIONAL HEADQUARTERS FOR THE CARIBBEAN

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

Amelia Bleeker

UNITED NATIONS

ECLAC

Thank you for your interest in this ECLAC publication

Please register if you would like to receive information on our editorial products and activities. When you register, you may specify your particular areas of interest and you will gain access to our products in other formats.

Register

UNITED NATIONS

ECLAC

www.cepal.org/en/publications

facebook.com/publicacionesdelacepal

www.cepal.org/apps

SERIES

STUDIES AND PERSPECTIVES | 94

ECLAC SUBREGIONAL
HEADQUARTERS
FOR THE CARIBBEAN

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

Amelia Bleeker

UNITED NATIONS

ECLAC

This document was prepared by Amelia Bleeker, Associate Programme Management Officer of the Caribbean Knowledge Management Centre (CKMC) of the Economic Commission for Latin America and the Caribbean (ECLAC) subregional headquarters for the Caribbean.

United Nations publication
ISSN: 1728-5445 (electronic version)
ISSN: 1727-9917 (print version)
LC/TS.2020/126
LC/CAR/TS.2020/4
Distribution: L

Printed at United Nations, Santiago
S.20-00657

This publication should be cited as: 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 (LC/TS.2020/126-LC/CAR/TS.2020/4), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC),2020.

Contents

Tables

Boxes

Abstract

Technological developments, such data profiling and automated decision-making, have made it possible for governments to improve public services and governance outcomes by digitising the delivery of services. This phenomenon, known as digital government or e-government, presents untapped opportunities for Caribbean Small Island Developing States (SIDS), including improving access to government, saving individuals and government time and money, and reducing potential for government corruption. As digital government involves the collection, storage and use of massive amounts of data, including personal information, it must be supported by modern data protection and sharing frameworks in order to build public trust in online services and protect individuals' right to privacy.

Advances in information and communication technologies (ICTs) are also exposing privacy rights to new threats by reducing the amount of control that individuals have over their personal information and increasing the possible negative consequences resulting from access to it. Recent high-profile data breaches affecting millions of individuals worldwide, including in the Caribbean, have demonstrated the need for modern, robust data protection laws and resulted in privacy frameworks being overhauled to create enhanced protections for personal data and to strengthen individual rights. One of the latest innovations is the European Union's General Data Protection Regulation (GDPR), which is gaining recognition as international best practice in the area of data protection.

This study examines the data protection laws of six Caribbean countries with a view to identifying gaps and weaknesses and making targeted recommendations for revision of existing legislation or adoption of new legislation in order to bring it into compliance with regional and international standards, including the GDPR. Due to its extraterritorial scope and influence, the GDPR is prompting the harmonisation of data protection legislation around the world and a number of Caribbean countries and territories are following suit. The study concludes that implementing data protection legislation aligned with the GDPR across the subregion will not only guarantee individual privacy rights but also help to create an enabling environment for data sharing and e-governance and facilitate data and trade flows within and outside the Caribbean.

Introduction

Privacy is a fundamental human right and essential enabler of individuals' autonomy, dignity and freedom of expression enshrined in national constitutions as well as international and regional conventions and frameworks. Where the private information of individuals is subject to unwarranted intrusions from governments and private actors, individuals may censor their communications and feel unable to fully participate in society due to fear of possible consequences. The right to privacy is therefore linked to the exercise of other rights that depend on the ability to determine how one's personal information is used and shared, including press freedoms and freedom of speech.

Technological developments, including the creation of 'big data', data sharing, matching, profiling, and automated decision-making, have exposed the right to privacy to new threats by reducing the amount of control that individuals have over their personal information and increasing the range of possible negative consequences resulting from access to this information. Such developments have also ushered in the use of information and communication technologies (ICTs) to deliver public services, known as digital government or e-government.

Digital government presents untapped opportunities for improving public service delivery and governance outcomes in Caribbean Small Island Developing States (SIDS), including saving governments and individuals time and money and limiting potential for government corruption. The COVID-19 pandemic has demonstrated the urgent need to facilitate better access to e-government in the subregion and to digitize government transactions with the customer experience in mind. However, risks to the right to privacy and other human rights must be anticipated and managed to ensure that digitization does not result in breaches of individual rights.

After a series of high-profile global data breaches affecting millions of users in recent years, both the right to privacy and data protection frameworks are undergoing a revolution. These breaches have underscored the need to protect privacy as an essential condition for effective and transparent democratic governance. The mass accumulation of personal data renders democratic societies vulnerable to manipulation of electoral processes and creates the risk of discriminatory decision-making

using automated profiling.[1] Recent experience has demonstrated that countries with less developed data protection laws, including in the Caribbean, are particularly vulnerable to such discrimination and manipulation.

In response, governments around the world are creating enhanced frameworks for the protection of personal data, including laws, regulations and policies to protect individual privacy rights. These laws typically provide individuals with rights over their personal data, impose rules on the way in which the public and private sectors use data, and establish regulators to monitor and enforce the laws. Such laws can have their limitations as regulators always need to stay one step ahead of new data systems and technological innovations. However, modern legislative and regulatory frameworks provide a fundamental starting point for the protection of privacy and personal data.

One of the latest innovations in global data protection frameworks is the European Union's General Data Protection Regulation (GDPR), which is gaining recognition as global best practice in the area of data protection. The GDPR regulates the collection and use of personal data across the European Union (EU) but also applies to the processing of personal data of European individuals by organizations outside the EU. As a result, countries outside the EU need to comply with the requirements of the GDPR in order to protect cross-border trade and data flows with the EU and are moving to put similar frameworks in place. Several Caribbean countries have followed suit, with a wave of data protection laws being drafted and enacted in recent years. However, some countries in the subregion still have no data protection laws in place, and others have outdated laws that require revision for consistency with modern data protection and sharing principles.

This study analyses the data protection laws of six Caribbean countries with a view to identifying gaps and weaknesses and making targeted recommendations for revision of existing legislation or creation of new legislation in order to bring it into compliance with regional and international data protection and sharing standards, in particular the GDPR. Among other things, recommendations are also provided on facilitating cross-border transfers of data, incentivising public and private sector information sharing, balancing freedom of expression with privacy rights, ensuring independent oversight and safeguards for exemptions and exceptions to data protection standards, and enabling the effective enforcement of data protection laws through adequate resourcing of and cooperation between supervisory authorities.

[1] 'Profiling' is defined in the GDPR as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. (Article 4(4)).

I. Background

A. Data protection, sharing and the development of e-government in the Caribbean

E-government, or the government application of ICTs for delivering public services, presents opportunities for improving public service delivery and governance outcomes in Caribbean SIDS. It can minimize the impact of distance between islands and countries, save governments and individuals time and money, facilitate ease of doing business for citizens and external investors, limit potential for government corruption through the standardization of processes, and reduce the constraints of diseconomies of scale and limited human resources. The introduction of e-government also tends to go hand in hand with a more customer-centred approach.

Governments around the world have introduced e-government tools in the past two decades, such as e-payments, electronic signatures, biometric passports, online e-services, digital identity systems, electronic voting systems, online citizen participation tools and online access to parliamentary and governmental sessions and meetings. The urgent need for these tools has been highlighted during the COVID-19 pandemic. Most Caribbean countries included in the 2018 UN E-Government Survey had reached the 'high' or 'middle' level of the E-Government Development Index (EGDI). All Caribbean countries had improved their EGDI scores in the 2018 survey when compared with the 2016 results. The EGDI measures the readiness and capacity of national institutions to use ICTs to deliver public services and is a composite of telecommunications infrastructure, human capital and online services indexes. However, the EGDI may in fact overstate Caribbean performance in the deployment of e-government services as it gives substantial weight to metrics that are not directly related to the implementation of e-government.[2]

[2] ECLAC, 2016.

As a case in point, recent research of the Inter-American Development Bank (IDB) revealed that 90 per cent of Caribbean government-to-individual transactions are still carried out in person, often requiring the filling out of forms and three or more visits to a physical office, some of which are located on another island in the case of multi-island countries.[3] Furthermore, government transactions usually involve long waits, requiring on average more than four hours to complete.

There is therefore a need to facilitate better access to e-government in the subregion and to digitize government transactions with the customer experience in mind. With the impetus of the Caribbean Community's (CARICOM) Single ICT Space project, several Caribbean countries are working towards these aims, with digital transformation programmes underway in Trinidad and Tobago, the Bahamas, Barbados and Jamaica. The Jamaican government has recently committed to having 90 per cent of government services integrated and available, with every citizen having a national digital identity. However, of the 361 services currently offered by the government, only 38 per cent can be started and completed online.[4]

The COVID-19 pandemic has also increased the impetus to introduce e-government solutions and embrace digital technologies. Caribbean governments have shared health information on mobile apps, government websites and social media platforms throughout the crisis. New digital services have also been made available to respond to the needs of populations, including e-learning tools for students. However, many Caribbean governments have also lacked the policy, financial and technical capabilities to quickly and efficiently bring digital services online.[5] Where such obstacles can be surpassed, implementing digital technologies will support countries' economic recovery from the crisis and contribute to regional growth in the long-term.

The Single ICT Space project aims to create an ICT-enabled borderless space that fosters the economic, social and cultural integration for the betterment of Caribbean citizens. A key pillar of this project is supporting the digitization of government and the economy by promoting the free flow of data, the standardization of e-services and the development of digital skills. Launched by CARICOM Heads of Government in 2017, the project is conceptualized as the digital layer to the Caribbean Single Market Economy (CSME). Member States are encouraged to work towards regionally harmonized ICT policy, legal and regulatory regimes, robust national and regional broadband infrastructure, common frameworks for governments, ICT service providers and consumers, and effective, secure technology and management systems.[6]

In weaving together these various elements, the Single ICT Space recognises that a successful system of e-government relies on an enabling environment, including widely accessible and affordable internet access and ICT infrastructure and appropriate, modern legal and regulatory frameworks for both data protection and sharing. E-government functionality requires multiple dynamic pathways of data flow, but systems must be designed to protect personal data and ensure data subjects' rights. For example, data subjects have the right not to be subject to solely automated decision-making or profiling producing legal effects. However, public bodies are increasingly implementing e-government tools based on these processes. Furthermore, anonymisation and pseudonymisation tools can be integrated into e-government systems to prevent the identification of individuals, but pseudonymised data still allows individuals to be identified when various data sets are linked and therefore falls within the scope of modern data protection frameworks.[7]

---

3 Inter-American Development Bank (IDB) (2019), 'Wait No More: Citizens, Red Tape, and Digital Government'.
4 The Gleaner, 'Williams reports progress on Digital Jamaica Initiative', 24 January 2020.
5 See e.g. Cayman Compass, 'Technological and social challenges complicate remote learning', 11 June 2020.
6 CTU, 2017.
7 See, for example, Recital 26 of the GDPR for pseudonymization and anonymization requirements under EU law.

Data protection legislation is also a priority since an online service that is viewed as insecure and incapable of protecting personal information will not gain the trust and acceptance of individuals. To this end, the protection of privacy and sufficient means of guarding against abuse are necessary pre-conditions of successful e-government. Access to information and data sharing is another important issue for Caribbean governments seeking to implement interoperable e-government systems, as many countries report that data exists in siloes across government and some countries even have legislation in place that restricts sharing of information between government agencies.

Governments should have a legal basis for sharing information between public bodies and using common electronic databases and registers. This will allow public sector data to be used to improve government service delivery and contribute to evidence-based decision-making. In the absence of appropriate risk management strategies grounded in legal or regulatory frameworks, public sector agencies are currently hesitant to share citizens' data, or data is being shared without appropriate rules or safeguards as to use. However, the risks of data sharing can be mitigated by appropriate organisational and technical safeguards, which can include data sharing agreements, privacy impact assessments, codes of practice for public and private sector data sharing, and designation of 'focal points' to monitor the implementation of data sharing agreements.

Globally, only 107 countries, or 64 per cent, have data protection and privacy legislation in place.[8] Meanwhile, 8 per cent have produced draft legislation and 18 per cent have no legislation. Caribbean countries' data protection and sharing regimes are at varying stages of development, with a number of countries having no relevant laws in place. Many other countries in the subregion have outdated laws that require revision for consistency with modern data protection and sharing principles. Public bodies also lack regulations to clarify and explain what is in their laws and other guidance in the form of principles, codes of practice and technical standards.

While data protection and other e-government legislation and regulations should ideally precede the implementation of an e-government strategy, many Caribbean governments have developed their laws alongside their strategies or have plans to create their legislative foundations in the future. Moreover, some Caribbean countries have adopted a suite of new laws addressing e-government at one time, while other countries have made incremental changes to their laws as the need became apparent.

B. The right to privacy in the digital age

The right to privacy and the protection of personal data have taken on greater significance in the digital age with technological developments increasing government surveillance capabilities and allowing private organisations to conduct targeted advertising and profiling.

Recent data breaches involving the non-consensual harvesting of the personal data of millions of social media users and use of this data in political advertising to intentionally sway voters demonstrate the insidious ways personal data can now be collected and used and the resulting need for enhanced data protection frameworks at the domestic, regional and global levels. Data sharing from various sources and databases is also widespread amongst public and private sector organizations, with governments regularly sharing intelligence on individuals both internationally and domestically without legal protections or adequate oversight in place.[9]

---

[8] UNCTAD, 'Data protection and privacy legislation worldwide', https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

[9] Office of the High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age', 3 August 2018, A/HRC/39/29.

Box 1

Contact tracing apps in the context of COVID-19

An example of government surveillance in response to COVID-19 is mobile phone applications being used to trace human-to-human contact through interaction and proximity analysis. These apps have the potential to infringe privacy rights when unaccompanied by safeguards and limitations on the data collected and the length of storage. For example, an app being used in Guatemala for contact tracing, Alerta Guate, collects users' exact locations even when the app is closed. According to international NGO, Global Witness, the app's privacy policy allows data to be held for up to ten years, beyond the likely duration of the pandemic, and permits data to be used for advertising and shared with third parties when the developer reasonably believes it is necessary to protect the safety of the company, its users or others. Concerns have also been raised about potential misuse of data collected by the app for other forms of surveillance.

Source: Prepared by the author.

In 2013, Edward Snowden, a former employee of the United States' National Security Agency (NSA), publicly disclosed an estimated 1.7 million sensitive documents that revealed the agency's global mass surveillance programs and communication networks. The documents revealed that the NSA used covert mass surveillance technology to indiscriminately monitor the internet and phone activity of hundreds of millions of people across the world, with the close cooperation of its sister agencies in the United Kingdom, Canada, Australia and New Zealand. According to the disclosed documents, the NSA also used secret orders to require technology companies, including Facebook, Microsoft and Google, to share customers' data and to compel telecommunications providers to intercept private communications.

Snowden's revelations brought new focus to privacy issues around the globe and enabled privacy advocates to push for stronger protections in the EU's General Data Protection Regulation (GDPR).[10] Several national and regional courts have subsequently deemed the surveillance programs unlawful owing to the absence of meaningful oversight and legal safeguards. In *Big Brother Watch and Others v. the United Kingdom,* the European Court of Human Rights held that bulk data collection programmes between the United States and the United Kingdom violated Article 8 of the European Convention on Human Rights (ECHR) by failing to incorporate adequate privacy safeguards and oversight.[11]

Such activities might have seemed far removed from Caribbean shores until the exposé of the Cambridge Analytica scandal revealed illegal data and communication mining activities in Trinidad and Tobago in 2013. It is alleged that AIQ, an affiliate company of Cambridge Analytica, worked with the majority-Indian United National Congress party to defeat the incumbent People's National Movement, which is primarily supported by Afro-Trinbagonian voters, in the lead up to the 2013 local government elections. Specifically, the company used the practice of 'micro targeting' to create political messaging known as the 'Do So' campaign aimed at building apathy amongst Afro-Trinbagonian youth voters.[12] This targeted messaging relied on the collection of individuals' internet browsing data without their consent in order to profile their attributes.

---

[10] A. Rossi, 'How the Snowden Revelations Saved the EU General Data Protection Regulation', (2018) The International Spectator vol. 53(4), pp. 95-111.

[11] ECtHR, Case of Big Brother Watch and Others v. the United Kingdom (App. nos. 58170/13, 62322/14 and 24960/15) 13 September 2018 (Chamber judgment) – case referred to the Grand Chamber in February 2019.

[12] In the Honourable Attorney General Faris Al-Rawi's statement to the Parliament of Trinidad and Tobago on 28 March 2018, he refers to micro targeting as "the process of analyzing data and communications to predict the behaviour, interests, and opinions held by specific groups of people and then serving them the messages that they are most likely to respond to or to be influenced by, specifically in the context of election campaigning." See the Hansard transcript of parliamentary proceedings in the House of Representatives of Trinidad and Tobago for 28 March 2018: http://www.ttparliament.org/hansards/hh20180328.pdf.

In whistle-blower testimony from Cambridge Analytica's former Director of Research, Christopher Wylie, before the House of Commons of the United Kingdom's Parliament, he stated that the data acquisition in Trinidad and Tobago was illegal and that there was "total disregard for the law".[13] Commentators have noted that the absence of data protections in Trinidad and Tobago made it easier for Cambridge Analytica to harvest data and manipulate voter behavior in secret.[14] The Data Protection Act 2011 governs public and private bodies' use and handling of personal information, but the only operative parts of the Act are the general privacy principles and the sections establishing the Office of the Information Commissioner. The investigative powers of the Information Commissioner are not yet in force.

Social media companies, such as Twitter and Facebook, have also come under scrutiny in recent years for their use of targeted advertising and data profiling. These companies collect vast amounts of data about user behavior which is then bought and sold by advertisers to run highly targeted social advertising campaigns, in some cases without users' consent or knowledge. This practice, known as Real-Time Bidding (RTB), has attracted the attention of privacy regulators as it involves collecting highly sensitive personal data, including about race, sex life, health and political affiliation, and sharing it with third parties usually without an adequate assessment of security risks or the period of data retention.[15]

However, it is not only governments, data analytic, social media, and technology companies collecting and using personal data on a large scale. As data processing technologies become more sophisticated, consumer industries ranging from healthcare, transport, insurance, tourism to hospitality are adopting new ways to use personal data to predict spending habits, including in the Caribbean. These industries have also experienced massive security breaches as a result of inadequate security arrangements for protecting personal data. In an example impacting the Caribbean's tourism industry, the Marriott hotel chain suffered a data breach in 2018 revealing the names, addresses and passport numbers of as many as 500 million guests.[16]

C. International and regional instruments and frameworks protecting the right to privacy

Comprehensive, modern data protection and sharing laws are essential for protecting human rights, including the right to privacy but also related freedoms that rely on the ability to determine how and with whom personal information is shared. In 1890, the right to privacy was defined as 'the right to be let alone'.[17] Both international and regional human rights frameworks contain commitments to protect against abuses of the right to privacy and to promote respect for that right.

---

[13] Testimony of Christopher Wylie to the UK's Digital, Culture, Media and Sport Committee, p. 12: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/81022.pdf.

[14] Global Voices, 'Netflix's 'The Great Hack' highlights Cambridge Analytica's role in Trinidad & Tobago elections', 5 August 2019.

[15] Office of the Information Commissioner (UK), 'Update report into adtech and real time bidding', 20 June 2019.

[16] Office of the Information Commissioner (UK), 'Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach', 9 July 2019.

[17] S. W. Warren and L. Brandeis, "The Right to Privacy" 4 Harvard Law Review 193, 15 December 1890.

Box 2

What is the difference between information privacy and other forms of privacy?

No definition of privacy is universally accepted. However, a distinction is generally made between personal privacy and information privacy. Information privacy is concerned with individuals' ability to determine how their personal information is collected, stored and used, while personal and other forms of privacy can take the form of protecting bodily integrity and personal space from unwarranted intrusions and the ability to make personal decisions free from external influence. This study is concerned with the protection of information privacy through modern data protection legal and regulatory frameworks.

Source: Prepared by the author.

Adopted in 1948, the Universal Declaration of Human Rights declares in Article 12 that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." This principle has gained binding recognition in the International Covenant on Civil and Political Rights (ICCPR) for the 173 State Parties that ratified it, including 12 Caribbean countries.[18]

Similarly, Article 11 of the American Convention on Human Rights (ACHR), which entered into force in 1978 and is ratified by five Caribbean countries,[19] recognises that: "No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation." Furthermore, everyone has the right to the protection of the law against such interference or attacks. The Inter-American Court of Human Rights (IACHR) has confirmed that Article 11 is subject to the principles of legality, necessity and proportionality, among others. The principle of legality requires both public and private sector organisations to use personal information as authorised by law, and for legal protections to be made accessible to the public and regularly updated by means of a participatory legislative or regulatory process in order to keep pace with technological developments.[20]

European countries also have a proud tradition of protecting and upholding the right to respect for private and family life, with Article 7 of the European Union's Charter of Fundamental Rights and Article 8 of the Council of Europe's European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Both Conventions allow qualified interferences with the exercise of this right "as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".[21] The European Court of Human Rights (ECtHR) has held that use and retention of personal data requires clear, detailed rules governing the scope and application of such use, as well as minimum safeguards concerning duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data, and procedures for destruction, in order to provide sufficient safeguards against the risk of abuse and arbitrariness.[22]

---

[18] ICCPR, Article 17. The ICCPR entered into force on 23 March 1976. For the ICCPR's ratification status, see https://indicators.ohchr.org/.

[19] Barbados (1982), Dominica (1993), Grenada (1978), Haiti (1977), and Jamaica (1978). Trinidad and Tobago acceded to the Convention in 1991 but subsequently denounced it in 1998.

[20] Inter-American Court of Human Rights, Case of Escher v. Brazil (2009).

[21] Charter of Fundamental Rights of the European Union, article 7 (entered into force in 2000) and ECHR, article 8(2) (entered into force in 1953).

[22] ECtHR, Case of S and Marper v. The UK (App. Nos. 30562/04 and 30566/04), para. 99.

The right to privacy is also protected in non-binding international and regional instruments, including the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[23] Updated in 2013 with changes to the provisions on cross-border data transfers, the OECD Guidelines act as a framework for OECD Member States wishing to harmonise their data protection and privacy legislation on a voluntary basis and stress the need to ensure the free flow of data between Member States as a result of new technologies.

At the regional level, the Standards for Personal Data Protection for Ibero-American States, approved in 2016 by the Ibero-American Data Protection Network, are also a useful reference point.[24] The Network, whose membership is open to Spanish-speaking Caribbean countries, created the Standards in order to establish a set of common principles and rights for the protection of personal data in Ibero-American States and to facilitate the adoption of harmonised national legislation in the Latin American and Caribbean region. The Standards refer to the GDPR in the Preamble and share considerable common ground with the EU's framework.

D. Key features of and interplay between data protection, sharing and related laws

Data protection laws provide rules for the collection, storage, use and disclosure of personal information by public and private sector entities, while data sharing legislation enable such entities to share data with each other under the conditions of individual data sharing agreements or other frameworks. Data protection and sharing requirements can also be found in legislation or policy frameworks not specifically related to these subjects, including in laws and policies on interception of communications, freedom of information, cybercrimes, electronic transactions, telecommunications and intellectual property.

While freedom of information laws encourage public bodies to provide access to public information, they usually do not contain arrangements or criteria for sharing of personal data within and between public or private bodies. Another point to note is that freedom of information laws apply to requests for public information held by public bodies while requests for personal data about the person making the request are the domain of data protection laws.

As the following table shows, at least 13 Caribbean countries and territories have both data protection and freedom of information laws, while some further countries have either one or the other. 13 countries and territories in the subregion do not have data protection legislation. Furthermore, no countries have standalone legislation specifically dealing with data sharing.

Table 1
Data protection, sharing and related legislation of Caribbean countries and territories

Caribbean countries	Data protection legislation	Data sharing and related legislation
Antigua and Barbuda	Data Protection Act No. 10 of 2013	Freedom of Information Act 2004
The Bahamas	Data Protection (Privacy of Personal Information) Act 2003 Chapter 324A	Freedom of Information Act 2017
Barbados	Data Protection Act 2019 (Not in Force)	None
Belize	Data Protection Bill 2014	Freedom of Information Act 2000
Cuba	None	None
Dominica	None	None
Dominican Republic	Data Protection Law 172-13 (2013)	Law on Free Access to Public Information 200-04 (2004)

[23] Organisation for Economic Co-Operation and Development (OECD), Recommendation of the Council concerning Guidelines covering the Protection of Privacy and Transborder Flows of Personal Data, adopted 23 September 1980, C(80)58/Final.

[24] Ibero-American Data Protection Network, 'Standards for Personal Data Protection for Ibero-American States', November 2016.

Caribbean countries	Data protection legislation	Data sharing and related legislation
Grenada	None	None
Guyana	None	Access to Information Act, 2011 (Act No. 21 of 2011)
Haiti	None	None
Jamaica	Data Protection Act 2020	Access to Information Act (Act 21 of 2002)
Saint Kitts and Nevis	Data Protection Act 2018	Freedom of Information Act, 2018
Saint Lucia	Data Protection Act No. 11 of 2011 (Not in Force)	None
Saint Vincent and the Grenadines	None	Freedom of Information Act (Act 26 of 1999)
Suriname	Data Protection Bill 2018	None
Trinidad and Tobago	Data Protection Act 2011 No. 13 of 2011 (partially in force)	Freedom of Information Act (Act 26 of 1999)

Caribbean territories	Data protection legislation	Data sharing and related legislation
Anguilla	None	None
Aruba	National Ordinance on Personal Registration	National Ordinance on Access to Government (1999)
Bermuda	Personal Information Protection Act 2016 (PIPA)	Public Access to Information Act 2010
British Virgin Islands	Data Protection Bill 2019	None
Cayman Islands	Data Protection Law 2017 Data Protection Regulations 2018	Freedom of Information Law (2015 and 2020 Revisions)
Curaçao	National Ordinance for the Protection of Personal Data 2010	National Ordinance on Access to Government (1995)
Guadeloupe	GDPR as a result of being a French Overseas Territory	Decree No. 2005-1755 of 30 December 2005
Martinique	GDPR as a result of being a French Overseas Territory	None
Montserrat	None	Electronic Transactions Act 2009
Puerto Rico	None	Open Data Law 122 and Transparency Law 141
Sint Maarten	National Ordinance for the Protection of Personal Data 2010	National Ordinance on Access to Government (2010)
Turks and Caicos Islands	None	None
United States Virgin Islands	Several relevant federal laws, including US Privacy Act 1974 and Federal Trade Commission (FTC) Act 1914	Freedom of Information Act (US)

Source: Prepared by the author.

Outside the subregion, some countries take the approach of combining data protection and sharing frameworks in a single piece of legislation, while other countries have separate pieces of legislation dealing with each subject. It is also possible to have standalone data protection legislation for public and private sector organizations, as in the case of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) 2000 governing private sector activities and the Privacy Act 1985 applying to Canadian government agencies.[25]

The United Kingdom combined data sharing and protection provisions in a single law when it enacted the Data Protection Act 2018 in order to implement the EU's GDPR. Under section 121 of the Act, the Information Commissioner is mandated to prepare a code of practice containing practical guidance in relation to the sharing of personal data in accordance with the requirements of the legislation, and such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data. A public consultation was completed at the end of 2019 with a view to updating the country's current data sharing code of practice.[26]

[25] Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c 5 (Canada) and Privacy Act, R.S.C. 1985, c P-21 (Canada).

[26] The UK has a separate Freedom of Information Act 2000, which provides public access to information held by public authorities. It obliges public authorities to publish certain information about their activities; and members of the public are entitled to request information from public authorities.

New Zealand's Privacy Act 1993 also merges both data protection and sharing principles in the same piece of legislation. A bill to amend this Act to bring it into GDPR-compliance is currently before New Zealand's Parliament.[27] As it stands, the Act controls how public and private agencies collect, use, disclose, store and give access to personal information through the application of information privacy principles and codes of practice. It also contains two separate frameworks governing information sharing and information matching.[28] The information sharing framework provides for the authorization and oversight of Approved Information Sharing Agreements (AISAs), while the framework for information matching provides a detailed set of rules dealing with the supervision and operation of authorized information matching programmes. The proposed Amendment Bill maintains all three frameworks in the same Act, with Part 7 consolidating information sharing and matching under the heading 'sharing, accessing, and matching personal information'.

An example of separate data sharing legislation is South Australia's Public Sector (Data Sharing) Act 2016. This Act enables public sector agencies in this state to share data with each other and other trusted entities or non-government organizations under the conditions of individual data sharing agreements. The state government also has a privacy committee, which handles privacy complaints related to agencies' compliance with a set of Information Privacy Principles. At the federal level, the Australian government is proposing a new framework authorizing the release of public sector data when appropriate safeguards are in place pursuant to a Data Availability and Transparency Act (DATA). This legislation takes a principles-based approach to safeguarding the sharing of public sector data and provides 'data custodians' with an alternative authorization to share public sector data to accredited entities and trusted non-government entities.

Unlike other countries, the United States does not have a general data protection law regulating the public and private sectors' collection and use of personal data. Rather, privacy is regulated through a series of federal and state laws applying to different industries and types of data.[29] At the federal level, there is the US Privacy Act 1974, which creates rights and rules in relation to personal data held by government agencies; the Health Insurance Portability and Accountability Act (HIPAA) 1966 containing privacy rules for health information; the Children's Online Privacy Protection Act (COPPA) regulating personal data collected from minors; the Gramm-Leach-Bliley Act (GLBA) with rules for consumer financial and banking data; and the Federal Trade Commission (FTC) Act 1914, which prohibits companies from engaging in 'unfair or deceptive acts or practices'. The FTC Act has enabled the Commission to levy substantial fines against social media companies, including Facebook, for 'misleading' representations regarding its collection and use of personal data.

In the absence of a federal-level data protection law, a handful of states have enacted laws, including California, Nevada and Maine. The California Consumer Privacy Act (CCPA) 2018 only applies to Californian residents but other states are in the process of drafting similar privacy laws. Furthermore, the CCPA is de facto becoming the standard for companies conducting business in the US with, for example, Microsoft pledging to honour California's privacy rules throughout the country.[30] The CCPA shares many of the protections and the requirements of the GDPR, including rights to access and delete personal data and to opt out of data processing, and also requires companies to implement and maintain reasonable security procedures and notify consumers of data breaches. In response to the

---

[27] See the proposed bill here: https://www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/BILL_77618/privacy-bill.

[28] Authorised information matching is the comparison of personal information held by specified agencies with other specified agencies. A positive match occurs when two specified agencies matching personal information identify a person as appearing in both sets of data and the discrepancy sought by the match is found.

[29] See J Kosseff, Cybersecurity Law, John Wiley & Sons, Incorporated, 2017.

[30] Microsoft, 'Microsoft will honor California's new privacy rights throughout the United States', 11 November 2019. <https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights/>

passing of the CCPA, the FTC has noted the cumbersome patchwork of regulatory frameworks at the state level and argued that a comprehensive federal privacy law "could facilitate global interoperability, helping to bridge the differences between U.S. and foreign privacy regimes."[31]

In July 2020, the Court of Justice of the European Union (CJEU) struck down the EU-US Privacy Shield, an adequacy decision adopted in 2016 allowing cross-border transfers of data between the US and EU for commercial purposes.[32] The CJEU found that US 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. In particular, certain surveillance programmes of the US government result in limitations on the protection of personal data that do satisfy the requirements of the GDPR. Since data transfers based on the EU-US Privacy Shield are no longer lawful, European and US data controllers will need to put in place alternative mechanisms for exporting data to and from these locations, including standard contractual clauses and binding corporate rules.

Whether enacting separate or merged data protection and sharing laws at the national level, accompanying regulations, codes of practice and technical standards are often necessary to guide the practical application of the provisions. Some countries have adopted general codes of practices for data sharing in the public and/or private sector or more specific mandatory or voluntary guidance for specific industries, such as the health sector. For example, New Zealand's Health Information Privacy Code 1994 sets specific rules for the collection, use, storage and disclosure of health information held by agencies in the health sector.[33] Organizations must be aware of general legal obligations and codes of practice as well as industry specific guidance in carrying out their data processing activities.

E. The European Union's General Data Protection Regulation (GDPR)

The GDPR regulates the collection and use of personal data by both governments and the private sector across the European Union (EU) as well as non-EU entities offering goods and services to or monitoring the behaviour of persons in the EU.

Enacted in 2016, it went into effect on 25 May 2018 in the 28 Member States of the EU and builds on and replaces the 1995 Data Protection Directive (Directive 95/46/EC). Owing to its extraterritorial scope, the GDPR has been heralded as 'a chance to break down borders' and spur the internationalization of data protection law.[34]

1. Material and territorial scope

The GDPR applies to the 'controllers' and 'processors' of 'personal data'. A data controller is a 'natural or legal person, public authority, agency or other body which, alone or jointly with others, 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 under the GDPR to include 'any information relating to an identified or identifiable person' and includes online identifiers and location data.

---

31 C.S. Wilson, Commissioner of US Federal Trade Commission (FTC), 'A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation', Speech at Future of Privacy Forum, 6 February 2020.

32 CJEU, Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, EU:C:2020:559, 16 July 2020.

33 See the Code at this link: https://www.privacy.org.nz/assets/Files/Codes-of-Practice-materials/Consolidated-HIPC-current-as-of-28-Sept-17.pdf

34 C. Kuner, D. Jerker, B Svantesson, F.H. Cate, O. Lynskey, C. Millard, N. Ni Loideain, 'The GDPR as a chance to break down borders', International Data Privacy Law 7(4), November 2017, pp. 231–232.

The GDPR's territorial scope includes both processing of European personal data carried out in the context of the activities of organisations in the EU as well as by organisations not established in the EU where such organisations offers goods or services to people in the EU, or monitor the behaviour of anyone in the EU. As a result, all organizations engaging in trade with an EU entity need to be cognizant of and comply with the requirements of the GDPR. Given that Caribbean economies rely heavily on tourism, service offerings and external trade, including with EU entities, becoming GDPR compliant will be advantageous for both Caribbean public and private sector organizations.

Box 3
Common data flows in and out of the Caribbean

Global commerce relies on organisations' ability to transfer personal data across borders. According to the McKinsey Global Institute, cross-border data flows added an estimated USD$2.8 trillion to global GDP in 2014. A cross-border data flow takes place every time a person in the Caribbean uses a social media service or buys an online good or service from outside the subregion e.g. buying a book on eBay or watching TV shows on Netflix or when a person outside the Caribbean engages in digital trade with a Caribbean business e.g. a person in the UK books a tour online with a Caribbean-based tourism operator.

Global businesses, such as restaurant and hotel chains, airlines, manufacturers, and transportation and logistics companies, pool the personal data of customers from across their various centres, including those in the Caribbean, to improve business processes and efficiency. Caribbean-based financial service providers hold large amounts of data of citizens from other countries as do businesses in other industries, including telecommunications, healthcare and tourism.

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. Such data flows could be increased to improve public service delivery e.g. by using international telemedicine suppliers and software to improve healthcare. The sharing of health data across the globe and use of cross-border e-health services has been critical in the fight against the COVID-19 pandemic.

Source: Prepared by the author.

Implementing privacy frameworks modelled on the GDPR across the region can also create the conditions for e-government and data sharing between Caribbean countries, leading to regional economic growth and harmonized privacy protection for individuals. Effective systems of e-government require multiple dynamic pathways of data flow, including private to private, public to public, and private to public. While in many cases data flows are transfers of non-personal data or anonymised data, e-government functionality also relies on the ability to transfer personal data securely. For example, public bodies increasingly use automated systems to make operational decisions about the management and delivery of public services. Data protection principles must be integrated into these systems to ensure data subjects are not subject to solely automated decisions, which have a legal or similarly significant effect.

2. Key protections and features of the GDPR

The main features of the GDPR are outlined in the following table:

Table 2
Key features and protections in the General Data Protection Regulation (GDPR)

GDPR element and article(s)	Explanation
Broad definitions of 'personal data' and 'processing' (Article 4(1)-(2))	Personal data is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (emphasis added)

GDPR element and article(s)	Explanation
	Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Extraterritorial scope (Article 3)	The GDPR applies to the processing of personal data both: • carried out in the context of the activities of controllers and processors in the EU, regardless of whether the processing takes place in the EU or not, and • of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or (b) the monitoring of their behaviour as far as their behaviour takes place within the EU.
General data protection principles (Article 5)	The GDPR contains general principles to guide controllers' data use and collection, including: • Lawfulness, fairness and transparency: personal data must be processed lawfully, fairly and in a transparent manner • Purpose limitation: personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes • Data minimisation: personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed • Accuracy and updating: personal data must be accurate and, where necessary, kept up to date • Storage limitation: personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed • Integrity and confidentiality: personal data must be processed in a manner that ensures appropriate security of the personal data using appropriate technical or organisational measures • Accountability of data controllers: the controller shall be responsible for, and be able to demonstrate, compliance with the principles
Establishing the lawfulness of processing (Article 6)	A processing of personal data is only lawful if it meets one of the six conditions set out in Article 6. They are: • Where consent is given for one or more specific purposes • Where necessary for performance of a contract to which the data subject is a party • Where necessary for compliance with a legal obligation • Where necessary to protect vital interests of a natural person • Where necessary for the performance of a task carried out in the public interest • Where necessary for the legitimate interests of the controller or a third party (with exceptions)
Consent (Articles 4, 7 and 8)	Genuine and informed consent is one of the six bases on which data controllers can collect, use, and share a person's personal data. Consent is defined 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". The GDPR allows consent to be withdrawn at any time and requires the data subject to be informed of this right before giving consent. Furthermore, it must be as easy to withdraw as to give consent. There are special provisions for obtaining consent from children. Children have the same rights as adults over their personal data. However, only children aged 13 or over are able to provide their own consent and, for children under this age, the data controller needs to obtain consent from whoever holds parental responsibility for the child.
Special protections for 'sensitive data' (Article 9)	The GDPR contains specific and stricter requirements concerning the processing of special categories of data. In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9 e.g. to protect the vital interests of a data subject physically or legally incapable of giving consent. 'Sensitive data' includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Individual rights (Articles 12-23)	The GDPR contains a number of individual rights, including: • The right to be informed about the collection, sharing, storage and use of personal data • The right to access personal data • The right to have inaccurate or incomplete personal data rectified and to receive notification thereof • The right to have personal data erased and to receive notification thereof • The right to request restriction or suppression of their personal data e.g. the ability to store but not use personal data • The right to obtain and reuse personal data across different services in a structured, machine-readable and commonly used format (data portability)

GDPR element and article(s)	Explanation
	• The right to object to the processing of personal data in certain circumstances • Rights in relation to automated decision making and profiling, including the right not to be subject to solely automated decisions, including profiling, which have a legal or similarly significant effect Article 23 also allows member states to introduce restrictions on transparency obligations and individual rights where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: • national security; • defence; • public security; • the prevention, investigation, detection or prosecution of criminal offences; • other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security; • the protection of judicial independence and proceedings; • breaches of ethics in regulated professions; • monitoring, inspection or regulatory functions connected to the exercise of official authority regarding • security, defence, other important public interests or crime/ethics prevention; • the protection of the individual, or the rights and freedoms of others; or • the enforcement of civil law matters.
Obligations of data controllers (Articles 24, 25, 30 and 32)	Data controllers are required to adopt "appropriate technical and organizational measures" to protect the rights of data subjects and ensure personal data is only processed for specific purposes, known as privacy by design. Article 32(1) states: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" 'Data protection by design and by default' means integrating data protection into processing activities and business practices, from the design stage through the lifecycle.
Obligations of data processors (Articles 28, 30 and 32)	The GDPR also requires the data processors to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. Whenever a controller uses a processor to handle personal data on their behalf, the GDPR requires the controller to put in place a written contract that sets out each party's responsibilities and liabilities.
Data breach notifications (Articles 33 and 34)	The GDPR introduces a duty on both controllers and processors to report certain types of personal data breaches to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must be informed without undue delay. A record of any personal data breaches must also be kept, regardless of whether there is a requirement to notify.
Data protection impact assessments and prior consultation (Article 35-36)	A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise data protection risks of a project. A DPIA must be carried out: • when processing data with new technologies, • when there is likely to be a high risk to the rights and freedoms of natural persons, • when processing special categories of data on a large scale, including relating to criminal convictions and offences; and • when conducting systematic and extensive evaluations of personal aspects of natural persons based on automated processing and profiling producing legal effects. Where a DPIA indicates a high risk to personal data, the GDPR requires the data controller to undertake prior consultation with a supervisory authority and seek authorisation to commence processing activities.
Data protection officers (Articles 37-39)	The GDPR introduces a duty to appoint a data protection officer (DPO) for public authorities, processing operations requiring regular and systematic monitoring of data subjects on a large scale, and processing operations of special categories of data or data relating to criminal convictions and offences. The DPO must be involved in a timely manner in all issues relating to the protection of personal data and be given the required independence to perform his or her tasks in addition to authorisation to report to the highest level of management.
Codes of conduct and certification (Articles 40-43)	Use of approved codes of conduct is encouraged to help apply the GDPR effectively. Furthermore, the GDPR promotes certification schemes as a means of verifying and demonstrating compliance with its provisions.

GDPR element and article(s)	Explanation
International transfers (Articles 44-49)	The GDPR imposes restrictions on the transfer of personal data outside the EU, to third countries and to international organisations. It requires safeguards to be in place for transfers of personal data to a third country or international organisation. In particular, data controllers and processors must verify and demonstrate that the intended recipient of the data has adequate safeguards in place to ensure the same level of protection of individuals afforded by the GDPR.
Supervision (Articles 5-60, 69)	EU Member States are required to establish an independent data protection authority with a board responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU.
Cooperation and mutual assistance (Articles 50, 60-67)	Supervisory authorities are required to cooperate with other supervisory authorities and provide mutual assistance in cases of cross-border personal data transfers. Mutual assistance includes the provision of information and 'any other measures for effective cooperation'.
Remedies (Articles 77-84)	Individuals have the right to lodge complaints with a supervisory authority and the ability to enforce their rights through a judicial remedy. Any person who has suffered material or non-material damage as a result of a GDPR infringement has the right to receive compensation from the controller or processor for the damage suffered.
Provisions relating to specific processing situations (Articles 23, 85-91)	The GDPR contains special provisions for specific processing situations, including permitting derogations and exemptions to the GDPR for certain processing activities. These include processing that relates to: • freedom of expression and freedom of information, • public access to official documents, • national identification numbers, • processing of employee data, • processing for archiving purposes and for scientific or historical research and statistical purposes, • secrecy obligations, and • churches and religious associations.

Source: Prepared by the author.

3. Facilitating data flows and trade between EU and Caribbean countries

The GDPR permits cross-border data transfer outside the EU, or onward transfer from or to a party outside the EU without further authorisation from a national supervisory authority, where the European Commission has issued a decision that the third country or international organisation offers a level of data protection that is essentially equivalent to that within the EU, referred to as an 'adequacy decision'. To facilitate data flows and trade with EU entities, Caribbean countries would ideally seek an adequacy decision from the European Commission. This would provide clear authority for transfers of personal data from the EU to the country in question. However, the adoption of an adequacy decision is a lengthy process and the Commission has so far only issued such decisions for 13 countries and territories.[35]

Fortunately, data transfers outside the EU are also possible where a third country or international organisation has in place 'appropriate safeguards'. Under Article 46(2)-(3) of the GDPR, appropriate safeguards can include:

- A legally binding and enforceable instrument between public authorities providing appropriate safeguards for the rights of individuals,
- Binding corporate rules regarding the intra-organisational cross-border transfers of personal data in a multinational group of companies or international organisations,
- Standard contractual clauses adopted by the European commission,

[35] The countries and territories with adequacy decisions are: Andorra, Argentina, Canada (for commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay. In July 2020, the European Court of Justice struck down an adequacy decision for commercial purposes of the United States of America, referred to as the EU-US Privacy Shield. See CJEU, *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (Case C-311/18) EU:C:2020:559.

- Standard contractual clauses adopted by a supervisory authority and approved by the European Commission,
- An approved code of conduct together with binding and enforceable commitments of the data controller or processor in the third country to apply the appropriate safeguards provided for in the code,
- Certification under an approved certification mechanism together with binding and enforceable commitments of the data controller or processor in the third country to apply the appropriate safeguards provided for by the mechanism,
- Contractual clauses between data controllers and/or processors approved by a supervisory authority, or
- Administrative arrangements, such as a Memorandum of Understanding, between public authorities or bodies which include enforceable and effective rights for the individuals whose personal data is transferred, and which have been authorised by a supervisory authority.

If a transfer of personal data to or from the EU is not made subject to 'appropriate safeguards', it is possible that it will be covered by an exception in Article 49 of the GDPR. These include where a data subject has given explicit consent to the transfer, a transfer is necessary to perform a contract with a data subject, a transfer is necessary to perform a contract in the interest of a data subject, a transfer is for important reasons of public interest, a transfer is necessary in relation to a legal claim, a transfer is necessary to protect the vital interests of an individual incapable of giving consent, a restricted transfer is being made from a public register, or a one-off transfer is being made for compelling legitimate interests.

Following from this, Caribbean countries should aim to put in place national data protection laws that provide a level of protection for personal data which is comparable or 'essentially equivalent'[36] to that of EU law and could therefore facilitate transfers of personal data subject to an adequacy decision or 'appropriate safeguards'. In the absence of an adequacy decision, putting in place legislation that incorporates as many of the GDPR's 'appropriate safeguards' as possible will increase options for individuals and organisations in the Caribbean wishing to facilitate data flows with EU entities. As a corollary, it should be noted that some of the areas of non-alignment between the GDPR and national data protection laws highlighted in this study may be acceptable on the basis that they are not inconsistent with establishing 'appropriate safeguards' or supporting an adequacy decision. The objective is not to mirror the GDPR but to establish the core requirements of the regulation and the means for ensuring their effective application in order to guarantee individual privacy rights and the protection of personal data.[37]

Having a robust data protection framework in place will also facilitate cross-border data flows with non-EU countries, including the US and the UK following its departure from the EU, since the GDPR is broadly recognised as global best practice for data protection and many non-EU countries are seeking to align their data protection laws with the GDPR. The UK has already implemented the GDPR with the enactment of the Data Protection Act 2018. As noted above, ensuring a continuous flow of information to and from the Caribbean can also have significant economic value for countries in the subregion, as global e-commerce offers new opportunities for Caribbean businesses to operate in international markets and cross-border data flows now have a greater impact on GDP growth than the global goods trade.[38]

---

[36] CJEU, Case C 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015.

[37] Article 29 Working Party of EU Data Protection Authorities, 'Adequacy Referential' as last revised and adopted on 6 February 2018, WP 254 rev.01, (online) [date of reference: 20 July 2020] < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108>.

[38] McKinsey Global Institute, 'Digital Globalization: The New Era Of Global Flows', March 2016, (online) [date of reference: 28 June 2020] <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>.

This is an important consideration for Caribbean countries whose largest trading partners, the US and the EU, are situated outside the subregion.[39]

Since organisations processing the personal data of EU citizens outside the EU are also liable for fines under the GDPR (of up to €20 million or 4% of total worldwide annual turnover), aligning national regimes with the GDPR will also reduce the risk of financial penalties for Caribbean organisations who achieve compliance with them. EU countries have so far used their extraterritorial powers sparingly, with only a handful of cases involving companies outside the EU.[40] Although no Caribbean-based organizations have been subject to penal sanction or investigation to date, several multinational companies with Caribbean branches have been affected. Furthermore, as Caribbean countries enact GDPR-aligned data protection regimes, local supervisory authorities will begin to bring enforcement actions and levy fines. There will likely also be increased cooperation between European and local data protection authorities, with the prospect of more enforcement actions and fines using extraterritorial powers.

Aligning data protection frameworks with the GDPR also offers multiple benefits from the viewpoint of e-government functionality, as Caribbean governments are increasing implementing digital tools at the domestic and regional level. E-government systems rely on the fluid flow of data between public and private organisations as well as regional stakeholders but must incorporate appropriate technical and organisational measures in order to secure personal data and prevent the identification of individuals.

4. Last word on data protection?

Although the GDPR is broadly viewed as the 'gold standard' of data protection and a major step forward for global privacy regulation, future improvements may be needed as technological developments, judicial decisions, and implementation and enforcement challenges expose its limitations.

Human rights organisations have expressed concerns that many of the restrictions on processing of personal data in the GDPR are subject to overly broad exceptions for the activities of public bodies, including where there is a 'national security', 'defence', 'important public interest' or 'public security' justification.[41] Although the exceptions can only be exercised where individual's fundamental rights and freedoms are respected and it is a necessary and proportionate measure in a democratic society, the potential for overreach and abuse remains. The GDPR also permits private sector organizations to collect and process personal data without consent if the entity's 'legitimate interests' outweigh an individual's rights and freedoms. Since direct marketing is a possible legitimate interest, this could create a major loophole for data collectors depending on how courts interpret it.

Other commentators have highlighted that the centrality of consent in the GDPR has potential flaws.[42] Even where individuals are capable of giving free, specific and unambiguous consent to data processing, they will not necessarily be equipped with the necessary information and expertise to fully assess the privacy consequences of giving such consent. Technological developments, such as the sharing and matching of Big Data, make it difficult to assess how data may be aggregated and used in the future. The concept of informed consent can also lack meaning in the context of large online services

---

[39] See the European Commission's website for more on the EU/Caribbean trading partnership: https://ec.europa.eu/trade/policy/countries-and-regions/regions/caribbean/.

[40] Lexology, 'Better Compliance Through One Year of GDPR Enforcement', 26 July 2019 (online) [date of reference: 28 June 2020] <https://www.lexology.com/library/detail.aspx?g=7df2fcbd-cc6e-468b-bcfa-9119eaa9ad28>.

[41] See Human Rights Watch, 'The EU General Data Protection Regulation: Questions and Answers', 6 June 2018.

[42] See S. Davies, 'The Data Protection Regulation: A Triumph of Pragmatism over Principle?' (2016) European Data Protection Law Review 2(3), pp. 290-296 and J. Herle and J. Hirsch, 'The Peril and Potential of the GDPR' Centre for International Governance Innovation, 9 July 2019.

with few competitors, such as Facebook. In these scenarios, data subjects can either consent to the service's terms or choose to forego use of popular social or professional platforms.

While it is important to be cognisant of future improvements that may be necessary to the EU's framework, the GDPR remains a widely accepted standard and an important benchmark for Caribbean countries wishing to facilitate trade with EU countries and modernise their data protection and sharing frameworks.

F. Research methodology

The study involved a review of the data protection and related laws of a selection of the Member and Associate Member Countries of the Caribbean Development and Cooperation Committee (CDCC), namely Antigua and Barbuda, the Bahamas, Barbados, Belize, Cayman Islands and Jamaica. The review aimed to assess the extent to which these laws are aligned with the EU's General Data Protection Regulation (GDPR) as well as international and regional best practice in the area of data sharing. Countries were selected on the basis of their interest in the study and the existence of a legal framework for data protection in their country.

ECLAC assessed whether a country's law is fully aligned, substantially aligned, partially aligned or non-aligned with the GDPR and international best practice in the area of data sharing. To do this, a matrix was developed with a series of indicators for each area of the GDPR and data sharing best practice (**Annex A**). Based on the criteria developed using these indicators, a law was deemed to be:

- **Fully aligned** with the GDPR or data sharing best practice when a response indicating compliance could be given for all questions under consideration;
- **Substantially aligned** with the GDPR or data sharing best practice when a response indicating compliance could be given for all but one or two questions under consideration;
- **Partially aligned** with the GDPR or data sharing best practice when at least one response indicating compliance was possible for the questions under consideration; and
- **Not aligned** with the GDPR or data sharing best practice when a response indicating compliance could not be given for any of the questions under consideration.

As a general guide to the alignment ratings, substantial alignment with an element of the GDPR will in most cases be sufficient to achieve essential equivalency or a comparable level of protection to EU law. In some cases, partial alignment with the GDPR would also be sufficient to facilitate a comparable level of protection. It should be noted that areas of less than full alignment do not necessarily indicate shortcomings in national data protection laws but may point to areas of the GDPR that are not appropriate for a particular national context due to differing institutional or supervisory arrangements. Where relevant, the summary of findings discusses areas of partial or non-alignment that may still be consistent with the GDPR and in keeping with regional and international good practice.

Based on the results of the analysis, a summary of findings, recommendations and a table summarising the status of GDPR alignment for the law in question was produced for each country. In addition, general recommendations for continued adoption and strengthening of data protection and sharing laws in the subregion were provided.

II. Analysis of data protection legislation of select Caribbean countries

This section presents overall findings and country-specific findings for each of the six data protection laws under review for their alignment with the GDPR, namely the laws of Antigua and Barbuda, the Bahamas, Barbados, Belize, Cayman Islands and Jamaica. For each law, a summary of findings, targeted recommendations and a table setting out the alignment of each area of the law in question with the GDPR is provided. Where relevant, the summary of findings will discuss areas of non-alignment with the GDPR that may still provide a comparable level of protection to EU law.

The aim of the study's findings and recommendations is to guide Caribbean countries to put in place data protection laws that provide a level of protection for personal data which is comparable or 'essentially equivalent' to that contained in EU law. National data protection laws need not mirror each article of the GDPR but should establish the core requirements of the EU regulation as well as the means for ensuring their effective application in order to guarantee individual privacy rights. As a result, areas of non-alignment do not necessarily indicate shortcomings in national data protection laws but may point to areas of the GDPR that are not appropriate for a particular national context due to differing institutional or supervisory arrangements.

A. Overall findings

The following table presents a snapshot of the alignment ratings of the six laws under review with each element of the GDPR. As a general guide, substantial alignment with an element of the GDPR will in most cases achieve essential equivalency or a comparable level of protection to EU law. In some cases, partial alignment would also facilitate a comparable level of protection.[43]

[43] See Part I above for further discussion of essential equivalency and how countries can provide a comparable level of protection to the GDPR.

While none of the laws were fully aligned with all elements of the GDPR, each law had one or more areas of both substantial and partial alignment. Three of the newer laws had at least one area of full alignment and several areas of substantial alignment. All laws, except Jamaica's Data Protection Act 2020, had at least one area of non-alignment.

Table 3
Alignment of selected 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: prepared by the author.

B. Antigua and Barbuda

The Data Protection Act (DPA) No. 10 of 2013 aims to 'promote the protection of personal data processed by public and private bodies'. It applies to 'data users', 'data processors' and 'data subjects'; however, 'personal data' is defined narrowly to only apply to information in respect of commercial transactions. The Act extends certain powers, functions and duties of the Information Commissioner under the Freedom of Information (FOI) Act 2004 for the purposes of data protection.

1. Areas of non-alignment with the GDPR

As Table 4 shows, the DPA 2013, in combination with the FOI Act 2004 where relevant, is substantially aligned with two areas of the GDPR, partially aligned with nine and not aligned with the remaining seven.

Table 4
Alignment of Antigua and Barbuda's legislation with the GDPR

GDPR element and article(s)	Alignment rating	Areas in law not aligned with GDPR
Material scope and definitions (Article 2 and 4)	Partially aligned	• Narrow definition of 'personal data' only applying in respect of commercial transactions (s2) • Definition of 'sensitive personal data' does not capture racial or ethnic origin, trade union membership, genetics, biometrics or sex life. However, Minister can designate further categories by Order (s2).
Territorial scope (Article 3)	Not aligned	• Territorial scope not defined
Fundamental principles relating to processing (Article 5)	Substantially aligned	• The privacy and data protection principles mirror the GDPR's principles for the most part. However, some elements are missing, including accountability of data users and the concepts of fairness and transparency from the GDPR's lawfulness, fairness, and transparency principle (Part II)
Lawfulness of processing (Article 6)	Partially aligned	• A data user may process personal data 'if necessary' when showing one of the lawful grounds, rather than *to the extent* necessary (s5(2)) • Consent is a lawful ground for processing, but there is no requirement that it be given *for specific purposes* (s5(1)(a)) (except as it relates to disclosure: s7 and 17) • No safeguards for the lawful grounds to be overridden by the rights or interests of data subjects • Broad grounds for disclosure of personal data in s17 not subject to safeguards
Consent (Articles 4, 7 and 8)	Not aligned	• No definition of consent • Consent only required to be 'explicit' in relation to sensitive personal data (s18(1)(a)) • No requirement to allow withdrawal of consent • No provisions regarding obtaining consent from children
Special categories of personal data (Article 9 and 10)	Partially aligned	• Definition of 'sensitive personal data' does not capture racial or ethnic origin, trade union membership, genetics, biometrics or sex life (but the Minister can designate further categories (s2)) • Legal or official authority not required for the processing of data relating to criminal convictions and offences
Individual rights (Articles 12-23)	Partially aligned	• Some individual rights provided for in Part III on rights of data subjects, but the Act does not contain rights to erasure, to request restriction or suppression of personal data, to obtain and reuse personal data across different services (data portability), to object to processing in certain circumstances, or in relation to automated decision making and profiling • Broad exemptions to privacy and data protection principles in s19 not subject to limitations or safeguards • Data user not required to inform data subjects about their rights
Obligations on data controllers (Articles 24, 25, 30 and 32)	Partially aligned	• No requirement on data users to maintain a record of processing activities • No obligation on data users to review and update 'practical steps' taken under the security principle in s8 as necessary • Minister may make regulations prescribing codes of practice (s28), but no requirement that codes of practice or a certification mechanism are used to demonstrate compliance with the security principle
Obligations of data processors (Articles 28, 30 and 32)	Partially aligned	• No requirement that the data user and processor enter into a contract to govern processing of personal data • No direct enforceable obligations on data processors e.g. obligation is on the data user, not processor, to ensure that that the data processor 'provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and takes reasonable steps to ensure compliance with those measures' (s8(2)) • No requirement on data processors to maintain a record of processing activities

GDPR element and article(s)	Alignment rating	Areas in law not aligned with GDPR
		• No requirement on data processor to obtain the authorisation of the controller to engage another processor or only act on the instructions of the controller
Data breach notifications (Articles 33 and 34)	Not aligned	• No definition of or provisions relating to personal data breaches • No obligation on data users or processors to record or report personal data breaches to either the supervisory authority or data subjects
Data protection impact assessments and prior consultation (Articles 35-36)	Not aligned	• No requirement on data users to carry out data protection impact assessments in particular circumstances • No requirement on data users to consult with supervisory authority in processing situations indicating a high risk to personal data
Data protection officers (Articles 37-39)	Not aligned	• Public authorities are required to have an information officer under the FOI Act 2004, but the DPA 2013 does not extend this requirement in relation to data protection • No requirement on private sector organisations to have information officers
Codes of conduct and certification (Articles 40-43)	Partially aligned	• The Minister may make regulations prescribing codes of practices (s28(2)(c)), but this is not a requirement • No certification scheme for the Information Commissioner to monitor compliance with codes of practice
International transfers (Articles 44-49)	Not aligned	• International transfers not dealt with in the Act • No safeguards for transfers of personal data to other countries • No complaint or enforcement procedure for breaches of personal data by organisations in other countries or international organisations
Supervision (Articles 51-60, 69)	Partially aligned	• Powers, functions and duties of the Information Commissioner established under the FOI Act are extended for data protection under the DPA, but neither Act establishes the roles and responsibilities of the Office of the Information Commissioner (only those of the Commissioner: s37 FOI Act) • Investigative and corrective powers not as extensive as GDPR e.g. no ability to order ban on processing or suspension of data flows • Authorisation and advisory powers more limited than GDPR e.g. no prior consultation or certification function, no power to issue opinions, draft code of conducts, or give adequacy decisions • No provision to deal with serious staff misconduct • No board established for Office of the Information Commissioner
Cooperation and mutual assistance (Articles 50, 60-67)	Not aligned	• No requirement on supervisory authority to cooperate with supervisory authorities in other countries and to facilitate mutual assistance
Remedies (Articles 77-84)	Partially aligned	• Right of complaint only applies to certain rights e.g. when the data user refuses to give data access (s14) • No requirement on Information Commissioner to keep complainant informed of progress and outcome of complaint within a certain time period • No right for data subjects to be represented by a not-for-profit organisation • No right to receive compensation from data user and processor • No administrative fine for undertakings as a percentage of annual worldwide turnover • No guiding factors to be considered in imposing fines
Specific processing situations (Articles 23, 85-91)	Substantially aligned	• No special rules relating to processing of churches and religious associations

Source: Prepared by the author.

2. Main findings

Based on the areas of non-alignment between the DPA 2013 and GDPR identified above, this section sets out key areas for Antigua and Barbuda to consider if seeking to strengthen its legislation:

Definitions of 'personal data' and 'sensitive personal data'

A major difference between the DPA 2013 and the GDPR is that the DPA 2013 only safeguards personal data in respect of commercial transactions.[44] This means that individuals only gain the DPA's protection when their personal data is being processed by public and private bodies as part of a transaction of a commercial nature. By targeting transactions with commercial value, a wide variety of non-commercial activities, including for educational, recreational, household, employment, health, taxation, social security and welfare purposes, are excluded. The Act includes a definition for 'commercial transaction'; however, the term can still invite a number of interpretations, leading to uncertainties in its application. It is unclear, for example, whether data processing activities carried out by companies for administrative purposes would fall within the definition of 'commercial transaction' since there is no clear profit-making motivation.

The DPA's definition of 'sensitive personal data' does not capture personal data relating to racial or ethnic origin, trade union membership, genetics, biometrics or sex life. These categories of data are highly sensitive but excluded from the Act's more stringent conditions and safeguards for the processing of sensitive data, such as the requirement to obtain a data subject's explicit consent. Although the Minister may determine further categories of sensitive personal data by Order published in the Gazette, it appears that this has not taken place.

Territorial scope

While the DPA 2013 clearly applies to both public and private bodies, it does not clarify whether it applies to overseas bodies and individuals processing personal data in Antigua and Barbuda or parties operating outside the country processing the personal data of nationals of Antigua and Barbuda. The borderless nature of the internet and data processing technologies necessitates making the scope of data protection laws clear and often giving them more than a domestic territorial scope. For this reason, the GDPR applies beyond the EU to organisations outside the EU that offer goods or services to individuals in the EU.

In order to provide effective protection to citizens, Antigua and Barbuda may wish to consider giving its data protection law extraterritorial scope. Even if authorities are not capable of enforcing extraterritorial claims, giving the law this scope could stand as a deterrent for overseas parties who may engage in illegal processing. To mitigate the challenges of enforcing extraterritorial claims, the law could be given extraterritorial effect for a small subset of rules.[45] In any case, the territorial scope of the law should be clarified in order to provide certainty to data users and subjects.

Consent of data subjects

Under section 5, a data user may process personal data of a data subject if, among other conditions, the data subject has given consent to the processing. In the case of sensitive personal data, consent must be 'explicit'. The DPA's notion of consent falls short of best practice in a number of respects. The term is undefined, leaving it unclear whether consent needs to be freely given, specific and informed or an unambiguous indication of the data subject's wishes. While section 18 makes clear that consent must be explicit when processing sensitive data, it is unclear what lower threshold short of 'explicit' applies to non-sensitive personal data.

In other points of difference to the GDPR, the Act does not provide for the right to withdraw consent or require that consent be given for one or more specific purposes (although personal

[44] "Commercial transaction" means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance.

[45] D. Svantesson, 'A "layered approach" to the extraterritoriality of data privacy laws' (2013) International Data Privacy Law 3, pp. 278-286. See also B. Greze, 'The extra-territorial enforcement of the GDPR: A genuine issue and the quest for alternatives' International Data Privacy Law 9(2), May 2019, pp. 109–128.

data may only be processed for a lawful purpose directly related to an activity of the data user (s5(3)) and personal data can not be disclosed for any other purpose than that for which it was collected (s7)).

Rights of data subjects and the privacy and data protection principles

The rights of data subjects provided for in the DPA 2013 are more limited in scope than those contained in the GDPR. Specifically, the DPA does not contain explicit rights to erasure of personal data, to request restriction or suppression of personal data, to obtain and reuse personal data across different services (known as data portability in the GDPR), to object to processing in certain circumstances, or in relation to automated decision-making and profiling. Furthermore, while the DPA's privacy and data protection principles mirror the GDPR for the most part, the principle of the accountability of data users is missing, meaning that data users are not required to ensure and demonstrate their compliance with the principles.

Furthermore, section 19 of the DPA 2013 contains broad exemptions to the privacy and data protection principles without safeguards or limitations, such as a balancing act to guide their exercise. For example, personal data processed for the prevention or detection of crime or for the purposes of investigations is not subject to the general, notice and choice, disclosure, and access principles. This means that law enforcement bodies do not need to identify a lawful ground for processing personal data when investigating crimes, even where it involves a high risk to the rights and freedoms of data subjects. A more balanced approach would be to require data users to assess whether the legitimate interests of crime investigation should override the data subjects' interests, rights and freedoms in each instance of data processing and to require consultation with the Information Commissioner or judicial scrutiny before exercising the exemption.

Obligations of data users and processors

As far as the obligations of data users and processors are concerned, there are some important differences between the DPA and the GDPR. Data users are not required to maintain a record of processing activities, or to review and update the practical steps they are taking to protect personal data as necessary under the security principle in section 8.

The DPA does not impose direct enforceable obligations on data processors, rather placing the burden on data users to ensure that data processors 'provide sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and take reasonable steps to ensure compliance with those measures'.[46] Furthermore, there is no requirement that data users and processors enter into a contract to govern processing of personal data.

Personal data breaches

The DPA 2013 does not contain a requirement on data users or processors to record or report personal data breaches to either the Information Commissioner or data subjects or include accompanying penalties when they fail to do so. A reporting obligation gives data subjects the right to be informed when their privacy rights have been breached and enables them to take steps to protect themselves against the effects of the breach. Such an obligation is therefore an important accountability mechanism enabling data subjects to exercise legal remedies and mitigate any harm caused to them.

Mechanisms to ensure sufficient technical and organizational security measures

The GDPR provides data controllers with a number of tools to help ensure and demonstrate compliance with their obligations. These tools, including data protection impact assessments, data

[46] DPA 2013, section 8(2).

protection officers, codes of conduct, a certification mechanism, and a prior consultation procedure, are all missing from the DPA 2013.

There is no requirement on data users to carry out data protection impact assessments. Public authorities are required to have an information officer under the FOI Act 2004, but the DPA 2013 does not extend this requirement in relation to data protection. Furthermore, private sector organisations are not required to have information or data protection officers. While the Minister may make regulations prescribing codes of practices under section 28(2)®, this is not a requirement and there is no certification scheme for the Information Commissioner to monitor data users' compliance with codes of practice.

Remedies

Data users who fail to comply with the provisions of the DPA 2013 may be subject to fines or imprisonment or both. However, the Act does not allow a data subject to claim compensation for distress or damage caused by a data user's failure to comply with its obligations.

Furthermore, the DPA 2013 does not give data subjects a general right to complain to the Information Commissioner about any processing of personal data infringing the Act, but a more limited right of complaint in respect of certain rights, including the rights to access and to rectification.

Cooperation and safeguards for transfers of personal data to other countries

The DPA 2013 does not include safeguards for the transfer of personal data to other countries or international organisations, such as giving the Information Commissioner a power to make decisions on whether the receiving country provides an adequate level of protection to personal data. Under the GDPR, personal data may only be transferred outside the EU to countries that provide an adequate level of data protection, meaning a level of protection essentially equivalent to that afforded by the EU.

There is also no requirement in the DPA 2013 that the Information Commissioner facilitate international cooperation or mutual assistance with other supervisory authorities or international organisations. With transnational data flows becoming increasingly commonplace and essential to economies, there is a critical need for legal frameworks to respond by empowering governments to cooperate in the enforcement of data protection laws.

Data sharing

Data sharing falls within definition of 'processing' in the DPA 2013, which includes 'disclosure of personal data by transmission, transfer, dissemination or other making available'. However, the Act does not contain general provisions to facilitate public or private sector data sharing, such as providing for a data-sharing code or a system of authorization and oversight of information sharing agreements.

Section 17 offers justifications for disclosing personal data for purposes other than the purpose for which it was to be disclosed when collected, such as for law enforcement purposes, where the data user acts in the reasonable belief that he or she would have had the data subject's consent, where the data user acted in the reasonable belief that he had in law a right to disclose personal data, and where justified as being in the public interest by the Minister. The sharing of personal data in cases where a data user has a reasonable belief that they would have had the data subject's consent falls short of the reinforced consent provisions in the GDPR and creates the potential for data sharing on ambiguous grounds. To further alignment with the GDPR, a data user should be required to show that they have a lawful right to disclose data, not merely a reasonable belief in such. Furthermore, in order to safeguard against abuse, there should be independent oversight of categories of data deemed by the Minister as being in the public interest to disclose as well as public notification of instances of the exercise of the power. This could take the form of judicial or parliamentary scrutiny, an example of the latter being a ministerial order requiring affirmative parliamentary resolution.

Pursuant to section 28, which permits the Minister to prescribe codes of practice, consideration should be given to establishing a code of practice or guidelines for public and/or private sector data sharing. Although this exceeds the requirements of the GDPR, it would guide data controllers to share data lawfully and with confidence, so that individuals, government entities and the private sector can enjoy the benefits of data sharing.

3. Summary of recommendations

In addition to the more exhaustive areas for strengthening identified in Table 4 above, the following recommendations are highlighted for enhancing the protection of personal data pursuant to the DPA 2013:

- Amend the definition of personal data to apply to all data processing activities of public and private bodies, including both commercial and non-commercial transactions;
- Expand the definition of 'sensitive personal data' to include further categories of highly sensitive personal data, including racial and ethnic origin, trade union membership, genetics, biometrics and sex life;
- Clarify the territorial scope of the law;
- Define the term 'consent' and introduce provisions requiring it only be given for specific purposes and allowing it to be withdrawn;
- Introduce a principle of accountability of data users and expand the rights of data subjects to include rights to erasure, to request restriction or suppression of personal data, to data portability, to object to processing in certain circumstances, and in relation to automated decision-making and profiling;
- Introduce safeguards to the exercise of broad exemptions to the privacy and data protection principles;
- Introduce a general right of complaint to the Information Commissioner and a right to receive compensation from data users and processors for personal data breaches;
- Require data users and processors to maintain a record of processing activities and to record and report personal data breaches to the Information Commissioner and data subjects in certain circumstances;
- Impose a direct requirement on data processors to ensure appropriate technical and organizational security measures when processing personal data;
- Introduce mandatory and optional mechanisms for data users and processors to verify and demonstrate compliance with the Act, including data protection impact assessments, a prior consultation procedure, data protection officers, codes of practice, and a certification mechanism;
- Amend section 17 on the extent of disclosure of personal data to provide safeguards and limit the circumstances in which data users can disclose personal data outside the purposes for which it was collected; and
- Consider establishing a code of practice or guidelines for public and/or private sector data sharing under section 28 to facilitate lawful data sharing in accordance with the law and good practice.

C. The Bahamas

The Data Protection (Privacy of Personal Information) Act 2003 Chapter 324A was the Caribbean's first data protection law. A pioneering piece of legislation at the time of its enactment, the 2003 Act aims to protect the privacy of individuals in relation to personal data and to regulate the collection, processing, keeping, use and disclosure of certain information relating to individuals. The Office of the Data Protection Commissioner is responsible for overseeing the implementation and enforcement of the Act and has produced a Guide for Data Controllers available on its website.[47]

1. Areas of non-alignment with the GDPR

As Table 5 demonstrates, the 2003 Act is substantially aligned with two areas of the GDPR, partially aligned with eight and not aligned with the remaining eight.

Table 5
Alignment of the Bahamas' legislation with the GDPR

GDPR element and article(s)	Alignment rating	Areas not aligned in law
Material scope and definitions (Articles 2 and 4)	Substantially aligned	• Ethnic origin and sexual orientation excluded from definition of 'sensitive personal data' (s2) • Physical or mental health is included in 'sensitive personal data' (s2) but is said to exclude employees' health data kept in the ordinary course of personnel administration and not used or disclosed for any other purpose • Definition of disclosure excludes data processors (s2) and definition of processing excludes disclosure (s2)
Territorial scope (Article 3)	Partially aligned	• More limited territorial scope than the GDPR capturing data controllers not established in the Bahamas but using equipment in the Bahamas for processing (s4))
Fundamental principles relating to processing (Article 5)	Substantially aligned	• Back-up data need not be kept up to date or accurate (s6(1)(b)) • No principle of accountability of data controllers – controllers need not demonstrate compliance with the principles
Lawfulness of processing (Article 6)	Not aligned	• The Act does not set out conditions to be met for a processing of personal data to be lawful • Consent is not a legal ground for lawful processing • Data can be used for purposes not disclosed when it was obtained provided it is not used in such a way that damage or distress is, or is likely to be, caused to any data subject (s6(2))
Consent (Articles 4, 7 and 8)	Not aligned	• No definition or provisions regarding consent • No special provisions regarding obtaining consent from children
Special categories of personal data (Articles 9 and 10)	Partially aligned	• No legal or official authority required for the processing of data relating to criminal convictions and offences • Ethnic origin and sexual orientation and employees' health data excluded from definition of 'sensitive personal data' (s2)
Individual rights (Articles 12-23)	Partially aligned	• No right to restriction or suppression of personal data in certain circumstances, to data portability, to object to processing (not only in relation to direct marketing), and in relation to automated decision making and profiling • Broad exceptions to application of individual rights not subject to judicial oversight or other safeguards (ss 5, 7, 9 and 13)

[47] See the Bahamas' Guide for Data Controllers.

GDPR element and article(s)	Alignment rating	Areas not aligned in law
		• No duty on data controller to inform data subjects about their rights • Fee chargeable for data access requests (s8(3))
Obligations on data controllers (Articles 24, 25, 30 and 32)	Partially aligned	• No requirement for 'appropriate security measures' to be proportionate to the risk or to be reviewed and updated where necessary (s6(1)(d)) • No requirement for data controllers to maintain a record of processing activities • No certification mechanism for data controllers to demonstrate compliance with their obligations
Obligations of data processors (Articles 28, 30 and 32)	Partially aligned	• No requirement that data controllers only use data processors who provide sufficient guarantees to implement appropriate security measures • Disclosure of data by a data controller to a third party must be governed by 'a contract or other legal means' (s12(2)) but definition of disclosure excludes data processors and it is unclear what 'other legal means' includes or what a contract should contain • No requirement that data processors maintain a record of processing activities • No certification mechanism or code of practice for processors to demonstrate 'appropriate security measures'
Data breach notifications (Articles 33 and 34)	Not aligned	• No duty to report or record personal data breaches • No definition of personal data breach
Data protection impact assessments and prior consultation (Articles 35-36)	Not aligned	• No requirement that the data controller carry out data protection impact assessments in particular circumstances • No requirement that a data controller consult with the Commissioner prior to the commencement of processing indicating a high risk to personal data
Data protection officers (Articles 37-39)	Not aligned	• No requirement that either public authorities or private organisations appoint data protection officers in certain circumstances
Codes of conduct and certification (Articles 40-43)	Partially aligned	• No certification mechanism for the Commissioner to certify organisations as compliant with the Act
International transfers (Articles 44-49)	Partially aligned	• Not specified how persons transferring data outside the Bahamas can demonstrate that they 'provide protection by contract or otherwise equivalent to that provided under [the] Act' (s17(1)) • No institutional arrangements to facilitate Commissioner's supervision of international transfers • International transfers can be made with the *implied* consent of data subjects (s17(8))
Supervision (Articles 51-60, 69)	Partially aligned	• No provision setting out the roles and responsibilities of the Commissioner or the Office as a whole • Authorisation and advisory powers of the Commissioner not set out • No board for the Office of the Data Protection Commissioner
Cooperation and mutual assistance (Articles 50, 60-67)	Not aligned	• No requirement that the Office of the Data Protection Commissioner cooperate with supervisory authorities in other countries and facilitate mutual assistance • No provisions on mutual assistance
Remedies (Articles 77-84)	Not aligned	• No time period set out within which Commissioner must inform complainant of the outcome of a complaint (only 'as soon as may be' – s15(2)(b)) • No right to an effective judicial remedy or to compensation for data subjects who have suffered material or non-material damage • No right for data subjects to be represented by a not-for-profit organisation • No requirement that administrative fines be effective, proportionate and dissuasive or guidance on factors to be taken into account to guide the imposition of fines
Specific processing situations (Articles 23, 85-91)	Not aligned	• No safeguards to protect journalistic activities and freedom of expression, such as an exemption for journalistic, literary and artistic material or a

GDPR element and article(s)	Alignment rating	Areas not aligned in law
		requirement to reconcile freedom of expression with data protection rights • Broad carve-outs from the Act's protections, including for national security (s5) • Further broad exemptions and derogations permitted by the Act without judicial oversight or other safeguards e.g. access rights where criminal investigation is concerned (s9) and disclosure rules where in Minister's opinion it is necessary to protect national security (s13)

Source: Prepared by the author.

2. Main findings

Based on the areas of non-alignment between the 2003 Act and GDPR identified above, this section sets out key areas for the Bahamas to consider if seeking to adopt new data protection legislation or strengthen its existing legislation:

Definitions of 'sensitive personal data', 'disclosure' and 'processing'

The 2003 Act's definition of 'sensitive personal data' does not capture personal data relating to ethnic origin or sexual orientation. These categories of data are highly sensitive but excluded from the more stringent conditions and safeguards typically applied to the processing of sensitive data. Furthermore, the Act does not set out additional safeguards in relation to sensitive personal data, rather the Guide for Data Controllers includes additional special conditions, such as a requirement to obtain a data subject's explicit consent to processing.

Physical or mental health is included as a category of sensitive personal data but is said to exclude employees' health data kept in the ordinary course of personnel administration and not used or disclosed for any other purpose. Given the sensitivity of health data and that individuals should also have data rights and security in the employment context, this carve-out should be reconsidered.

Furthermore, the Act's definition of disclosure excludes data processors (section 2). As discussed further below in relation to data sharing, this means that a data controller is not required to 'use contractual or other legal means to provide a comparable level of protection to data subjects' when disclosing information to a data processor for the purpose of data processing (s12(2)).

Grounds for lawful processing

A cornerstone of the GDPR is that data controllers must be able to show that data processing is undertaken in compliance with specific lawful grounds, the prime one being where consent is given for one or more specific purposes. Other lawful grounds include where processing is necessary for the performance of a contract to which the data subject is a party and where necessary for the legitimate interests of a controller or a third party.

The 2003 Act requires data collection to be lawful and fair in the circumstances of the case but does not require the data subject's consent for processing or set out other conditions to be met for a processing of personal data to be lawful. By requiring data collection to be lawful but not setting out lawful bases for processing, the 2003 Act lacks legal certainty and creates the possibility of data controllers relying on vague grounds to justify processing.

Furthermore, section 6(2) of the 2003 Act allows personal data to be used for purposes not disclosed when it was obtained provided it is not used in such a way that damage or distress is, or is likely to be, caused to any data subject. This means, for example, that data controllers can use data subjects' personal data for direct marketing without their consent or informing them it would be used for this purpose at the time of data collection, provided such use is not likely to cause damage or distress. This

provision falls short of the GDPR's reinforced consent requirements and is at odds with the requirements in section 6(1)® that data should only be kept for one or more specified and lawful purpose and should not be used or disclosed in any manner incompatible with that purpose or those purposes.

Consent of data subjects

The unambiguous, informed consent of the data subject is a key ground for data processing under the GDPR, premised on individual autonomy and freedom of choice. The EU regulation dedicates several articles to clarifying the notion of consent, including the ability to withdraw consent, requiring it to be given for specific purposes and special provisions on obtaining consent from children. Consent is defined 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".[48]

Under the 2003 Act, consent is a ground for disclosure of personal data (s13(h)) and for the transfer of personal data outside the Bahamas (s17(8)). However, it is not defined or expressed to be a condition for the lawful processing of personal data. While some commentators have noted the impracticalities of informed consent in the age of Big Data,[49] it is nonetheless an important mechanism in the GDPR's toolkit for guaranteeing individual's freedom of choice and holding data controllers accountable for their collection and use of personal data.

Individual rights

Individuals enjoy some important individual rights under the 2003 Act, including a right of access, to rectification or erasure, and to prohibit processing for purposes of direct marketing. Absent, however, are rights to restriction or suppression of personal data in certain circumstances, to data portability, to object to processing in circumstances beyond direct marketing, and in relation to automated decision making and profiling.

Several features of the 2003 Act also have the potential to undermine the individual rights it contains. For example, there is no duty of data controllers to inform individuals about their rights, which places the burden on individuals to be aware of their existence. Data controllers are also permitted to charge a fee for data access requests (s8(3)). Given that an individual's right of access to their own personal data is an individual right, it is arguable that it should be exercisable free of charge. In any case, the Minister should make regulations under section 8 to ensure the fee payable is proportionate and that data controllers are not obliged to charge it.

Broad exemptions not subject to safeguards

The Act also contains broad exceptions to the application of individual rights and other protections without independent oversight or other safeguards. Under section 5, there are broad exclusions to the Act for personal data 'that in the opinion of the Minister or the Minister for National Security are, or at any time were, kept for the purpose of safeguarding the security of The Bahamas' and 'pending civil, criminal or international legal assistance procedures'. While exceptions to the application of data protection principles for national security and criminal investigation and enforcement are common, it is unusual for such exceptions to be solely a matter of ministerial discretion or immune from challenge by directly affected data subjects. Furthermore, in many cases, data protection legislation now requires such exclusions to be exercised on a task-related rather than blanket basis with oversight by an independent court or tribunal.

---

[48] GDPR, Article 4(11).

[49] See, for example, F.H. Cate and V. Mayer-Schönberger, 'Notice and consent in a world of Big Data', International Data Privacy Law, Volume 3, Issue 2, May 2013, pp 67–73.

Sections 7, 9 and 13 also contain broad carve-outs to the exercise of individual rights. Under section 7, data need not be collected lawfully or fairly if it would prejudice criminal investigation and detection or tax collection. Section 9 contains several exceptions to the right of access, such as for discharging functions under any enactment, for protecting the international relations of the Bahamas, and for back-up data, among others. Under the GDPR, individual rights apply equally to back-up data and therefore an individual can request access and to be informed of back-up data held by a data controller.

Furthermore, the 2003 Act's restrictions on disclosure of personal data do not apply to a variety of categories of personal data under section 13, including where disclosure is in the Minister's opinion necessary for national security purposes, where required for criminal investigation and detection or tax collection, and where required for protecting the international relations of the Bahamas. In the latter case, this means personal data can be disclosed where a data controller deems it to be necessary to protect the Bahamas' international relations without any checks and balances, such as judicial oversight. The vagueness of the term 'international relations' creates the risk that public authorities could rely on it to share large amounts of personal data with foreign governments, without applying rules for international transfers in section 17.

Obligations of data processors and controllers

The 2003 Act contains several differences with the GDPR in the area of the obligations of data controllers and processors. Pursuant to sections 6(1)(d) and 6(3), both data controllers and processors are required to take 'appropriate security measures...against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.' However, there is no requirement that those measures ensure a level of security appropriate to the risk or that they be reviewed and updated where necessary. Neither controllers nor processors are required to maintain a record of processing activities. Furthermore, the 2003 Act does not contain a certification mechanism by which data controllers and processors can verify and demonstrate compliance with their obligations.

The GDPR requires processing of personal data to be governed by a contract between the data controller and processor and stipulates what such a contract should contain. By comparison, the 2003 Act only requires disclosure of data by a data controller to a third party to be governed by 'a contract or other legal means' (s12(2)). The definition of 'disclosure' excludes data processors, employees and agents of the controller. Furthermore, the requirement does not apply to all forms of processing (only 'disclosure' which is excluded from the definition of processing) and it is unclear what 'other legal means' includes or what a contract with a third party should contain.

Mechanisms to ensure sufficient technical and organizational security measures

The principle of accountability under the GDPR requires data controllers and processors to 'implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation'.[50] The Regulation offers a variety of measures and mechanisms by which controllers can demonstrate accountability and implement the data protection principles, including an obligation to perform data protection impact assessments in cases where processing operations present a high risk to the rights and freedoms of natural persons and an obligation to appoint a data protection officer in certain circumstances.

These mechanisms by which controllers and processors can proactively identify, assess and mitigate risks to personal data are excluded from the 2003 Act. It requires data controllers to take 'appropriate security measures' to protect personal data and the Commissioner may encourage trade

[50] GDPR, Article 24(1).

associations and 'bodies representing categories of data controllers to prepare codes of practice to be complied with by those categories in dealing with personal data' (s20). A Code of Practice has been produced by the Commissioner's Office; however, under the Act, codes of practice are not linked to any certification mechanism by which the Commissioner can verify organisations as compliant with the Act's obligations.

Furthermore, data controllers are not obliged to carry out data protection impact assessments in particular circumstances or consult with the Data Protection Commissioner prior to undertaking 'high risk' processing. Neither public authorities nor private organisations are required to appoint data protection officers in any circumstances.

Reporting personal data breaches

A requirement to notify personal data breaches serves a number of important functions, including enabling data subjects to mitigate harm caused by serious breaches, incentivising data controllers to be proactive in preventing breaches by investing in appropriate security measures, bringing awareness to the frequency and extent of personal data breaches, and making individual rights in data protection laws effective by enabling individuals to exercise legal remedies.

There is no duty in the 2003 Act to report or record personal data breaches to the Commissioner or affected data subjects. As a result, data subjects in the Bahamas are not notified of breaches of their personal data even where the breach is likely to result in a high risk to their rights and freedoms.

Safeguards for transfers of personal data to other countries

The 2003 Act requires persons transferring data outside the Bahamas to 'provide protection either by contract or otherwise equivalent to that provided under this Act' (s17(1)). The Commissioner may prohibit international transfers where the transfer would likely cause damage or distress to any person and after having regard to the 'desirability of facilitating international transfers of data'.

Notably, the requirement to demonstrate equivalent protection does not apply to international transfers where they are made pursuant to the express or implied consent of data subjects (s17(8)). While this is a reasonable exception where a data subject gives express consent, relying on implied consent to transfer data is no longer possible under the GDPR. The EU regulation requires a clear affirmative action or statement from the data subject to establish consent.

The 2003 Act also does not contain institutional arrangements to facilitate the Commissioner's supervision of international transfers and does not specify how persons transferring data outside the Bahamas can demonstrate that they provide equivalent protection to the Act. For example, the GDPR requires safeguards to be in place for transfers of personal data to a third country or international organisation, such as binding corporate rules, a certificate of compliance from the receiving country's supervisory authority or a legally binding data protection agreement approved by the country's supervisory authority.

Cooperation and mutual assistance

The 2003 Act is silent on whether the Data Protection Commissioner should cooperate with supervisory authorities in other countries and facilitate mutual assistance in order to contribute to the effective global enforcement of data protection legislation. Therefore, the Commissioner does not have express authority to cooperate or provide mutual assistance in cases of cross-border personal data transfers.

This is an important feature of modern data protection legislation, given the global nature of data processing and the GDPR's requirement for EU supervisory authorities to develop international cooperation and mutual assistance mechanisms with third countries and international organisations.

While these mechanisms are yet to be developed, including cooperation and mutual assistance in Caribbean data protection laws will facilitate eventual participation in them.

Remedies

Under the GDPR, individuals have the right to lodge complaints with a supervisory authority and the ability to enforce their rights through a judicial remedy. This is accompanied by an individual right to receive compensation for any material or non-material damage suffered.

The 2003 Act allows individuals to make complaints to the Commissioner and includes a right of appeal to the Supreme Court. However, remedies available under the Act could be enhanced to further alignment with the GDPR and empower individuals to exercise their rights. The Commissioner must inform a complainant of the outcome of a complaint 'as soon as may be' (s15(2)(b)) but ideally this should take place within a specified time period. Individuals should have a right to an effective judicial remedy as well as a right to compensation where they have suffered material or non-material damage as a result of data processing. Furthermore, administrative fines should be effective, proportionate and dissuasive, with factors set out to guide the Commissioner or the Court in deciding whether to impose fines and at what amount.

Lack of protection for journalistic activities and freedom of expression

The 2003 Act is silent on freedom of expression and journalistic activities, leaving open the possibility that individuals could attempt to bring data protection claims in order to stifle or prevent critical reporting.[51] The Commissioner's powers in relation to journalistic activities and freedom of expression are also not limited by safeguards. Given the special role of the press in enabling the functioning of democratic societies, it is important that data protection laws contain strong protections for freedom of expression and preventing vexatious data protection claims against the media. A common method of guaranteeing this is through an exemption for journalism, literary and artistic purposes.

Data sharing

The 2003 Act contains separate definitions of 'disclosure' and 'processing'. The former definition refers to the disclosure of information extracted from personal data and excludes data processors, employees and agents of the controller. The definition of processing includes transmission, dissemination or otherwise making available information or data, thereby capturing data sharing. When disclosing information to a third party for the purpose of data processing, a data controller is required to use contractual or other legal means to provide a comparable level of protection to data subjects (s12(2)). This protection does not apply to disclosures from a data controller to a data processor, given the Act's definition of disclosure excludes data processors. It is also not specified what a contract should stipulate or what qualifies as 'other legal means'.

While the Commissioner may encourage trade associations and other bodies representing categories of data controllers to prepare codes of practice (s20), there is no requirement to establish a code of practice or guidelines for public sector data sharing. The Act could set out conditions for data sharing agreements or require the Commissioner to provide separate guidance on the topic in the form of a code of practice or regulations.

Furthermore, the Act also includes some broad exceptions to the application of rules relating to data disclosure, including for the purposes of criminal investigation, when in the opinion of the Minister or the Minister of National Security disclosure is required for the purpose of safeguarding the security

[51] N.J. Reventlow, 'Can the GDPR and Freedom of Expression coexist?' (2020) American Journal of International Law 114, pp. 31-34.

of the Bahamas, and when required in the interests of protecting the international relations of the Bahamas. These exceptions are not subject to judicial or parliamentary oversight or any other safeguards, such as a requirement that data controllers undertake privacy impact assessments before sharing data in situations where there is a high risk to the rights and freedoms of data subjects and consult with the Commissioner where an assessment indicates a high risk.

3. Summary of recommendations

In addition to the more exhaustive areas for strengthening identified in Table 5 above, the following recommendations are highlighted for enhancing the protection of personal data pursuant to the 2003 Act:

- Amend definitions of 'sensitive personal data', 'disclosure' and 'processing' and introduce a definition of 'consent' as outlined above to further alignment with the GDPR;
- Strengthen the Act's data protection principles by including back-up data in the obligation to keep data up-to-date and accurate and introducing a principle of accountability on data controllers;
- Introduce conditions to be met for a processing of personal data to be lawful, including the informed consent of the data subject given for specific purposes;
- Establish a duty on data controllers to inform data subjects of their individual rights as well as a more expansive set of rights, in particular to restriction or suppression of personal data in certain circumstances, to object to processing (not only in relation to direct marketing), and in relation to automated decision making and profiling;
- Introduce safeguards, including parliamentary and judicial oversight where appropriate, to broad exceptions to individual rights in sections 5, 7, 9 and 13;
- Introduce safeguards to protect journalistic activities and freedom of expression, such as an exemption for journalistic, literary and artistic material or a requirement to reconcile freedom of expression with data protection rights;
- Require 'appropriate security measures' in section 6(1)(d) to be proportionate to the risk and to be reviewed and updated where necessary;
- Require both data controllers and processors to maintain a record of processing activities and to record and report personal data breaches;
- Require processing of personal data between a data controller and processor to be governed by a contract (not only disclosure to a third party as in section 12(2));
- Introduce mechanisms by which data controllers and processors can proactively identify, assess and mitigate risks to personal data, including data protection officers, data protection impact assessments and a prior consultation procedure;
- Establish a certification mechanism for data controllers and processors to verify and demonstrate compliance with their obligations;
- Specify how persons transferring data outside the Bahamas under section 17 can demonstrate that they 'provide protection by contract or otherwise equivalent to that provided under this Act';
- Set out the roles, duties and responsibilities of the Data Protection Commissioner and Office as a whole, including authorisation and advisory powers and a duty to facilitate international cooperation and mutual assistance; and

- Enhance the remedies provided for in the Act by introducing a time period within which the Commissioner must notify decisions to complainants, a right to an effective judicial remedy and to compensation for data subjects who have suffered material or non-material damage, and factors to be taken into account when imposing fines.

D. Barbados

Modelled closely on the GDPR, the Data Protection Act (DPA) 2019 is a modern piece of legislation aimed at regulating the collection, keeping, processing, use and dissemination of personal data and protecting the privacy of individuals in relation to their personal data. Given the close alignment of the DPA 2019 and EU law, an organization's compliance with the former would in many cases satisfy the requirements of the latter.

The Ministry of Innovation, Science and Smart Technology is currently tasked with implementing the Act and establishing the Office of the Data Protection Commissioner.

1. Areas of non-alignment with the GDPR

As Table 6 demonstrates, the DPA 2019 is fully aligned with seven areas of the GDPR, substantially aligned with eight, partially aligned with two and not aligned with the remaining one.

Table 6
Alignment of Barbados' legislation with the GDPR

GDPR element and article(s)	Alignment rating	Areas not aligned in law
Material scope and definitions (Articles 2 and 4)	Fully aligned	
Territorial scope (Article 3)	Fully aligned	
Fundamental principles relating to processing (Article 5)	Substantially aligned	• Data controllers not responsible for demonstrating compliance with the data protection principles
Lawfulness of processing (Article 6)	Fully aligned	
Consent (Articles 4, 7 and 8)	Substantially aligned	• No explicit requirement that consent be as easy to withdraw as to give
Special categories of personal data (Articles 9 and 10)	Substantially aligned	• No requirement of a legal or official authority for the processing of data relating to criminal convictions and offences
Individual rights (Articles 12-23)	Fully aligned	
Obligations on data controllers (Articles 24, 25, 30 and 32)	Substantially aligned	• The Data Protection Commissioner may 'prepare appropriate codes of practice' (s71(c)) but no requirement that a code of conduct or certification mechanism be put in place by which a controller can demonstrate appropriate technical and organisational measures
Obligations of data processors (Articles 28, 30 and 32)	Substantially aligned	• No requirement that a code of conduct or certification mechanism be put in place by which a processor can demonstrate appropriate technical and organisational measures
Data breach notifications (Articles 33 and 34)	Fully aligned	
Data protection impact assessments and prior consultation (Articles 35-36)	Fully aligned	
Data protection officers (Articles 37-39)	Fully aligned	
Codes of conduct and certification (Articles 40-43)	Partially aligned	• The Data Protection Commissioner may 'prepare appropriate codes of practice' (s71(c)) but there is no provision encouraging use of codes of practice as a means of verifying compliance with the Act

GDPR element and article(s)	Alignment rating	Areas not aligned in law
		• No certification scheme whereby the Commissioner monitors compliance with a code of practice and certifies controllers and processors as compliant with it
International transfers (Articles 44-49)	Substantially aligned	• No institutional arrangements to facilitate adequacy decisions and approval of transfers outside Barbados
Supervision (Articles 51-60, 69)	Substantially aligned	• No requirement that the Commissioner act independently and remain free from external influence • No board established for the Data Protection Commissioner, but the Act does establish a Data Protection Tribunal
Cooperation and mutual assistance (Articles 50, 60-67)	Not aligned	• No requirement that the Commissioner cooperate with supervisory authorities in other countries or facilitate mutual assistance
Remedies (Articles 77-84)	Partially aligned	• No general right of complaint to the Commissioner or general right of appeal from a decision of the Commissioner to the Tribunal • Commissioner not required to keep complainants updated and to advise on outcome within a specified period of time • No requirement that administrative fines be effective, dissuasive and proportionate • No right for data subjects to be represented by not-for-profit organisations • No requirement that processor only be liable for damage where it has acted outside the law or contrary to the lawful instructions of the controller • Where more than one controller or processor are involved in the same breach, no requirement that both be held liable for the entire damage
Specific processing situations (Articles 23, 85-91)	Substantially aligned	• Some broad exemptions not subject to safeguards or limitations e.g. section 30 on safeguarding national security

Source: Prepared by the author.

2. Main findings

Based on the areas of non-alignment between the DPA 2019 and GDPR identified above, this section sets out key areas for Barbados to consider if seeking to strengthen its data protection legislation:

Obligation to demonstrate compliance with the data protection principles

One of the GDPR's innovations is a reinforced principle of accountability for data controllers, requiring data controllers to be responsible for, and able to demonstrate compliance, with the principles of the Regulation. This principle pervades all the data protection principles under the GDPR and aims to encourage a shift towards a proactive approach to the management of personal data.

The DPA 2019 requires data controllers to comply with the data protection principles in Part II but does not go a step further to require controllers to *demonstrate* compliance with those principles. Instead, the DPA 2019 requires persons to register as data controllers and keep the Commissioner updated as to their data processing activities.

Introducing a requirement on data controllers to demonstrate compliance would reinforce and encourage use of the mechanisms in Part VI which controllers can use to identify, assess and mitigate risks to personal data, such as data protection impact assessments, prior consultation and designation of data privacy officers.

Broad exemptions not subject to safeguards

The DPA 2019 includes some broad exemptions exempting data controllers from applying its protections not subject to adequate safeguards or limitations. For example, the individual rights and other protections of the DPA do not apply to the processing of personal data for the safeguarding of

national security in Barbados.[52] As a result, there is no judicial oversight or other safeguards to ensure the proportionality of limitations placed on individuals' right to data protection for the purposes of safeguarding national security.

While it is undesirable to subject national security measures to heavy scrutiny given their sensitive nature, data protection laws should endeavour to balance data protection rights with national security and law enforcement interests. For example, the GDPR requires Member States to only restrict the scope of obligations and rights under the GDPR to safeguard national security, defence, and public security when the restriction respects 'the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard'.

Furthermore, substantive and procedural safeguards can be put in place to prevent abuse or unlawful access or transfer as a result of exemptions.[53] These can take the form of independent oversight from a closed court or Tribunal accompanied by a requirement to exercise exceptions on a case-by-case basis with consideration of the individual merits of the proposed data processing activity.

Codes of practice and certification mechanism

Under the DPA 2019, the Data Protection Commissioner may 'prepare appropriate codes of practice for the guidance of persons processing personal data' (s71(r)) but there is no requirement that a code of practice or certification mechanism be put in place by which a controller or processor can demonstrate appropriate technical and organisational measures. Furthermore, the DPA 2019 does not encourage use of codes of practice or a certification mechanism as a means of voluntarily verifying compliance with the Act. Persons directly affected by data processing may request that the Commissioner undertake an assessment of whether it complies with the Act, but this procedure cannot be initiated voluntarily by a data controller (s78).

It would be worthwhile to strengthen provisions relating to codes of practice and provide for a voluntary certification mechanism in the DPA 2019 in order to give organisations a means of verifying their compliance with the law at any stage of data processing activities and for all types of processing operations. This would complement the DPA's requirement to undertake data protection impact assessments before commencing 'high risk' data processing activities.

Cooperation and mutual assistance

There is no requirement in the DPA 2019 that the Data Protection Commissioner cooperate with supervisory authorities in other countries or facilitate mutual assistance for the effective global enforcement of data protection legislation. Ideally, the law would define the term 'mutual assistance' and set out its modalities, including timelines for response to requests and the format in which requested information should be supplied. Furthermore, the circumstances in which the Commissioner can refuse to comply with a request should also be set out.

Introducing a requirement to facilitate cooperation and mutual assistance would contribute to strengthening the enforcement of data protection law in the Caribbean and with EU countries and support the harmonisation of legal protections across the subregion. This is necessitated by the borderless nature of data flows and widespread sharing of data between countries.

Remedies

The DPA 2019 introduces strong remedies for individuals whose data protection rights have been breached, including a right to compensation and a specialist Data Protection Tribunal to hear appeals

[52] DPA 2019, section 30.
[53] GDPR, Article 23(2).

from persons who have been served with an enforcement notice, an information notice or a special information notice.[54]

Remedies could be further strengthened by providing a general right of complaint to the Commissioner and general right of appeal from a decision of the Commissioner to the Tribunal. Furthermore, the Commissioner should be required to keep complainants updated on the progress of complaints or to advise on an outcome within a specified period. Although unlikely to be necessary to establish a comparable level of protection or essential equivalency with the GDPR, further amendments available for consideration include a requirement that compensation provide an effective remedy and that fines be effective, dissuasive and proportionate.

The GDPR also contains rules for the apportionment of liability between data controllers and processors not reflected in the DPA, such as that the processor only be liable for damage where it has acted outside the law or contrary to the lawful instructions of the controller, and that where more than one controller or processor are involved in the same breach, both be held liable for the entire damage. Finally, the DPA does not contain a right for data subjects to be represented by not-for-profit organisations when making complaints and pursuing appeals.

Data sharing

Data sharing falls within the definition of processing in the DPA 2019, with the inclusion of "the disclosure of the information or data by transmission, dissemination or otherwise making available". The Act does not contain specific provisions facilitating public or private sector data sharing but nonetheless places several requirements on data controllers and processors that engage in data sharing. Data controllers are required to carry out data protection impact assessments before undertaking high risk forms of processing, and the sharing of data between data controllers and processors must be governed by a written contract.[55]

Although not necessary to further alignment with the GDPR, data sharing protections could be enhanced as a matter of best practice by also requiring the sharing of personal data between data controllers to be governed by a contract and stipulating what such a contract should contain. Furthermore, pursuant to section 71(c), the Data Protection Commissioner could consider sharing a code of practice for public and private sector data sharing.

3. Summary of recommendations

In addition to the more exhaustive areas for strengthening identified in Table 6 above, the following recommendations are highlighted for enhancing the protection of personal data pursuant to the DPA 2019:

- Establish an explicit duty of accountability on data controllers requiring them to demonstrate compliance with the data protection principles;
- Further refine the notion of consent by requiring it to be as easy to withdraw as to give;
- Introduce safeguards and limitations on broad exemptions to the DPA's protections, including independent oversight in appropriate cases and requiring a legal or official authority for the processing of data relating to criminal convictions and offences;
- Enhance the Data Protection Commissioner's supervisory powers by requiring him or her to act independently and remain free from external influence, to cooperate with supervisory authorities in other countries, and to facilitate mutual assistance;

[54] See sections 90-93 of the DPA 2019.
[55] See sections 58 and 65 of the DPA 2019.

- Enhance the remedies provided for in the DPA 2019 as outlined above to further GDPR alignment;
- Introduce voluntary means for data controllers to verify their compliance with the Act, such as a code of practice and certification mechanism; and
- Consider enacting a code of practice for public and private sector data sharing under section 71(c).

E. Belize

Drafted in 2014, Belize's Data Protection Bill aims to promote the protection of personal data processed by public and private bodies and provide for the establishment of the Office of the Information Commissioner. The Bill is currently undergoing a review by the Ministry of Investment, Trade and Commerce (MITC) working in partnership with the Central Information Technology Office (CITO).

1. Areas of non-alignment with the GDPR

As Table 7 demonstrates, the Bill is substantially aligned with one area of the GDPR, partially aligned with eleven and not aligned with the remaining six.

Table 7
Alignment of Belize's legislation with the GDPR

GDPR element and article(s)	Alignment rating	Areas not aligned in law
Material scope and definitions (Articles 2 and 4)	Partially aligned	• Definition of personal data only applies in respect of commercial transactions (s2) • No definition of data processor or profiling • Definition of sensitive personal data does not include data revealing race, ethnic origin, trade union membership, genetics, biometrics, and sex life (s2)
Territorial scope (Article 3)	Partially aligned	• Limited extraterritorial scope • Unclear wording used in relation to data controllers not established in Belize (s4(2)(b))
Fundamental principles relating to processing (Article 5)	Substantially aligned	• No principle of accountability of data controllers • Overly broad exceptions to disclosure principle in s19(c), (d) and (c) based on data users' reasonable beliefs and ministerial discretion without judicial oversight or other safeguards • Concepts of fairness and transparency from the GDPR's lawfulness, fairness, and transparency principle (Part II) missing from the general principle (s7)
Lawfulness of processing (Article 6)	Partially aligned	• A data user may process personal data 'if necessary' when showing one of the lawful grounds, rather than to the extent necessary (s7(2)) • Consent is a lawful ground for processing, but there is no requirement that it be given for specific purposes (s7(1)(a)) • No grounds for processing for the performance of a task carried out in the public interest or in the exercise of official authority or for the purposes of the legitimate interests pursued by the controller
Consent (Articles 4, 7 and 8)	Not aligned	• No definition of consent • Consent only required to be 'explicit' in relation to sensitive personal data (s20(1)(a)) • No requirement to allow withdrawal of consent • No provisions regarding obtaining consent from children
Special categories of personal data (Articles 9 and 10)	Partially aligned	• Definition of 'sensitive personal data' does not capture racial or ethnic origin, trade union membership, genetics, biometrics or sex life

GDPR element and article(s)	Alignment rating	Areas not aligned in law
		• Processing of sensitive personal data permitted where necessary for 'any other purposes as the Minister thinks fit' without judicial or parliamentary oversight (s20(1)(b)(x)) • Legal or official authority not required for the processing of data relating to criminal convictions and offences
Individual rights (Articles 12-23)	Partially aligned	• No right to erasure, to restriction or suppression of personal data, to data portability, to object to processing, and in relation to automated decision making and profiling • A fee is chargeable to access personal data (s14) • Alternative format available for sensory disabilities but not mental and intellectual disabilities (s17(2)) • Data user not required to inform data subjects about their rights
Obligations on data controllers (Articles 24, 25, 30 and 32)	Partially aligned	• Data users not required to review and update as necessary practical steps to protect personal data under security principle (s10) • Data users not required to maintain a record of processing activities • Minister may make regulations prescribing codes of practice under s44 but there is no provision for codes of practice or a certification mechanism for data users to demonstrate compliance with their obligations
Obligations of data processors (Articles 28, 30 and 32)	Partially aligned	• Obligation is on data user, not processor, to ensure that the processor implements appropriate technical and organisational measures (s10(2)) • No requirement that data processing between a data user and processor be governed by a contract • Data processor not required to maintain records of data processing activities • Data processor not required to obtain the authorisation of the data user to engage another processor or only act on the user's instructions
Data breach notifications (Articles 33 and 34)	Not aligned	• No definition of personal data breach • No requirement that data users record or report personal data breaches to Information Commissioner or data subjects • No requirement that data processor report personal data breaches to data user
Data protection impact assessments and prior consultation (Article 35-36)	Not aligned	• No requirement that data users carry out impact assessments for high risk or sensitive forms of processing
Data protection officers (Articles 37-39)	Not aligned	• No requirement on public or private bodies to appoint data protection officers in certain circumstances
Codes of conduct and certification (Articles 40-43)	Partially aligned	• Minister may make regulations prescribing codes of practice (s44) but no specification as to what they should contain or system for data users to use them to verify compliance with the law • Assessment of processing mechanism in s31 cannot be triggered by data users as a means of verifying compliance with the law
International transfers (Articles 44-49)	Not aligned	• International transfers not dealt with in the Act • No safeguards for transfers of personal data to other countries or international organisations • No complaint or enforcement procedure for breaches of personal data by organisations in other countries or international organisations
Supervision (Articles 51-60, 69)	Partially aligned	• Information Commissioner not required to act independently or remain free from external influence • Roles and responsibilities of the Office of the Information Commissioner not set out (only for Commissioner – s24) • Authorisation and advisory powers not as extensive as in GDPR e.g. no certification or prior consultation procedures

GDPR element and article(s)	Alignment rating	Areas not aligned in law
		• Investigative and corrective powers not as extensive as GDPR e.g. suspension of data flows and bans on processing of data not provided for • No board for Office of Information Commissioner • No provisions dealing with serious staff misconduct
Cooperation and mutual assistance (Articles 50, 60-67)	Not aligned	• No requirement on supervisory authority to cooperate with supervisory authorities in other countries and to facilitate mutual assistance
Remedies (Articles 77-84)	Partially aligned	• No requirement on Information Commissioner to keep complainant informed of progress and outcome of complaint within a certain time period • No right to an effective judicial remedy or to receive compensation from data user and processor, only to institute civil proceedings (s32) • No administrative fine for undertakings as a percentage of annual worldwide turnover • No guiding factors to be considered in imposing fines
Specific processing situations (Articles 23, 85-91)	Partially aligned	• No rules to reconcile secrecy obligations with the power of the supervisory authority to obtain access to personal data and information and search premises • Broad exemptions not subject to safeguards or limitations e.g. for the prevention or detection of crime or for the purpose of investigations, and for the assessment and collection of tax

Source: Prepared by the author.

2. Main findings

Based on the areas of non-alignment between the 2014 Bill and GDPR identified above, this section sets out key areas for Belize to consider if seeking to revise the Bill or adopt new data protection legislation:

Definitions of 'personal data' and 'sensitive personal data'

Like some other data protection laws in the subregion,[56] Belize's bill defines 'personal data' to only apply in respect of commercial transactions (s2). This means that personal data is only captured when being processed by public and private bodies as part of a transaction of a commercial nature, thus excluding a wide variety of non-commercial activities for educational, employment, health, taxation, social security and welfare purposes. At noted above, the term 'commercial transactions' can also invite a number of interpretations, leading to uncertainties in its application.

The Bill does not contain definitions of data processor, profiling and automated decision-making. Under the GDPR, data controllers and processors each have obligations when processing personal data. In particular, it is important to include a definition of 'data processor' in data protection legislation for each party to understand their obligations when processing personal data and to ensure the effective enforcement of the law.

Furthermore, the definition of 'sensitive personal data' does not include data revealing race, ethnic origin, trade union membership, genetics, biometrics, and sex life (s2). These categories of highly sensitive data are thereby excluded from the Act's more stringent conditions and safeguards for the processing of sensitive data, such as the requirement to obtain a data subject's explicit consent.

Territorial scope, cooperation and mutual assistance

The Bill applies to two groups: 1) persons established and processing personal data in Belize; and 2) persons not established in Belize but using equipment in Belize for processing personal data

[56] See the review of Antigua and Barbuda's Data Protection Act 2013 above.

otherwise than for the purposes of transit through Belize. The language of this section could be simplified to refer to the location where processing takes place and omit any mention of the equipment being used for this purpose.

Belize may also want to consider extending the extraterritorial scope of its law to persons not established in Belize processing personal data of Belizean nationals outside of Belize. As noted above, there is a global trend for data protection laws to be given extraterritorial jurisdiction to provide citizens with effective protection in light of the borderless nature of data flows and processing technologies.[57] The GDPR limits its extraterritorial effect to non-EU controllers and processors targeting EU data subjects, thereby attempting to avoid overreach. Enforcement of extraterritorial data protection legislation can provide a challenge, particularly for states with small data protection authorities and limited investigative capacity.

In any case, the Bill should be revised to require the Information Commissioner to cooperate with other supervisory authorities and facilitate mutual assistance. In lieu of more extensive extraterritorial reach, a duty to provide mutual assistance will nonetheless enable the Information Commissioner to cooperate with foreign supervisory authorities in cases impacting the data protection rights of Belizeans and help to prevent forum shopping by foreign companies.[58]

Consent of data subjects

Consent is a lawful ground for data processing under the Bill, but the term 'consent' is not defined and there is no requirement that it be given for one or more specific purposes (s7(1)(a)). Furthermore, consent need only be 'explicit' in relation to sensitive personal data (s20(1)(a)), suggesting that implied consent might be sufficient to establish lawful grounds for processing of non-sensitive personal data. Relying on implied consent to transfer data is no longer possible under the GDPR as the regulation requires a clear affirmative action or statement from the data subject in order to establish consent.

The Bill also does not allow withdrawal of consent or contain special provisions for obtaining consent from children. Ensuring that data subjects can withdraw consent to having their personal data processed is a critical component of consent provisions under the GDPR. Withdrawal of consent must be as easy as it was to give. Furthermore, the GDPR provides that persons under the age of 16 cannot give consent for the processing of personal data for the provision of online services[59] and therefore consent must be sought from the person who holds parental responsibility for a child. Although the default age of consent is 16, EU Member States have some flexibility to set the age between the ages of 13 and 16.

Rights of data subjects and the privacy and data protection principles

The data protection principles and individual rights contained in the Bill depart from the GDPR's provisions in some important respects. There is no principle of accountability of data controllers, requiring them to be able to demonstrate compliance with the data protection principles. The concepts of fairness and transparency are also missing from the general principle in section 7, which sets out the lawful grounds for processing.

Data subjects' rights are also less extensive than those found in the GDPR. There is no right to erasure, to restriction or suppression of personal data in certain circumstances, to data portability, to

---

[57] B. Greze, 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives' International Data Privacy Law 9(2), May 2019, pp. 109–128.

[58] On forum shopping, see B. Greze, above, p. 124.

[59] Specifically, this restriction applies in relation to the offer of Information Society Services, which are defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". See Article 1(1)(b) of Directive (EU) 2015/153.

object to processing, and in relation to automated decision making and profiling. The right to object to processing is an important measure that allows individuals to stop or prevent data controllers from processing their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing, but in other cases data controllers can continue processing if they demonstrate that they have a compelling reason to do so.

In other points of difference to the GDPR, data users are not required to inform data subjects about their rights and a fee is chargeable to access personal data (s14). When responding to a data access request, data users are required to provide a copy of the data in an alternative format to persons with sensory disabilities, but this requirement does not extend to persons with mental and intellectual disabilities (s17(2)).

Obligations on data users and processors

Under the security principle in section 10, data users must take 'practical steps' to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

However, section 10 departs from the GDPR's integrity and confidentiality principle in some important respects. Data users are not required to review and update the practical steps they take to protect personal data as necessary and the obligation is on the data user, not processor, to ensure that the processor implements appropriate technical and organisational measures (s10(2)).

Neither data users nor processors are required to maintain a record of processing activities and, importantly, there is no requirement that data processing between a data user and processor be governed by a contract. Data processors are also not required to obtain the authorisation of the data user to engage another processor or act only on the instructions of the data user.

Broad exceptions and exemptions not subject to independent oversight or other safeguards

The Bill contains some broad exceptions to the disclosure principle in sections 19(c)-(c) based on ministerial discretion and data users' reasonable belief as to the existence of a lawful right or the consent of data subjects. These circumstances allow data users to disclose personal data "for any purpose other than the purpose for which the personal data was to be disclosed at the time of its collection or any other purpose directly related to that purpose." This runs contrary to the requirement in section 9 that data only be disclosed without consent for the purpose for which it is collected. Furthermore, permitting ministers to disclose personal data for purposes unrelated to those for which it was collected creates the risk of abuse and thus should be subject to independent oversight or other safeguards. Likewise, allowing data users to disclose personal data on the basis of 'reasonable beliefs' falls short of the conditions for data disclosure in the GDPR.

Processing of sensitive personal data is permitted under the Bill where necessary for 'any other purposes as the Minister thinks fit' (s20(1)(b)(x)). A discretion to define new conditions for the processing of sensitive personal data should be subject to judicial or parliamentary oversight and/or other safeguards, since this power relates to categories of highly sensitive data and its arbitrary exercise could place the rights of data subjects at risk.

The Bill also contains a number of exemptions to its application in section 21, where personal data is processed for crime prevention or investigation and tax assessment and collection purposes, among others. These exemptions are not limited by any limitations or safeguards, such as that they can only be exercised where necessary to enable the processing of personal data in a way that is required or necessary, the processing is not likely to cause substantial damage or distress to an individual, and the processing is subject to appropriate safeguards for individuals' rights and freedoms. Under section 22, the Minister may also create further exemptions upon the recommendation of the Information Commissioner. Given that exemptions can run contrary to the Bill's aims, they should constitute an

exhaustive list or, failing this, be subject to judicial or parliamentary oversight (for example, a ministerial order subject to affirmative resolution).

Requirement to report personal data breaches

The GDPR requires data controllers to report personal data breaches to the supervisory authority and, in some cases, affected data subjects. This requirement can be avoided where the breach is 'unlikely to result in a risk to the rights and freedoms of natural persons'. Data breach notifications are an important part of the GDPR's transparency and accountability approach and are also international best practice featuring in the legislation of a number of other jurisdictions, including Australia, Canada and the US, to name a few.

The Bill does not contain a requirement that data users either record or report personal data breaches to the Information Commissioner or seriously affected data subjects. There is also no requirement that data processors assist data users to perform this duty by reporting data breaches to them. Foreign supervisory authorities may take the absence of a breach notification requirement into account when determining whether Belize offers 'equivalent protection' to that afforded by their legislation for the purposes of authorising international transfers.

Mechanisms to ensure sufficient technical and organizational security measures

Although the Bill requires data users to take practical steps to protect personal data from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, this obligation is not accompanied by tools that data users can adopt to proactively identify, assess and mitigate risks to personal data.

There is no requirement that data users carry out impact assessments for high risk or sensitive forms of data processing or that public and private bodies appoint data protection officers in certain circumstances. The Minister may make regulations prescribing codes of practice (section 44) but the Bill does not specify what they should contain or establish a system whereby they can be used to verify compliance with the law. Furthermore, the assessment of processing mechanism in section 31 cannot be triggered by data users as a means of verifying compliance with the law.

Safeguards for transfers of personal data to other countries

International transfers not dealt with in the Bill, leaving it unclear in what circumstances data users in Belize can make cross-border data transfers. There are also no safeguards for transfers of personal data to other countries or international organisations. The substantive requirements for such transfers in addition to supporting procedural and enforcement mechanisms should be introduced to Belize's data protection law.

Both the importance of, and risks associated with, cross-border data flows are well-recognised in modern data protection laws, which usually require the recipient country to guarantee an equivalent level of protection to that provided for in the law of the sending country. This provides protection to data subjects that their information will not be subject to lower standards once transferred to another country and makes it more difficult for data controllers to circumvent data protection principles by moving their processing operations to countries with less onerous laws.[60]

Remedies

The Bill does not contain a requirement on the Information Commissioner to keep complainants informed of progress and the outcome of complaints within a certain time period, rather imposing a

[60] For more on this subject, see J. Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) International Data Privacy Law pp. 1-20.

more murky requirement that the Information Commissioner notify the data subject of his or her decision 'as soon as is reasonably practicable' (s25(2)(b)).

Data subjects also do not have a right to an effective judicial remedy or to receive compensation from data users or processors, only to institute civil proceedings (s32). Furthermore, both public and private bodies can rely on a defence that they took 'such care as in all the circumstances was reasonably required' to comply with the requirement concerned, regardless of the damage or distress that has been caused to data subjects as a result of the breach. The Bill does not allow the imposition of fines for undertakings as a percentage of annual worldwide turnover and there are no guiding factors to be considered in imposing fines.

Data sharing

The sharing of personal data is captured by the Bill's definition of processing, with the wording 'the disclosure of personal data by transmission, transfer, dissemination or otherwise making available' (section 2).

However, the Bill does not contain provisions facilitating public and/or private sector data sharing with appropriate safeguards. For example, there is no requirement that data users undertake privacy impact assessments before sharing data in high risk or novel situations or that sharing of personal data between data users and processors be governed by a contract. The Minister may make regulations under section 44 prescribing codes of practice but there is no requirement that one be established specifically for data sharing.

Furthermore, as outlined above, the Bill contains some broad exceptions to the disclosure principle in sections 19(c)-(c), allowing data to be shared based on ministerial discretion without oversight and data users' reasonable beliefs as to the existence of a lawful right or the consent of data subjects.

3. Summary of recommendations

In addition to the more exhaustive areas for strengthening identified in Table 7 above, the following recommendations are highlighted for enhancing the protection of personal data in Belize pursuant to new or amended data protection legislation:

- Amend the definition of personal data to apply to all data processing activities of public and private bodies, including both commercial and non-commercial transactions;
- Enhance the privacy and data protection principles by introducing a duty of accountability on data users and adding requirements of fairness and transparency to the general principle;
- Refine the lawful grounds for processing by only allowing data users to process 'to the extent necessary', requiring consent to be given for specific purposes, and adding further grounds for processing as outlined above;
- Improve the protection of sensitive personal data by adding further categories of highly sensitive data to the definition as outlined above, requiring a legal or official authority for processing of data relating to criminal convictions and offences, and removing the ability for the Minister to process for any other purpose he or she thinks fit;
- Clarify the notion of consent by defining the term, allowing withdrawal of consent, and introducing provisions on obtaining consent from children;
- Introduce further individual rights for data subjects, require data users to inform data subjects of their rights, remove the obligation to pay a fee to access personal data in the first instance, and make an alternative format available for persons with sensory, mental and intellectual disabilities;

- Improve the obligations on data users and processors by requiring both users and processors to maintain a record of processing activities, directly obliging data processors to ensure they have in place appropriate security measures, requiring that data processing between a data user and processor be governed by a contract, and requiring security measures to be reviewed and updated as necessary;
- Introduce a data breach notification requirement on both data users and processors;
- Introduce mechanisms by which data users and processors can proactively identify, assess and mitigate risks to personal data, including impact assessments, prior consultation, data protection officers and a certification mechanism;
- Introduce independent oversight and other safeguards for any exceptions or exemptions to the Bill's application, including those based solely on ministerial discretion;
- Introduce substantive requirements in addition to supporting procedural and enforcement mechanisms for transfers of personal data to other countries;
- Enhance the position of the Information Commissioner by requiring this person to act independently and free from external influence in order to investigate actions of public bodies in an objectively fair and impartial manner, permitting the suspension of data flows and bans on processing, and requiring cooperation and provision of mutual assistance to other supervisory authorities;
- Enhance the Bill's remedies by introducing a right to an effective judicial remedy and compensation and requiring the Information Commissioner to inform complainants on the outcome of complaints within a certain time period; and
- Facilitate public and private sector data sharing with appropriate safeguards by establishing a code of practice on data sharing, requiring data sharing to be governed by a contract and removing broad exceptions to the disclosure principle based on ministerial discretion and data users' reasonable beliefs.

F. Cayman Islands

The Data Protection Law (DPL) 2017, which came into force on 30 September 2019, is a law to provide for the protection of personal data and incidental and connected purposes. It is supplemented by the Data Protection Regulations 2018, which provide additional rules in relation to personal data requests, duties of data controllers, and certain exemptions under the Law.

The Office of the Ombudsman is the Cayman Islands' supervisory authority for data protection. The Ombudsman replaces and has the powers and functions of the Information Commissioner referred to in the DPL, pursuant to the Freedom of Information Law (2007 and 2020 Revisions).[61] The Ombudsman has published a comprehensive guide for data controllers on the application of the DPL 2017.[62]

1. Areas of non-alignment with the GDPR

As Table 8 shows, the DPL 2017, in combination with the Freedom of Information Laws (2007 and 2020 Revisions) where relevant, is fully aligned with one area of the GDPR, substantially aligned with ten, partially aligned with five and not aligned with the remaining two.

[61] See section 59 'Transitional provisions' of the Freedom of Information law (2020 Revision).
[62] See the Cayman Islands' Guide for Data Controllers.

Table 8
Alignment of the Cayman Islands' legislation with the GDPR

GDPR element and article(s)	Alignment rating	Areas not aligned in law
Material scope and definitions (Article 2 and 4)	Substantially aligned	• Definition of personal data includes unnecessary distinctions on 'expressions of opinion about the living individual' and 'any indication of the intentions of the data controller or any other person in respect of the living individual' (s2) • Sex life but not sexual orientation included in categories of sensitive personal data (s3)
Territorial scope (Article 3)	Substantially aligned	• Extraterritorial scope on different basis to GDPR • DPL 2017 applies both to data controllers established and not established in Cayman Islands provided they are processing data in the Islands (s6)
Fundamental principles relating to processing (Article 5)	Substantially aligned	• No principle of accountability of data controllers: data controllers shall comply with but are not explicitly required to demonstrate compliance with the data protection principles (Schedule 1)
Lawfulness of processing (Article 6)	Substantially aligned	• Processing for the exercise of public functions not subject to limitations i.e. no requirement to balance prejudice to the rights and freedoms of the data subject (schedule 2(5))
Consent (Articles 4, 7 and 8)	Partially aligned	• No special provisions on obtaining consent from children • Right to withdraw consent exists but no right to be informed of this right (schedule 5(3)) • No requirement that consent be as easy to withdraw as to give • No requirement that request for consent be in an intelligible and easily accessible form, using clear and plain language, other than stating that it 'be presented in an appearance that is distinguishable from the other matter' (schedule 5(2))
Special categories of personal data (Articles 9 and 10)	Substantially aligned	• Sex life but not sexual orientation included in categories of sensitive personal data (s3) • No legal or official authority required for processing of data relating to criminal convictions and offences
Individual rights (Articles 12-23)	Substantially aligned	• No right to reuse personal data across different services (data portability) • Limitations and safeguards on exemptions to individual rights require strengthening
Obligations on data controllers (Articles 24, 25, 30 and 32)	Substantially aligned	• No requirement on data controller to maintain a record of processing activities • Ombudsman can encourage but not require trade associations to make codes of practice and verify whether such codes promote good practice
Obligations of data processors (Articles 28, 30 and 32)	Partially aligned	• No requirement on data processor to maintain a record of processing activities • No direct obligation on data processors to implement appropriate technical and organisational measures under the DPL (but data processors must enter into a contract with data controller requiring compliance with data security obligations (see s5(4) and schedule 1, pt. 2(3)(c)) • Mechanism in s42(4) for the Ombudsman to assess processing of personal for adherence to good practice only applies to data controllers
Data breach notifications (Articles 33 and 34)	Substantially aligned	• No requirement on the data processor to report personal data breaches to the data controller as soon as it becomes aware
Data protection impact assessments and prior consultation (Articles 35-36)	Not aligned	• No requirement that data controllers carry out data protection impact assessments in particular circumstances • Regulations required under s15 before giving effect to prior approval mechanism
Data protection officers (Articles 37-39)	Not aligned	• No requirement that public or private sector organisations appoint data protection officers • Public authorities under the Freedom of Information Law (2020 Revision) are required to appoint information managers, but this requirement is not extended to data protection under the DPL 2017
Codes of conduct and certification (Articles 40-43)	Partially aligned	• No requirement to draw up codes of practice, however Cabinet may make regulations for the preparation and dissemination of codes of practice (s42) • Ombudsman empowered to assess processing of data controllers for adherence to good practice (s42(4), but no requirement that this be guided by a code of practice
International transfers (Articles 44-49)	Fully aligned	

GDPR element and article(s)	Alignment rating	Areas not aligned in law
Supervision (Articles 51-60, 69)	Substantially aligned	• No provisions to deal with serious misconduct of staff • The Ombudsman reports to a Standing Committee of the Legislative Assembly instead of a board
Cooperation and mutual assistance (Articles 50, 60-67)	Partially aligned	• No definition of mutual assistance • No provisions setting out the modalities of mutual assistance, including timelines and formats for requests or when the Ombudsman can refuse to comply with a request
Remedies (Articles 77-84)	Partially aligned	• No requirement on Ombudsman to keep complainant informed of progress or outcome of complaint within a specified time • No requirement that the imposition of administrative fines be effective, proportionate and dissuasive • No ability to impose a fine amounting to a percentage of annual worldwide turnover in the case of an undertaking • No requirement that a controller and processor both involved in same breach be liable for entire damage • No requirement that a processor only be liable for damage where it acted outside the law or contrary to the lawful instructions of the controller
Specific processing situations (Articles 23, 85-91)	Substantially aligned	• Exemptions relating, for example, to national security (s18) and public safety, prevention of crime and public interests not subject to adequate limitations and safeguards (s21)

Source: Prepared by the author.

2. Main findings

Based on the areas of non-alignment between the DPL 2017 and the GDPR identified above, this section sets out key areas for the Cayman Islands to consider if seeking to revise its legislation:

Definition of 'personal data' and 'sensitive personal data'

The definition of personal data contained in the DPL 2017 makes a distinction between 'expressions of opinion about the living individual' and 'any indication of the intentions of the data controller or any other person in respect of the living individual'.[63] The GDPR simply defines personal data as 'any information relating to an identified or identifiable natural person'. The inclusion of these distinctions in the DPL's definition of 'personal data' is unnecessary since both categories would in any event constitute personal data where they enable identification of a living individual and could lead to particular focus on journalist's work.

Furthermore, the DPL 2017 does not include sexual orientation as a category of personal data that is highly sensitive and deserving of special protection. The category of 'sex life' is included, but this carries a different meaning to 'sexual orientation'. To give one example, while a child may identify as having the sexual orientation of bisexual, sex life is a term generally only used in relation to persons above the age of consent.

Consent of data subjects

The definition of consent in the DPL 2017 mirrors that found in the GDPR. However, the DPL 2017 does not go as far as the GDPR in further fleshing out the concept of consent. While the right to withdraw consent is provided for in schedule 5(3), there is no requirement that data subjects be informed of this right. The DPL 2017 requires that a request for consent 'be presented in an appearance that is distinguishable from the other matter' in schedule 5(2), but not that it be provided in an intelligible and easily accessible form, using clear and plain language. Similarly, there is no requirement that consent be as easy to give as to withdraw.

[63] DPL 2017, section 2.

Furthermore, the DPL 2017 does not provide guidance on obtaining consent from children, other than to state that consent shall not provide a legal basis for data processing 'where there is a significant imbalance between the position of the data subject and the data controller' (schedule 5(4)). This is similar to the language of 'clear imbalance' used in Recital 43 of the GDPR.

It is arguable that a significant or clear imbalance exists in nearly all situations where data controllers obtain consent from data subjects who are children. It is for this reason that the GDPR provides separate guidance on obtaining consent from children. The same can be said of data subjects consenting to share personal data with large social media services, such as Facebook. In these scenarios, data subjects inevitably face a situation of significant imbalance as they can either consent to the service's terms or choose to forego use of a popular platform.

Obligations of data controllers and processors

Absent from the data protection principles in the DPL 2017 is a principle of accountability on data controllers. This means that data controllers are not explicitly required to demonstrate compliance with the data protection principles in Schedule 1, although in practice this would be required retroactively when they are subject to an investigation following a complaint or on the Ombudsman's own initiative.

Moreover, the DPL 2017 does not impose direct enforceable obligations on data processors to implement appropriate technical and organisational measures to secure personal data, rather requiring data controllers to ensure that processors comply with the data protection principles in relation to the personal data processed on their behalf (s5(4)). Furthermore, if a data controller engages a processor, the two parties must enter into a contract where the processor agrees to implement appropriate organisational and technical measures (schedule 1, part 2(3)(c)).

This approach places a heavier burden on data controllers, especially small undertakings, than the GDPR's approach of requiring both data controllers and processors to take direct responsibility for putting in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. It also removes the possibility of direct recourse against the data processor, meaning that the Ombudsman would need to pursue the data controller for any unlawful acts of the processor, failure of the processor to act on the controller's instructions or breach of the contractual obligation to implement appropriate security measures.

Exemptions subject to limited safeguards

Part 4 of the DPL 2017 contains a number of exemptions to the application of the data protection principles and fundamental rights. Most of the exemptions are subject to express limitations but, in some cases, these could be strengthened to further ensure the proportionate and reasonable exercise of the discretion. For example, processing activities for the exercise of a public function relating to public safety, prevention of crime and important economic and financial interests are exempt from the right to access personal data (s8) and the first data protection principle that data be processed lawfully and fairly[64] 'to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of the function.' To ensure risks to human rights are taken into account, the data controller could also be required to consider whether exercising the exemption respects individuals' rights and is a necessary and proportionate measure in a democratic society.[65]

---

[64] To the extent to which it requires compliance with paragraph 2 of Part 2 of Schedule 1. See the DPL's definition of 'subject information provisions'.

[65] Article 23 of the GDPR allows Member States to restrict the rights and obligations of data controllers and processors by way of legislative measure where "such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard."

Furthermore, personal data is exempt from the data protection principles, the rights of data subjects, and the provisions on restricted processing, personal data breaches and enforcement (Parts 2, 3 and 6) where necessary for safeguarding national security. There is some oversight by way of the Governor issuing certificates for exercise of the exemption in consultation with the National Security Council and the Ombudsman being empowered to determine whether a certificate applies to personal data subject to a complaint (s18(7)). However, it is possible for the Governor to issue blanket, prospective exemptions as certificates do not need to be task-related or consider the individual merits of each application. There is also no requirement that the Governor consider whether issuing an exemption certificate is a necessary and proportionate measure in a democratic society or would unjustifiably threaten individual rights.

The DPL 2017 could be further strengthened by explicitly providing data subjects with judicial review rights of national security certificates issued by the Governor. Although the Governor may consult the National Security Council (s18(3)), this body comprises members of the executive branch of government and therefore cannot provide independent oversight of the exercise of executive powers.[66] Furthermore, the right to seek judicial review under section 47 of the DPL is only available to persons who have received an information requirement, enforcement order or monetary penalty.

Personal data breaches

Data controllers are required to report personal data breaches to both individuals and the Ombudsman without undue delay and in any event no longer than five days after the controller should have been aware of the breach. The DPL 2017 exceeds the requirements of the GDPR in that individuals must be notified of all breaches, not just where a breach is likely to result in a high risk of adversely affecting individuals' rights and freedom.

However, there is no requirement on data processors to report data breaches to the data controller or Ombudsman, creating a gap in the legislation where a processor is responsible for a personal data breach.

Mechanisms to ensure sufficient technical and organizational security measures

The DPL 2017 contains some mechanisms by which data controllers can take actively steps to monitor and ensure compliance with their obligations. For example, the Ombudsman is empowered to assess whether the processing activities of data controllers adhere to good practice under section 42(4). Furthermore, Cabinet may make regulations for the preparation and dissemination of codes of practice and the Ombudsman may encourage trade associations to prepare and disseminate codes of practice to guide good practice. While such regulations and codes of practice are yet to be made, the Ombudsman has published a Guide for Data Controllers pursuant to the DPL 2017.

However, the legislation does not include other important security mechanisms contained in the GDPR, including data protection impact assessments and data protection officers. While controllers and processors could implement these voluntarily to put in place 'appropriate technical and organizational measures', there is currently no requirement that they carry out data protection impact assessments in certain circumstances, such as when using new technologies or where data processing presents a high risk to the rights and freedoms of individuals. Public authorities under the Freedom of Information Law (2020 Revision) are required to appoint information managers, but this requirement is not extended to data protection under the DPL 2017. Therefore, neither public nor private bodies are required to appoint data protection officers.

[66] See section 58 of the Cayman Islands Constitution Order 2009. See the Recommendations in Part III for further discussion of independent oversight.

Furthermore, regulations are required to give effect to the 'preliminary determination' procedure in section 15 which would require data controllers to seek prior approval for processing considered particularly likely to cause substantial damage or distress to data subjects or otherwise significantly prejudice the rights and freedoms of data subjects.

Mutual assistance

While the Ombudsman (previously, the Commissioner) is the designated authority in the Cayman Islands for the purposes of international cooperation related to data protection, the DPL 2017 does not require the Ombudsman to provide mutual assistance to other countries and international organizations in the enforcement of data protection legislation.

While the term cooperation is interpreted broadly to include mutual assistance in some jurisdictions, it can be useful to refer specifically to mutual assistance since it imports a subset of rules under international law by which States can seek and help in gathering evidence for use in investigations and proceedings.[67] The adoption of common rules in the field of mutual assistance for data protection matters across the Caribbean would strengthen the enforcement of data protection law as well as support the harmonisation of legal protections in the subregion.

Beyond designating the Ombudsman as the relevant authority to facilitate international cooperation and mutual assistance, regulations could be made under section 37(2) in order to import requirements to provide mutual assistance in data protection matters, establish mutual assistance mechanisms and engage in joint enforcement actions with other countries.

Remedies

The DPL 2017 does not require the Ombudsman to keep complainants informed of progress in processing complaints or the outcome of those complaints. The Ombudsman could have a duty to advise data subjects 'without undue delay', 'as soon as feasible' or within a specified timeframe in order to enhance the effectiveness of remedies available to data subjects. Furthermore, the Ombudsman does not have the power to impose monetary penalty orders on data processors, meaning that where a controller and processor are involved in the same personal data breach the controller is liable for the entire damage.

The DPL 2017 states that a monetary penalty may not exceed two hundred and fifty thousand dollars but does not allow the Ombudsman to impose a penalty amounting to a percentage of annual worldwide turnover in the case of an undertaking. It is questionable whether a fine of two hundred and fifty thousand dollars would operate as an effective deterrent for large global companies processing data in the Islands. Guidance on the imposition of monetary penalty orders has been published under section 56 of the DPL 2017.[68]

Data sharing

The DPL 2017 does not contain any special provisions to facilitate public or private sector data sharing, although data sharing is captured in the definition of personal data and therefore any data sharing must be carried out in accordance with the conditions for processing in schedule 2 or, in the case of sensitive data, schedule 3.[69] While any provisions specifically facilitating data sharing would be in

[67] See Article 61 of the GDPR on mutual assistance.
[68] See https://ombudsman.ky/images/pdf/OMB_DP_Guidance_on_Monetary_Penalties.pdf.
[69] See definition of processing in section 2 where it refers to 'disclosing the personal data by transmission, dissemination or otherwise making it available.'

addition to the requirements under the GDPR, they are recommended as a matter of best practice to incentivise legitimate data sharing subject to necessary limitations and safeguards.

The Ombudsman's Guide for Data Controllers contains some guidance for controllers wishing to share data, such as noting that each controller has a 'duty to make reasonable efforts to ensure that the receiving controller will be compliant' and that it is 'best practice to agree upfront on the handling of the shared data, especially for when you no longer need to share the data'.[70] Furthermore, it states that the right to be informed requires organisations to inform individuals that they plan to share their personal data.

However, the DPL 2017 does not require the sharing of personal data between data controllers to be governed by a contract (only between data controllers and processors). As a matter of best practice, a requirement could be introduced that data sharing between controllers be governed by a contract in addition to requiring a lawful basis for processing. The contract would set out, *inter alia*, the data to be shared, security measures, retention periods, and apportionment of liability for personal data breaches. Where the data sharing involves a high risk to individuals' rights and freedoms, the DPL should also require data controllers to seek the approval of the Ombudsman.

3. Summary of recommendations

In addition to the more exhaustive areas for strengthening identified in Table 8 above, the following recommendations are highlighted for enhancing the protection of personal data pursuant to the DPL 2017:

- Align the definition of 'personal data' with the GDPR's definition by removing the distinctions between expressions of opinion and intentions of the data controller;
- Expand the definition of 'sensitive personal data' to include further categories of highly sensitive personal data, namely sexual orientation;
- Introduce an explicit principle of accountability of data controllers requiring them to demonstrate compliance with the data protection principles;
- Enhance consent provisions by requiring data subjects to be informed of the right to withdraw consent, requiring a request for consent to be presented in clear and plain language, and including additional guidance on obtaining consent from children;
- Require data controllers and processors to keep a record of data processing activities;
- Introduce a direct requirement on data processors to implement appropriate technical and organisational measures and require data processors to report personal data breaches to data controllers;
- Provide additional safeguards and limitations on exemptions to the DPL's protections to ensure respect for individual rights;
- Make regulations under section 15 to give effect to the preliminary determination procedure and under section 42 for the preparation and dissemination of codes of practice;
- Introduce requirements to carry out data protection impact assessments and to appoint data protection officers in certain circumstances;

[70] See the Cayman Islands' Guide for Data Controllers, pp. 57, 124 and 200.

- Require the Ombudsman to facilitate mutual assistance in addition to general international cooperation and establish institutional arrangements for such assistance;
- Require the Ombudsman to keep complainants informed of progress in processing complaints and the outcome of those complaints;
- Empower the Ombudsman to impose monetary penalty orders on data processors in addition to controllers as well as penalties amounting to a percentage of annual worldwide turnover in the case of undertakings; and
- Create a data sharing code of practice and/or introduce a requirement that sharing of personal data between data controllers be governed by a contract in order to create incentives and gateways for legitimate data sharing (as a matter of best practice in addition to the requirements of the GDPR).

G. Jamaica

Jamaica has recently enacted the Data Protection Act (DPA) 2020, which aims to 'enable the public and private sectors to strengthen the protection of personal data' and establishes an Information Commissioner to monitor compliance with it.

The DPA 2020 replaces a data protection bill that was tabled in Parliament in 2017 and reviewed by a Joint Select Committee. Following the Committee's review, the House of Representatives withdrew the 2017 bill with a view to re-tabling the DPA 2020.

1. Areas of non-alignment with the GDPR

As Table 9 shows, the DPA 2020 is fully aligned with two areas of the GDPR, substantially aligned with eleven, and partially aligned with the remaining five.

Table 9
Alignment of Jamaica's Act with the GDPR

GDPR element and article(s)	Alignment rating	Areas not aligned in law
Material scope and definitions (Articles 2 and 4)	Substantially aligned	• Definition of 'personal data' includes individuals deceased for less than 30 years, expressions of opinion and indications of the data controller about the individual (s2) • Definition of 'process' includes information and personal data although the DPA only aims to protect personal data • Definition of 'sensitive personal data' (s2) excludes sexual orientation
Territorial scope (Article 3)	Fully aligned	
Fundamental principles relating to processing (Article 5)	Substantially aligned	• No explicit principle of accountability of data controllers requiring them to demonstrate compliance with the data protection standards in Part IV
Lawfulness of processing (Article 6)	Fully aligned	
Consent (Articles 4, 7 and 8)	Substantially aligned	• Not specified how a data controller should present a request to process personal data
Special categories of personal data (Articles 9 and 10)	Substantially aligned	• Sexual orientation excluded from categories of sensitive personal data • Legal or official authority not required for the processing of data relating to criminal convictions
Individual rights (Articles 12-23)	Partially aligned	• No requirement that data controllers inform data subjects about their rights (although Information Commissioner required to disseminate information about the Act) • No explicit right to erasure • Fee payable for right of access to personal data (s6(2)(c))

GDPR element and article(s)	Alignment rating	Areas not aligned in law
		• Minister has power to make further exemptions to rights conferred in Part II without independent oversight (s43)
Obligations on data controllers (Articles 24, 25, 30 and 32)	Substantially aligned	• Journalists subject to registration requirements with potential implications for press freedoms (s14-18)
Obligations of data processors (Articles 28, 30 and 32)	Partially aligned	• No directly enforceable obligations on data processors e.g. obligation is on data controller, not processor, to provide sufficient guarantees in respect of the processor's technical and organisational security measures (s30(4)-(5)) • Data processors not required to maintain a record of processing activities (although data controllers required to register a description of data processed on their behalf (s16(2)(d)))
Data breach notifications (Articles 33 and 34)	Substantially aligned	• No definition of 'security breach' under s21(3) (although see s30(1)(a) for possible definition by extension)
Data protection impact assessments and prior consultation (Articles 35-36)	Substantially aligned	• Regulations need to be made under s74(3)(c) to specify categories of 'specified processing' for which an assessment will be required under s19 • No legislative requirement under s45 for the data controller to seek the views of data subjects when carrying out annual impact assessments
Data protection officers (Articles 37-39)	Partially aligned	• Data protection officers under s20 not required to be involved in a timely manner in all issues relating to the protection of personal data and to be given the required independence to perform his or her tasks • No requirement to be bound by secrecy and confidentiality concerning the performance of his or her tasks • No provision as to adequate resourcing of data protection officers to enable the performance of tasks
Codes of conduct and certification (Articles 40-43)	Substantially aligned	• Code of conducts only required for assessment notices (s47(6)) and data sharing (s57), although further guidelines can be prepared and disseminated as the Commissioner considers appropriate (s4(5)(c))
International transfers (Articles 44-49)	Substantially aligned	• International transfers can be made without ensuring an adequate level of protection for the rights and freedoms of data subjects where 'the transfer is necessary for reasons of substantial public interest' and for 'the purposes of national security or the prevention, detection or investigation of crime' (s31(4)(d) and (j)) • Minister may specify circumstances and extent to which transfers on these grounds can be made without ensuring an adequate level of protection after consultation with the Commissioner, but independent oversight and/or other safeguards not required (s31(3))
Supervision (Articles 51-60, 69)	Substantially aligned	• No requirement that the Data Protection Oversight Committee act independently when performing its tasks and exercising its powers
Cooperation and mutual assistance (Articles 50, 60-67)	Partially aligned	• Regulations to be made under s60 as to cooperation by the Commissioner with supervisory authorities in foreign States and exchange of information with such authorities • In the absence of regulations, there is no duty to cooperate or provide mutual assistance to other supervisory authorities
Remedies (Articles 77-84)	Partially aligned	• Commissioner not required to keep complainant informed on the progress and outcome of complaints within a specified period of time, including appeal rights • No right to compensation from data processors involved in breaches of the law or provisions dealing with the liability of data processors • No requirement that fines be effective, proportionate and dissuasive
Specific processing situations (Articles 23, 85-91)	Substantially aligned	• Limited oversight and safeguards for some exemptions under Part V • Ministerial power to make exemptions to non-disclosure provisions without consultation or independent oversight (s43(2))

Source: Prepared by the author.

2. Main findings

Based on the areas of non-alignment between the DPA 2020 and the GDPR identified above, this section sets out key areas for Jamaica to consider if seeking to strengthen its legislation:

Definitions of 'personal data', 'sensitive personal data' and 'process'

The DPA's definition of personal data includes 'any expression of opinion about that individual and any indication of the intentions of the data controller or any other person in respect of that individual'. This oft-criticised distinction between statements of opinion and statements of the data controller's intentions featured in the United Kingdom's Data Protection Acts of 1984 and 1998,[71] but was removed from the GDPR-aligned Data Protection Act 2018. The distinction is unnecessary as both forms of statement would qualify as 'information relating to a living individual' provided they enable the identification of the individual in question, and they could also promote undue focus on journalists' work. Another point of difference between the two instruments is that the DPA 2020 applies to information relating to individuals deceased for less than 30 years, while the GDPR only applies to information which relates to an identifiable living individual.[72]

Other definitions in the DPA 2020 could also be amended to further alignment with the GDPR. The definition of 'sensitive personal data' excludes personal data relating to sexual orientation as a category of highly sensitive data that is subject to more stringent conditions and safeguards. The category of 'sex life' is included, but carries a different meaning to 'sexual orientation'. For example, while a child may identify as having the sexual orientation of bisexual, sex life is a term generally only used in relation to persons above the age of consent.

'Process' means 'in relation to *information* or *personal data* ... obtaining, recording or storing the information or personal data, or carrying out any operation or set of operations (whether or not by automated means) on the information or data' [emphasis added]. The rationale for incorporating both the terms 'information' and 'personal data' is unclear when the DPA's aim is to strengthen the protection of personal data. There is likely no material difference between the two terms and therefore including them alongside each other could produce confusion.[73]

Consent of data subjects

Under section 9 of the DPA, consent is defined as 'any informed, specific, unequivocal, freely given, expression of will by which the data subject agrees to the processing of that data subject's personal data'. While it is clear that data subjects should express their will in an unequivocal manner to establish consent, it is not mentioned how data controllers should present a request for consent to data subjects (i.e. in an intelligible and easily accessible form, using clear and plain language as under the GDPR). In the case of sensitive personal data, processing must be consented to in writing and presumably requested in the same manner (s24(1)(a).

Processing of personal data relating to criminal convictions

The DPA classifies the alleged commission of any offence by the data subject or any proceedings for any offence alleged to have been committed by the data subject as 'sensitive personal data', excluding data relating to criminal convictions. This is similar to the GDPR's approach of dealing with personal data relating to criminal convictions and offences separately under Article 10. However, the DPA differs from the GDPR in that data controllers processing personal data relating to criminal convictions need not possess legal or official authority to undertake this form of processing (although they must appoint a data protection officer under section 20 of the DPA).

---

[71] See I.J. Lloyd, Information technology Law (2011, 6th ed.), Oxford University Press, p.40.

[72] GDPR, Recital 27.

[73] See K. McCullagh, 'Protecting 'privacy' through control of 'personal' data processing: A flawed approach', (2009) International Review of Law, Computers & Technology, 23:1-2, p. 48.

While the conditions in section 23 of the DPA limit the circumstances in which data controllers can process personal data relating criminal convictions, it would add a further layer of protection to require legal or official authority for such processing. There are limited circumstances in which it is appropriate for processing of personal data relating to criminal convictions to take place without legal or official authority, such as for employment criminal record checks, which could be accommodated with a specific carve-out.

Individual rights

The DPA 2020 affords data subjects a range of individual rights, including the right to be informed and access personal data, the right to prevent processing, the right to rectification of inaccuracies, and rights in relation to direct marketing and automated decision-making. However, it does not include a general right to erasure. While section 11 grants data subjects the right to require data controllers to cease processing "in a specified manner" and it is possible that data subjects could interpret this to request erasure of their personal data, it would strengthen data subjects' rights to set this out explicitly in the legislation.

The right to erasure, also known as the right to be forgotten, is a centrepiece of the GDPR. It allows data subjects to demand that data concerning them be deleted under a number of specific circumstances, such as where the data subject objects to processing based on legitimate interests and the controller cannot demonstrate overriding legitimate grounds. Data controllers are not required to fulfil erasure requests in certain situations, including where necessary to protect the right to freedom of expression and information. This aims to prevent individuals from using the right to hide factual but embarrassing information about them legitimately in the public domain. The right to erasure is also important to give meaning to other data protection rights. For example, the right to withdraw consent to data processing loses impact if not accompanied by an explicit right to erasure of the data in question.

There is also no requirement under the DPA 2020 that data controllers inform data subjects about their rights (although it should be noted that the Commissioner is required to disseminate information about the Act (s4(5)(d)). Given the general public's unfamiliarity with data protection rights and the power imbalance that often exists between data subjects, data processing technologies and data controllers, data controllers should be obliged to inform data subjects of their rights in particular circumstances, such as where they are responding to a data access request or requesting a data subject's consent. This would relieve individuals of the onus to make themselves aware of their data protection rights, and share the burden on the Information Commissioner to inform the public about the Act.

Furthermore, the Minister has the power to make further exemptions to certain rights conferred in Part II under section 43. This power is subject to a limitation clause that it can only be exercised where 'the Minister considers it necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other individual'. However, the Minister is only required to consult with the Commissioner where considering an exemption to the disclosure to data subject requirements and not where it relates to the non-disclosure provisions.[74]

At a minimum, ministerial powers to alter the application of the Act's protections should be subject to judicial or parliamentary scrutiny, for example, a statutory instrument subject to affirmative resolution. This will encourage Ministers to approach their powers conservatively, including by conducting a thorough balancing act between data protection rights and other interests demanding

[74] Section 2 of the DPB states that the non-disclosure provisions are, to the extent to which they prohibit the disclosure in question, the first data protection standard, except to the extent to which disclosure is required for compliance with the conditions set out in sections 23 and 24; the second, third, fourth and fifth data protection standards; and sections 11 and 13(3) and (4).

their restriction. Finally, a fee is also payable for the right of access to personal data under section 6(2)(c), raising the question of whether an individual should pay to exercise an individual right.

Obligations of data controllers and processors

The DPA 2020 imposes several obligations on data controllers, including a prohibition on processing without registration under section 15. Among other particulars, data controllers must provide the Commissioner with a description of the personal data being, or to be, processed by or on behalf of the controller, the categories of data subjects to which this personal data relates, and the purposes for which the personal data are being, or are to be, processed (s14-18).

Journalists are subject to the registration requirements without any carve-out to protect the identity of confidential sources. Since there is potential for overlap between confidential sources and the categories of data subjects to which personal data relates, consideration should be given to exempting journalists from registration requirements or limiting the specificity of the particulars that they are expected to provide by order under section 15(2). A balancing of the DPA's registration requirements with freedom of expression and information is important to prevent self-censorship by journalists and revelation of sources.[75]

Furthermore, data controllers are required under the Seventh Standard to put appropriate technical and organisational measures in place to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. However, in the case of data processors, the onus is on the data controller to provide sufficient guarantees in respect of the processor's technical and organisational security measures (section 30(4)). This approach places a heavy burden on data controllers, especially small undertakings, by requiring them to monitor their own data processing activities in addition to those of processors they engage. While it is appropriate for data controllers to carry a heavier burden than processors, the GDPR spreads this burden by directly imposing enforceable obligations on data processors and making compliance a shared duty. Data processors are also not required to maintain a record of processing activities (although data controllers are required to register a description of data processed on their behalf under section 16(2)(d)).

Mechanisms to ensure appropriate technical and organisational security measures

The DPA 2020 contains several mechanisms to ensure that data controllers implement the data protection standards and safeguard individual rights, including data protection officers (s20), prior consultation for 'specified processing' (s19), assessments of good practice (s4(8)), annual data protection impact assessments (DPIAs) (s45), and codes of practice and guidelines in certain areas.

Some fine-tuning of the DPA could, however, be undertaken to increase the effectiveness of these mechanisms. There is no requirement under section 45 for data controllers carrying out their annual DPIAs to consult data subjects on the risks to their rights and freedoms, where appropriate. Under Article 35(9) of the GDPR, data controllers are required to seek the views of data subjects when performing DPIAs, provided this does not prejudice commercial or public interests or the security of processing operations. Furthermore, data protection officers should also be required to be involved in a timely manner in all issues relating to the protection of personal data, bound by secrecy and confidentiality and given the required independence to perform their tasks. The DPA also makes no provision for the adequate resourcing of data protection officers to enable the effective performance of their tasks.

---

[75] See J Posetti, 'Protecting Journalism Sources in the Digital Age', <http://www.unesco.org/new/fileadmin/ MULTIMEDIA/ HQ/CI/CI/ pdf/protecting_journalism_sources_in_digital_age.pdf?>.

Moreover, regulations need to be made under section 74(3)(c) to specify categories of 'specified processing' for which an assessment will be required under section 19. These regulations should incorporate all the categories of personal data for which DPIAs are required under the GDPR, including when using new technologies, when there is a high risk to the rights and freedoms of natural persons taking into account the nature, scope, context and purposes of the processing, when processing sensitive categories of data on a large scale, including relating to criminal convictions and offences, and when conducting systematic and extensive evaluations of personal aspects of natural persons based on automated processing and profiling producing legal effects.

Cooperation and mutual assistance

Section 60 of the DPA states that 'the Minister may...make regulations as to co-operation by the Commissioner with authorities in foreign States exercising functions analogous to those of the Commissioner under this Act...and, in particular, as to the exchange of information with such authorities.' In addition to the possibility of making regulations, the DPA would be strengthened by including an obligation to cooperate with other supervisory authorities and provide mutual assistance in cases of cross-border personal data transfers. This would be especially important for the period before any regulations are brought into effect and would reinforce regulations thereafter.

Regulations made under section 60 should include modalities for both cooperation and mutual assistance, such as timelines for response to requests, the format in which requested information should be supplied, and the circumstances in which the Commissioner can refuse to comply with a request.

Remedies

The DPA does not contain a general right of complaint to the Information Commissioner but sets out specific rights to complaint in various sections. When data subjects make complaints pursuant to these sections, the Commissioner is not required to keep the complainant informed on the progress and outcome of the complaint within a specified period of time, including appeal rights. It would reinforce the remedies available to data subjects to set a time limit, for example, a response is required within three months under Article 78 of the GDPR.

Furthermore, under the DPA, an individual who suffers damage by reason of a contravention by a data controller of any of the DPA's requirements is entitled to compensation from the data controller for that damage. Given that the DPA does not impose any directly enforceable obligations on data processors, there is no corresponding right to compensation from data processors who have acted unlawfully or contrary to the controller's instructions. To further align the DPA with the GDPR, it could be considered imposing a limited set of enforceable obligations on data processors who act unlawfully or contrary to a data controller's instructions in addition to a right to compensation from the processor in these instances.

Individuals also have a right to compensation where they suffer distress as a result of a contravention of the DPA where the distress is suffered in conjunction with damage, and standalone where the contravention relates to the processing of personal data for the special purposes (namely, journalism, artistic and literary purposes). To avoid a chilling effect on public interest journalism and to ensure a balance between privacy rights and freedom of expression, it would be useful to set out the factors that the court should take into account when deciding whether to award compensation in proceedings relating to data processing for special purposes and the amount in each individual case.

Broad exemptions and powers to make exemptions without consultation or independent oversight

The DPA contains some broad exceptions and exemptions not subject to independent oversight or only subject to oversight where a directly affected person appeals to a court. As an example of the latter, the Minister may issue a certificate under section 33 exempting personal data from the data

protection standards and the Act's other substantive requirements for the purpose of safeguarding national security. There is no judicial or other form of independent oversight of such certificates unless a person directly affected by the issuing of a certificate appeals to a Court (s33(4)). Since the Minister does not appear to be required to publish or otherwise make such certificates available to the public, it is unclear how directly affected persons would become aware of them.

Furthermore, as mentioned above, the DPA also contains a ministerial power to make additional exemptions to the non-disclosure provisions for disclosures of personal data where the Minister considers that the exemption is 'necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other individual' (s43(2)). While the latter limitation restricts the scope of the Minister's power and necessitates a balancing exercise, the power can be exercised without consultation with the Commissioner or judicial or parliamentary oversight.

Data sharing

The DPA notably requires the Commissioner to prepare and submit to the Minister a data-sharing code, recognising the importance of enabling public and private sector entities to share personal data while safeguarding privacy rights. Section 57 states that the code should contain practical guidance on the sharing of personal data in accordance with the requirements of the Act and such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data.

Data sharing is, however, allowed under the DPA with few safeguards or protections in certain cases. Under section 31(4)(d) and (j), international transfers of personal data can take place without ensuring that a State or territory provides an adequate level of protection for the rights and freedoms of data subjects 'where the transfer is necessary for reasons of substantial public interest' and 'for the purposes of national security or the prevention, detection or investigation of crime.' The Minister may prescribe by order subject to affirmative resolution the circumstances in which a transfer is necessary for reasons of substantial public interest (s31(5)). However, the Minister also has the power under section 31(3) to specify the circumstances and extent to which transfers on other grounds can be made without ensuring an adequate level of protection after consultation with the Commissioner. The exercise of this latter power is not subject to judicial or parliamentary scrutiny.

3. Summary of recommendations

In addition to the more exhaustive areas for strengthening identified in Table 9 above, the following recommendations are highlighted for enhancing the protection of personal data pursuant to the DPA 2020:

- Amend definitions of 'personal data', 'sensitive personal data' and 'process' to further align the same with the GDPR;
- Refine the notion of consent to specify how data controllers should present requests for consent;
- Require a legal or official authority for the processing of personal data related to criminal convictions;
- Introduce an explicit principle of accountability of data controllers requiring them to demonstrate compliance with the data protection standards in Part IV;
- Require data controllers to inform data subjects about their rights and introduce an explicit right to erasure of personal data;
- Limit the registration particulars that journalists are expected to provide under section 15 in order to protect confidential sources and other press freedoms;

- Impose a limited set of enforceable obligations on data processors, such as requiring them to directly provide sufficient guarantees in respect of their technical and organisational security measures and to maintain a record of processing activities;
- Enhance the mechanisms by which data controllers can proactively identify, assess and mitigate risks to personal data by, inter alia, requiring the adequate resourcing and active involvement of data protection officers in all issues relating to the protection of personal data;
- Introduce an obligation in the DPA to cooperate with other supervisory authorities and provide mutual assistance in cases of cross-border personal data transfers in addition to making regulations in these areas under section 60;
- Enhance the remedies available to data subjects under the DPA by requiring the Commissioner to inform complainants of the outcome of complaints within a specified period, providing a right of compensation from data processors in limited circumstances, and introducing guidance on awards of compensation for damage and distress; and
- Require independent oversight of exercise of exemptions and exceptions to the DPA's application as well as ministerial powers to make further exemptions.

III. Recommendations

Drawing on the review of data protection legislation of Antigua and Barbuda, the Bahamas, Barbados, Belize, Cayman Islands and Jamaica in Part II of this study, this section provides recommendations for countries across the Caribbean wishing to adopt or strengthen their data protection legislative and regulatory frameworks to safeguard individual privacy rights and personal data while creating an enabling environment for data sharing and e-government in the subregion.

A. Align national data protection legislation with the GDPR in order to guarantee privacy rights, support e-government and facilitate cross-border data flows and sharing

As a result of its extraterritorial scope and influence beyond European borders, the GDPR is expected to have a global impact and contribute to the harmonisation of data protection legislation around the world.[76] As one commentator has noted, "the only real way to avoid complying with the GDPR will be to avoid doing business with the EU entirely. Given that the EU is the largest trading bloc in the world, this would be impractical for any organisation that wants to take advantage of the Internet or works with modern global markets and supply chains."[77]

As set out in more detail in Part I, there are three main ways for Caribbean countries to facilitate GDPR-compliant data flows with EU entities. These are:

- Seeking a decision from the European Commission that the country in question offers a level of data protection that is essentially equivalent to that within the EU, known as an 'adequacy decision';
- Making transfers of personal data subject to 'appropriate safeguards' as outlined in Article 46(2)-(3) of the GDPR; and

[76] 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.

[77] ITGP Privacy Team, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide, IT Governance Ltd, 2017.

- Relying on an exception in Article 49 of the GDPR, such as where the data controller has the data subject's explicit consent or a transfer is necessary for performance of a contract with a data subject.

Adequacy decisions provide a clear, general authority for safe transfers of personal data from the EU to a third country, whereas transfers subject to appropriate safeguards and exceptions carry the administrative burden of having to guarantee sufficient protections on a case-by-case basis and, in some cases, consult with or seek approval from a supervisory authority. Given the added complexities of making cross-border data transfers absent an adequacy decision, several countries beyond the EU have consequently begun adopting similar, if not almost identical, regimes for data protection. According to one count, nearly 120 countries have already adopted GDPR-aligned data protection laws.[78]

In August 2018, Brazil enacted a data protection law, known as Lei Geral de Proteção de Dados (LGPD). Modelled on the GDPR, the LGPD provides Brazilian data subjects with more control over their personal information, has extraterritorial scope and applies to the government, private sector and individuals. Similarly, Japan amended its Act on the Protection of Personal Information 2015 to bring it in line with the GDPR. Caribbean countries have also been part of the trend to adopt GDPR-style data protection regimes. In 2016, Bermuda passed the Personal Information Protection Act, which includes many of the stringent conditions and protections of the EU regulation, while Barbados is in the process of implementing its Data Protection Act 2019 as reviewed in Part II of this study.

Given that Caribbean economies are highly reliant on tourism and external trade, including with EU individuals and companies, becoming GDPR compliant will be advantageous, if not essential, for both Caribbean public and private sector organizations. Private sector organisations can avoid the GDPR's stringent fines and gain competitive advantage by aligning their data protection and sharing regimes with the GDPR's privacy principles and accountability measures. Adopting GDPR-aligned laws can also facilitate data flows and trade with non-EU countries, since the GDPR is gaining recognition as international best practice and other countries are putting modern, robust data protection framework in place based on it.

Small and medium-sized enterprises (SMEs) may find it challenging to upgrade their systems and processes in order to maintain compliance with GDPR-style laws. Under the GDPR, small businesses are exempt from certain requirements, such as the obligation to have a Data Protection Officer. Some Caribbean countries follow this approach with, for example, Barbados' Data Protection Act 2019 only requiring a data privacy officer to be appointed in limited circumstances.[79] However, to achieve alignment with the GDPR, Caribbean data protection laws should require all organisations processing personal data, regardless of their size, to meet the basic content and procedural data protection principles and mechanisms set out in the GRPR.[80] This includes processes and policies to secure data, taking into account the nature, scope, context and purposes of the data processing. While there will be associated time and resource use, these efforts will enable small Caribbean businesses to avoid fines and other compliance penalties under local and EU data protection standards and to engage in e-commerce and digital trade beyond local markets.

Implementing data protection legislation modelled on the GDPR across the subregion can also help to create an enabling environment for data sharing and e-government between Caribbean countries, leading to regional economic growth and harmonized privacy protections for individuals. The COVID-19 pandemic has highlighted the importance of countries embracing digital technologies,

---

[78] A. Bradford, The Brussels Effect: How the European Union rules the World (2020) Oxford University Press, p. 148.

[79] Barbados' Data Protection Act 2019, section 67.

[80] For the basic content and procedural principles of the GDPR, see the Adequacy Referential document adopted by the European Data Protection Board (EDPB) referred to below.

implementing e-government solutions, and sharing data across borders. However, it is essential that e-government and data sharing go hand in hand with robust data protection and information security standards and practices, as they work in tandem to ensure public trust in online services and the protection of personal data. Furthermore, there is a need to strengthen the policy and technical capabilities of Caribbean governments in order to make e-government effective.

In the short- and medium-terms, Caribbean countries will need to rely on 'appropriate safeguards' or the exceptions set out in the GDPR to facilitate transfers of data to and from EU countries, since the European Commission has so far only issued 13 adequacy decisions.[81] However, putting in place data protection legislation that incorporates as many of the GDPR's safeguards and protections as possible would facilitate an eventual application to the European Commission for an adequacy decision. As highlighted above, it would also increase options for Caribbean organisations wishing to facilitate data flows and trade with non-EU countries outside the subregion. While applying for an adequacy decision can be a lengthy and complicated process, it should be noted that the European Commission has already adopted adequacy decisions in respect of some small island territories, including the Faroe Islands, Guernsey, Isle of Man, and Jersey.

As the review of data protection legislation in Part I highlighted, there are a number of safeguards and protections that countries can incorporate in their legislation to further alignment with the GDPR. Some points likely to be considered essential by the European Commission in the assessment of the level of data protection in a non-EU country include basic data protection concepts, grounds for lawful processing of personal data, principles of data protection, including lawfulness, fairness and transparency, data subjects' rights, appropriate technical and organizational measures to ensure data security, restrictions on international transfers, independent oversight with sufficient powers to ensure compliance with data protection standards, and the availability of effective remedies to data subjects.

Reference can be made to the 'Adequacy Referential' document of the Article 29 Working Party of EU data protection authorities for 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 in order to achieve essential equivalence with the EU framework.[82] Subsequently adopted by the European Data Protection Board (EDPB), this document sets out the basic content principles, additional content principles for special categories of data, procedural aspects and enforcement mechanisms, and guarantees on national security and law enforcement access that should be reflected in national laws.

As the Court of Justice of the European Union (CJEU) noted in *Schrems*, "the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union..."[83]. Revised legislation can also draw inspiration from approaches taken in other jurisdictions given that a number of non-EU countries have introduced legislation closely modelled on the GDPR and incorporating global best practice.

---

[81] See the list of countries and territories with adequacy decisions at footnote 26 above.

[82] The Adequacy Referential can be found at this link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

[83] CJEU, Case C 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015, paragraph 74.

B. Facilitate public and private sector information sharing through creating clear guidance and incentives for sharing

Data sharing can benefit individuals, government bodies, private organisations, and society as a whole. Within the private sector, data sharing is an enabler of growth, employment and innovation. When data is used collaboratively, it can address sectoral challenges and create new insights, technologies and problem-solving capabilities. The sharing of data in the public sector and between public and private bodies informs evidence-based policy making, leading to better-designed, cost-efficient public services that meet individuals' needs. Cross-government data sharing also reduces duplication, enables the sharing of best practice between public bodies and increases transparency and accountability to individuals. In the Caribbean, increased inter-regional data sharing can lead to regional economic growth by addressing data shortages and enabling region-wide solutions for common issues.

However, data sharing can run counter to the data protection principles that personal data should be collected directly from the individual to whom it pertains and used for the specific purposes for which it was collected. As a result, modern data protection laws often seek to create incentives or gateways for lawful data sharing through systems of authorisation of information sharing agreements or a requirement to publish guidance in the form of data-sharing codes. Systems for authorising agreements usually require some form of parliamentary or judicial oversight or, failing this, consultation with a data protection authority and affected data subjects to ensure the necessity and proportionality of the proposed sharing and a balancing of other considerations.

Data sharing is a type of 'processing' under most, if not all, data protection laws in the Caribbean. This is usually achieved through including a phrase in the definition of processing such as 'the disclosure of personal data by transmission, transfer, dissemination or otherwise making available.' While Caribbean data protection laws provide a number of gateways for data sharing, they rarely oblige or create incentives for the sharing of data. Instead they restrict whom data can be shared with and the circumstances within which this is permissible, including requiring data to only be shared when and to the extent necessary, with prior consultation and for the specific purposes for which it was collected. Failure to observe these requirements can result in monetary penalties and, in some serious cases, imprisonment.

This is one of the reasons why Caribbean governments report that data sharing often does not take place between public bodies even when they have the legal power to do so. In some cases, public bodies believe that they are prevented from data sharing because the law is unclear, difficult to interpret or found in a range of sources. In other cases, public bodies are hesitant to share data due to a lack of safeguards to protect privacy and ensure data security. Without data protection frameworks in place, many public bodies lack the technical and organisational measures necessary to secure data transfers. This results in fears of sanctions and reputational damage for unauthorised disclosures of information often compounded by inter-organisational distrust and incompatible ICT systems.

Beyond a clear, enabling legal framework, this highlights that improving data sharing between public and private bodies requires a comprehensive approach that addresses cultural and institutional barriers in addition to legal ones at both the domestic and regional levels. Policy guidance in the form of codes of practice and guidelines can support organisations to adopt an effective approach to data protection compliance by providing practical guidance that demystifies the requirements of the law and sets them out in a user-friendly manner. As an example of good practice in this area, 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.[84]

Caribbean governments also report that interoperability of ICT systems is a major determinant of successful data sharing for public bodies in the Caribbean. Interoperability refers to the ability of two or more ICT systems to interact and exchange data according to a defined method in order to obtain the expected results.[85] One component of interoperability is standards to enable secure access to public sector data and exchange of information or 'appropriate technical or organisational measures' using the language of the GDPR. At present, many government departments in the Caribbean operate in silos with different ICT systems and security measures in place preventing secure, seamless transfers of data. Governments should therefore consider developing cross-government strategies for the procurement of interoperable ICT systems, hardware and software. Cross-government information systems should integrate 'data protection by design' in order to foster greater integration, but also make the secure sharing of data a possibility.

Developing interoperable e-government tools and ICT systems can also support regional integration efforts. As the digital layer to the Caribbean Single Market Economy (CSME), CARICOM's Single ICT Space project encourages Member States to work towards regionally harmonized ICT policy, legal and regulatory regimes, robust national and regional broadband infrastructure, common frameworks for governments, ICT service providers and consumers, and effective, secure technology and management systems. Where Caribbean governments implement interoperable ICT and e-government architecture, this can support sector specific initiatives in the subregion as well as information sharing and other forms of regional cooperation on common issues in areas including disaster preparedness, trade, tourism, health, education, agriculture, environment and security.

Beyond interoperability, sharing of best practice and training of public service employees should also form part of a strategy to drive cultural and institutional change at the domestic and regional levels. Public service training on data sharing and use of new ICT systems can help to create a culture of innovation within government and grow awareness of the importance and benefits of data sharing in the context of e-government and CARICOM's Single ICT Space project.

C. Ensure data protection legislation adequately balances the right to privacy with press freedoms and freedom of expression

Personal information and human stories have been described as the 'raw material of journalism'.[86] Given the special role of journalism and the press in enabling the functioning of democratic societies, it is essential that the protection of information privacy does not compromise press freedoms. The rights to privacy and freedom of expression are mutually reinforcing but also potentially conflicting rights. On the one hand, the right to privacy allows individuals to confidently exercise their right to freedom of expression through, for example, remaining anonymous. On the other hand, publication of personal data can infringe the right to privacy.[87]

The GDPR seeks to manage the delicate balance between privacy and freedom of expression through a journalistic exemption, which requires Member States 'to reconcile the right to the protection of personal data...with the right to freedom of expression and information, including processing for

---

[84] See Jamaica's DPA 2020, section 57.

[85] Government of Trinidad and Tobago, National Information and Communication Technology Company Limited, 'Policy on e-Government Inter-Operability Framework', 4 February 2013.

[86] J. Glanville, 'The Journalistic Exemption', 40 London Rev. Books 9-10, 5 July 2018.

[87] Article 19, 'The "Right to be Forgotten": Remembering Freedom of Expression', 2016.

journalistic purposes and the purposes of academic, artistic or literary expression'.[88] Implementation of this exemption has been uneven, with only 16 out of 28 Member States having incorporated a journalistic exemption into their law at the time of this review.[89] The quality of protections also varies with Spain, for example, only mentioning freedom of expression in the preamble of its law.

Caribbean data protection legislation also differs in its approaches to balancing the rights to privacy and freedom of expression. As noted above, the Bahamas' Data Protection (Privacy of Personal Information) Act 2003 is silent on freedom of expression and journalistic activities, and does not create safeguards to limit the Data Protection Commissioner's powers in relation to journalistic activities. Laws created more recently tend to include an exemption for journalism, art and literature, but in some cases these exemptions are drafted narrowly and would still allow individuals to bring claims, including those aimed at stifling reporting, against journalists.

Several countries' legislation contains a complex definition of 'personal data' making a distinction between expressions of opinion and statements of the intentions of data controllers about an individual.[90] These definitions are out of step with the GDPR's more straightforward definition of personal data and could generate an undue focus on journalistic activities.[91] Under one piece of Caribbean legislation, journalists are required to register with an Information Commissioner before processing personal data, which would oblige them to give a description of the personal data they hold, the categories of data subjects to which it relates and the purposes for which they are using this data. The right of confidentiality for journalists' source is an important press freedom, which safeguards the public's right to information and is necessary for the functioning of a democratic society. Therefore, data protection legislation should ensure that journalists are exempt from any requirement that could potentially threaten the confidentiality of sources. This includes limiting the specificity of registration particulars to be provided where revealing categories of data subjects could lead to the identification of journalists' sources.

Human rights advocates have expressed concern about the implications of some of the GDPR's individual rights for freedom of expression, including the right to erasure. Also known as the right to be forgotten, this right allows data subjects to demand that data concerning them be deleted under a number of specific circumstances. However, data controllers are not required to fulfil requests where necessary to protect the right to freedom of expression and information. This is meant to prevent individuals from hiding information about them legitimately in the public domain. The right has been keenly embraced, with Google recording almost 3.7 million requests to have URLs delisted since 2014 and actually delisting 53.6 per cent of URLs pursuant to those requests.[92]

When adopting individual data protection rights with freedom of expression implications, countries should ensure that the law provides adequate safeguards to prevent a chilling effect on free expression and any impediments on legitimate public interest journalism. In particular, data controllers and subjects should have access to an independent adjudicatory body to weigh the balance between the two rights. Furthermore, where there is an overriding interest that information remains in the public sphere, legislation should offer a 'public interest' exception or similar accompanied by appeal rights.

---

88 GDPR, Article 85.

89 Bird and Bird, 'GDPR Tracker: Personal data and freedom of expression', https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression.

90 See analysis of Jamaica's Data Protection Act 2020 and the Cayman Islands' Data Protection Law 2017 in Part II of this study.

91 The GDPR defines personal data as 'any information relating to an identified or identifiable natural person ('data subject')' (Art. 4).

92 Google, 'Transparency Report: Requests to delist content under European privacy law', https://transparencyreport.google.com/eu-privacy/overview?hl=en.

D. Enable effective domestic and cross-border enforcement of Caribbean data protection laws through cooperation and adequate resourcing of supervisory authorities

In this era of digital globalisation, cross-border data processing is commonplace, facilitated by the borderless nature of the internet and data processing technologies. The growth in international data flows has necessitated cooperation in privacy law enforcement as well as enhanced sharing of information between data protection authorities across the world. As early as 1980, OECD Member States agreed to facilitate cross-border privacy law enforcement co-operation, promote interoperability among privacy frameworks, and develop internationally comparable metrics for transborder flows of personal data.[93]

The GDPR requires Member States' supervisory authorities to cooperate with each other and provide mutual assistance in cases of cross-border personal data transfers. Mutual assistance includes the provision of information and 'any other measures for effective cooperation'. Under Article 50, the European Commission and EU supervisory authorities are also required to adopt international cooperation and mutual assistance mechanisms with third countries and international organisations. As EU Member States begin to examine possible international cooperation mechanisms, Caribbean countries should include provisions in their laws to facilitate involvement in eventual cooperation and mutual assistance frameworks.

Several new or draft Caribbean data protection laws include cooperation provisions, including the Cayman Islands' Data Protection Law 2017 and Jamaica's Data Protection Act 2020 both reviewed in this study. However, these laws do not require authorities to engage in mutual assistance or flesh out its modalities, including timelines for response, the format in which requested information should be supplied, and the circumstances in which an authority can refuse to comply with a request.

In the meantime, there are a number of international and regional forums on data protection that Caribbean countries can participate in to build capacity and exchange knowledge with other supervisory authorities, including the Global Privacy Assembly (formerly, the International Conference of Data Protection and Privacy Commissioners), the Global Privacy Enforcement Network, the Ibero-American Data Protection Network, and the Common Thread Network (CTN) for data protection and privacy authorities of Commonwealth countries.[94] The CTN promotes cross-border cooperation and sharing of knowledge on emerging trends, regulatory changes and best practices for effective data protection.

Another aspect of the cross-border enforcement discussion is extraterritoriality. The GDPR limits its extraterritorial effect to non-EU controllers and processors targeting EU data subjects, thereby attempting to avoid overreach. Although there is a global trend for data protection laws to be given extraterritorial jurisdiction, Caribbean legislators have so far only enacted a few laws with effect beyond national borders. As set out in Part II of this study, Barbados' Data Protection Act 2019 and Jamaica's Data Protection Act 2020 both apply to data controllers not established in Barbados and Jamaica where they process personal data of individuals in those countries in some circumstances.

Enforcement of extraterritorial data protection legislation provides a challenge, particularly for states with small data protection authorities and limited investigative capacity. On one view, it is important to give data protection laws extraterritorial effect for symbolic effect and to deter illegal processing by foreign organisations. Others argue that only a real risk of enforceable sanctions will have

---

[93] OECD, Guidelines covering the Protection of Privacy and Transborder Flows of Personal Data, adopted 23 September 1980.

[94] For more information on the Common Thread Network (CTN), see https://www.commonthreadnetwork.org/.

any influence on foreign data controllers.[95] As discussed above in relation to Antigua and Barbuda, one intermediate option would be to give data protection laws extraterritorial effect only for a small subset of rules.[96] This could go some way to mitigating the challenges of enforcing extraterritorial claims. In any case, the territorial scope of laws should be made clear in order to provide legal certainty to data controllers, processors and subjects.

Giving Caribbean data protection laws extraterritorial effect and requiring authorities to cooperate and provide mutual assistance would contribute to strengthening the enforcement of privacy protections in the subregion and with EU countries and support the harmonisation of data protection standards across the subregion. Importantly, it would also make it more difficult for non-compliant data controllers to move data processing operations to Caribbean countries and territories with lesser privacy protections to avoid having to comply with stringent protections – a practice known as forum shopping. At the European level, there have been some promising examples of cooperation efforts between supervisory authorities with, for example, the French supervisory authority working in concert with its European counterparts to impose a €50 million fine on Google in 2019.[97]

However, as the experience of implementing the GDPR has shown, providing data protection authorities with extraterritorial powers and the ability to cooperate is likely to be insufficient. For the most part, European cross-border privacy enforcement is still in its infancy.[98] Academics have argued that a legally binding requirement to cooperate is necessary to effectively enforce data protection law, but adequate resourcing is more determinative of a willingness to cooperate.[99] Caribbean data protection authorities should therefore be adequately staffed and resourced on a fixed, ongoing basis in order to enable both domestic and cross-border enforcement in a robust, timely manner. This is a challenge for the Caribbean public sector with its high levels of indebtedness and inability to service debts, a situation which has been exacerbated by the COVID-19 pandemic.

Since the GDPR came into effect, European supervisory authorities have been slow to cooperate and issue enforcement actions against global technology companies. While France's data protection authority made history with its enforcement action against Google, other authorities have been accused of lagging behind. Ireland is the home of European headquarters for tech giants, including Facebook, Twitter, Google and Apple, but its supervisory authority has so far only issued its first draft decisions in May 2020.[100] A funding shortage has been cited as one reason for the Irish authority's delay in resolving complaints. In 2019, the authority had a budget of €15.3 million to deal with more than 7,000 complaints, almost 5,000 breach notifications and more than 40,000 requests for guidance from data controllers.

European authorities have also been hesitant to commence joint investigations and other forms of cooperation as a result of 'divergent national legal systems, cultural differences and an outmoded information exchange system'.[101] On the last point, it has been observed that authorities are ill-equipped to manage cross-border complaints due to outdated ICT systems and a lack of basic capabilities for sharing data.

---

95 B. Greze, 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives' (2019) International Data Privacy Law 9(2), pp. 109–128.

96 D. Svantesson, 'A "layered approach" to the extraterritoriality of data privacy laws' (2013) International Data Privacy Law 3, pp. 278-286.

97 Politico, '"We have a huge problem": European regulator despairs over lack of enforcement', 28 December 2019, https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs-over-lack-of-enforcement/.

98 B. Greze, 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives' (2019) International Data Privacy Law 9(2), p. 117.

99 Ibid.

100 Cnet, 'Twitter, WhatsApp in firing line as Ireland submits first draft GDPR decisions', 22 May 2020, https://www.cnet.com/news/twitter-and-whatsapp-in-firing-line-as-ireland-submits-first-draft-gdpr-decisions/.

101 Politico, '"We have a huge problem": European regulator despairs over lack of enforcement', 28 December 2019.

This highlights that strong enforcement of data protection laws in the Caribbean will not only require supervisory authorities to be empowered to cooperate but also to be given sufficient staff and budget to investigate complaints and issue timely sanctions in addition to interoperable ICT systems. Caribbean countries already have some experience funding ICT projects through sharing and joint procurement arrangements. Following this trend, Caribbean data protection authorities could agree to jointly procure and use interoperable software and ICT systems so as to efficiently share data and enable other forms of cooperation. Language differences between the Caribbean's English, Spanish, French and Dutch-speaking countries and territories will also need to be navigated in cross-border investigations.

E. Introduce independent oversight and safeguards to limit exercise of broad exemptions and exceptions to data protections

Recent large-scale data breaches involving national crime and security programmes, such as the Snowden Revelations discussed in Part I, have raised questions about the relevance and effectiveness of data protection frameworks from which matters of national security and crime are excluded. Government powers to access personal data in the context of national security and law enforcement have steadily increased since the terrorist attacks of 9/11. This increase in data access for surveillance purposes to fight terrorism and address other cross-border security issues has often gone hand in hand with the reduction or removal of oversight and consultation mechanisms as well as other safeguards to prevent against possible abuses.

Even before 9/11, there was a well-established tradition in data protection legislation to include exceptions to the application of data protection principles for national security and criminal investigation and enforcement.[102] The GDPR continues this tradition by allowing Member States to legislate restrictions to the rights and obligations contained in the regulation on the grounds of national security, the prevention, investigation, detection or prosecution of criminal offences and freedoms, and important public interests, among others. Any such restriction must be a necessary and proportionate measure in a democratic society.[103]

Similar exemptions can also be found in the majority of Caribbean data protection laws. In contrast to the GDPR, a balancing of the necessity and proportionality of the exercise of an exemption is usually not required by Caribbean legislation. Some laws in the subregion also allow broad exemptions to be exercised solely as a matter of ministerial discretion without independent oversight or review rights for affected data subjects. For example, the Bahamas' Data Protection (Privacy of Personal Information) Act 2003 provides for broad exclusions to the Act's protections for personal data 'that in the opinion of the Minister or the Minister for National Security are, or at any time were, kept for the purpose of safeguarding the security of the Bahamas' and 'pending civil, criminal or international legal assistance procedures'.

Other laws require ministers to apply for a certificate from the Governor in order to exercise the national security exemption, sometimes in consultation with a National Security Council.[104] However, in most cases, the Governor is not required to balance human rights considerations before issuing certificates and there is no system of oversight by an independent body. By contrast, Jamaica's Data Protection Act 2020 allows the minister responsible for national security to issue certificates after

[102] I. Lloyd, Information technology Law (2011, 6th ed.), Oxford University Press, p. 16.
[103] Article 23, GDPR.
[104] See e.g. the Cayman Islands' Data Protection Law 2017.

consultation with the minister responsible for technology. Persons directly affected by the issuing of a certificate can appeal to the Supreme Court, who may quash the certificate.[105]

Another concern is that ministers are sometimes permitted to use executive orders to make further exemptions without judicial or parliamentary scrutiny.[106] This means that ministers can alter or limit individuals' data protection rights without independent oversight. Given that new exemptions could run contrary to the legislative aims, they should be subject to judicial or parliamentary oversight or otherwise constitute an exhaustive list.

In order to guarantee the rights of data subjects and ensure that ministerial powers are exercised lawfully, transparently and fairly, four guarantees should apply when processing data for national security or law enforcement purposes: 1) processing should be based on clear, precise and accessible rules, 2) the data controller should demonstrate the necessity and proportionality of the processing based on legitimate objectives, 3) the processing should be subject to independent oversight, and 4) data subjects should have access to effective remedies.[107]

Caribbean data protection laws should incorporate these four guarantees, including a requirement to balance the necessity and proportionality of the exercise of an exemption or exception for national security or law enforcement purposes and a mechanism for prior independent oversight of such exercise. While intense scrutiny of national security or law enforcement decisions can in some circumstances compromise legitimate interests, independent oversight offers an important check on executive power and ensures respect for the rule of law. The principle of ministerial responsibility is respected because the minister retains the power to make executive orders and the oversight body can only block or legitimate the order.[108]

Ministers cannot provide independent oversight alone as they are part of the government. Rather, independence is best guaranteed with judicial or parliamentary scrutiny, the latter being possible in the form of a specialised committee or a ministerial order subject to affirmative resolution. Members of an oversight body should be transparently appointed subject to established procedures and be given adequate powers and resources to ensure their effectiveness, including the power to issue binding decisions.[109] In the absence of judicial or parliamentary oversight, a requirement to consult with the head of the country's data protection authority can provide some measure of independence, provided the person in question is empowered to block the exercise of the power. Furthermore, any oversight mechanism should offer a complaint procedure to affected data subjects, even if the procedure is secret in order to protect national security interests.

The system should also guarantee that oversight takes place prior to the processing of personal data pursuant to the exercise of the exemption or exception. Furthermore, legislation should require exemptions to be exercised on a case-by-case basis consistent with the data minimisation principle that personal data should be adequate, relevant and limited to what is necessary for the purposes for which it was collected. This would prevent the issue of certificates allowing systematic collection in favour of targeted collection.

---

[105] See section 33(4)-(5) of the Jamaican Data Protection Act 2020.

[106] See e.g. Belize's Data Protection Bill 2014.

[107] See Article 29 Working Party of EU Data Protection Authorities, 'Adequacy Referential' as last revised and adopted on 6 February 2018.

[108] N., van Eijk, 'Standards for Independent Oversight: The European Perspective' in F. H. Cate and J. X. Dempsey, Bulk Collection: Systematic Government Access to Private-Sector Data (2017), Oxford University Press, p. 390.

[109] Ibid.

Bibliography

International and regional conventions and instruments

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, entry into force 3 September 1953.

European Union, Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, 18 December 2000 (2000/C 364/01), entry into force 1 December 2009.

European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) 2016/679, entry into force 25 May 2018.

Ibero-American Data Protection Network, 'Standards for Personal Data Protection for Ibero-American States', November 2016, (online) (date of reference: 26 June 2020) <https://iapp.org/media/pdf/resource_center/Ibero-Am_standards.pdf>

Organization of American States (OAS), American Convention on Human Rights, 'Pact of San Jose', Costa Rica, 22 November 1969, entry into force 18 July 1978.

Organisation for Economic Co-Operation and Development (OECD), Recommendation of the Council concerning Guidelines covering the Protection of Privacy and Transborder Flows of Personal Data, adopted 23 September 1980, C(80)58/Final.

UN General Assembly, International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, entry into force 23 March 1976.

UN General Assembly, Universal Declaration of Human Rights, adopted 10 December 1948, 217 A (III).

National legislation and regulations

Act on the Protection of Personal Information 2015 (Japan).

Data Availability and Transparency Bill (Australia).

Data Protection Act No. 10 of 2013 (Antigua and Barbuda).

Data Protection Act 2018 (United Kingdom).

Data Protection Act 2019 (Barbados).

Data Protection Bill 2014 (Belize).

Data Protection Bill 2020 (Jamaica).

Data Protection Law 2017 (Cayman Islands).

Data Protection (Privacy of Personal Information) Act 2003 Chapter 324A (The Bahamas).

Data Protection Regulations 2018 (Cayman Islands).

Freedom of Information law (2020 Revision) (Cayman Islands).
Health Information Privacy Code 1994 (New Zealand).
Lei Geral de Proteção de Dados (LGPD) 2018 (Brazil).
Personal Information Protection Act 2016 (Bermuda).
Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c 5 (Canada).
Privacy Act, R.S.C. 1985, c P-21 (Canada).
Privacy Act 1993 (New Zealand).
Public Sector (Data Sharing) Act 2016 (South Australia).

Regional case law

Court of Justice of the European Union (CJEU), Case C 362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015.
____Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, EU:C:2020:559, 16 July 2020.
European Court of Human Rights (ECtHR), *Case of Benedik v. Slovenia* (App. 62357/14), 24 April 2018.
____*Case of Catt v. The UK* (App. No. 43514/15), 24 January 2019.
____*Case of S and Marper v. The UK (*App. Nos. 30562/04 and 30566/04),
____*Case of M.S. v Sweden* (App. Nos. 20837/92), 27 August 1997.
____*Case of Big Brother Watch and Others v. the United Kingdom* (App. nos. 58170/13, 62322/14 and 24960/15) 13 September 2018 (Chamber judgment).
Inter-American Court of Human Rights, *Case of Escher v. Brazil* (2009).

Book, articles and other documents

Article 19, 'The "Right to be Forgotten": Remembering Freedom of Expression', 2016, (online) [date of reference: 29 May 2020] <https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf>
Article 29 Working Party of EU Data Protection Authorities, 'Adequacy Referential' as last revised and adopted on 6 February 2018, WP 254 rev.01, (online) [date of reference: 20 July 2020] < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108>
Bird and Bird, 'GDPR Tracker: Personal data and freedom of expression', (online) [date of reference: 29 May 2020] <https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression>
Bradford, A., *The Brussels Effect: How the European Union rules the World*, 2020, Oxford University Press.
Caribbean Telecommunications Union (CTU) (2017), 'Vision and Roadmap for a CARICOM Single ICT Space', (online) [date of reference: 28 May 2020] <https://caricom.org/documents/15510- vision_and_roadmap_for_a_single_ict_space_-_final_version_updated.pdf>
Cate, F. H., and Dempsey, J. X., *Bulk Collection: Systematic Government Access to Private-Sector Data* (2017), Oxford University Press.
Cate, F. H., and Mayer-Schönberger, V., 'Notice and consent in a world of Big Data', *International Data Privacy Law,* Volume 3, Issue 2, May 2013, pp 67–73.
Cnet, 'Twitter, WhatsApp in firing line as Ireland submits first draft GDPR decisions', 22 May 2020, (online) [date of reference: 29 May 2020] <https://www.cnet.com/news/twitter-and-whatsapp-in-firing-line-as-ireland-submits-first-draft-gdpr-decisions/>
Cayman Compass, 'Technological and social challenges complicate remote learning', 11 June 2020, (online) [date of reference: 22 June 2020] <https://www.caymancompass.com/2020/06/11/technological-and-social-challenges-complicate-remote-learning/>
Davies, S., 'The Data Protection Regulation: A Triumph of Pragmatism over Principle?' (2016) *European Data Protection Law Review* 2(3), pp. 290-296
ECLAC (2016), 'Regional approaches to e-government initiatives in the Caribbean', Studies and Perspectives Series 47 (LC/CAR/L.483). Port of Spain.
Glanville, J., 'The Journalistic Exemption', 40 *London Rev. Books* 9-10, 5 July 2018.

Global Voices, 'Netflix's 'The Great Hack' highlights Cambridge Analytica's role in Trinidad & Tobago elections', 5 August 2019, (online) [date of reference: 16 June 2020] <https://globalvoices.org/2019/08/05/netflixs-the-great-hack-highlights-cambridge-analyticas-role-in-trinidad-tobago-elections/>

Global Witness, 'COVID-19 tracing apps must not interfere with human rights', 14 May 2020, (online) [date of reference: 28 May 2020] www.globalwitness.org/en/campaigns/covid-19-tracing-apps-must-not-interfere-human-rights.

Google, 'Transparency Report: Requests to delist content under European privacy law', (online) [date of reference: 29 May 2020] <https://transparencyreport.google.com/eu-privacy/overview?hl=en>

Government of Trinidad and Tobago, Hansard transcript of parliamentary proceedings in the House of Representatives, 28 March 2018, (online) [date of reference: 28 May 2020] http://www.ttparliament.org/hansards/hh20180328.pdf>.

____National Information and Communication Technology Company Limited, 'Policy on e-Government Inter-Operability Framework', 4 February 2013.

Greze, B., 'The extra-territorial enforcement of the GDPR: A genuine issue and the quest for alternatives,' *International Data Privacy Law* (2019) 9(2), pp. 109–128.

Herle, J., and Hirsch, J., 'The Peril and Potential of the GDPR' Centre for International Governance Innovation, 9 July 2019. (online) [date of reference: 28 May 2020] https://www.cigionline.org/articles/peril-and-potential-gdpr.

Human Rights Watch, 'The EU General Data Protection Regulation: Questions and Answers', 6 June 2018. (online) [date of reference: 28 May 2020] <https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation>.

ITGP Privacy Team, *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*, IT Governance Ltd, 2017.

Inter-American Development Bank (IDB) (2019), 'Wait No More: Citizens, Red Tape, and Digital Government', (online) [date of reference: 28 May 2020] <https://publications.iadb.org/en/wait-no-more-citizens-red-tape-and-digital-government-caribbean-edition>.

Kosseff, J., *Cybersecurity Law*, 2017, John Wiley & Sons, Incorporated.

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

Lexology, 'Better Compliance Through One Year of GDPR Enforcement', 26 July 2019 (online) [date of reference: 28 June 2020] <https://www.lexology.com/library/detail.aspx?g=7df2fcbd-cc6e-468b-bcfa-9119eaa9ad28>.

Lloyd, I.J., *Information technology Law* (2011, 6th ed.), Oxford University Press.

McCullagh, K., 'Protecting 'privacy' through control of 'personal' data processing: A flawed approach', (2009) *International Review of Law, Computers & Technology*, 23:1-2.

McKinsey Global Institute, 'Digital Globalization: The New Era of Global Flows', March 2016, (online) [date of reference: 28 June 2020] <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>.

Microsoft, 'Microsoft will honor California's new privacy rights throughout the United States', 11 November 2019, (online) [date of reference: 18 June 2020] https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights/.

Office of the High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age', 3 August 2018, A/HRC/39/29.

Office of the Data Protection Commissioner of the Bahamas, A Guide for Data Controllers, (online) [date of reference: 28 May 2020] https://www.bahamas.gov.bs/wps/wcm/connect/d4ed9b45-f989-4a6d-a298-1ef5103a0eec/Data%2520controllers%2520guide.pdf.

Office of the Information Commissioner (United Kingdom), 'Update report into adtech and real time bidding', 20 June 2019.

Office of the Information Commissioner (United Kingdom), 'Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach', 9 July 2019.

Office of the Ombudsman (Cayman Islands), Guide for Data Controllers: Data Protection Law 2017, (online) [date of reference: 28 May 2020] https://ombudsman.ky/images/pdf/pol_guide/Data-Protection-Law-2017---Guide-for-Data-Controllers.pdf.

Politico, '"We have a huge problem": European regulator despairs over lack of enforcement', 28 December 2019, (online) [date of reference: 28 May 2020] https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs-over-lack-of-enforcement/.

Posetti, J., 'Protecting Journalism Sources in the Digital Age', UNESCO with funding from Sweden, (online) [date of reference: 11 August 2020] http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/protecting_journalism_sources_in_digital_age.pdf?.

Reventlow, N.J, 'Can the GDPR and Freedom of Expression coexist?' (2020) *American Journal of International Law* 114, pp. 31-34.

Rossi, A., 'How the Snowden Revelations Saved the EU General Data Protection Regulation', The International Spectator (2018) vol. 53(4), pp. 95-111.

Svantesson, D., 'A "layered approach" to the extraterritoriality of data privacy laws' (2013) *International Data Privacy Law* 3, pp. 278-286.

The Gleaner, 'Williams reports progress on Digital Jamaica Initiative', 24 January 2020, (online) [date of reference: 28 May 2020] http://jamaica-gleaner.com/article/business/20200124/williams-reports-progress-digital-jamaica-initiative.

UNCTAD, 'Data protection and privacy legislation worldwide', (online) [date of reference: 28 May 2020] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

United Kingdom, Digital, Culture, Media and Sport Committee of the House of Commons, Oral evidence: Fake News, HC 363, 27 March 2018, (online) [date of reference: 28 May 2020] <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/81022.pdf>.

Warren, S. W. and Brandeis, L., 'The Right to Privacy', 4 *Harvard Law Review* 193, 15 December 1890.

Wagner, J., 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) *International Data Privacy Law*, pp. 1-20.

Wilson, C.S., 'A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation', Speech at Future of Privacy Forum by Commissioner of US Federal Trade Commission (FTC), 6 February 2020.

Annex

Annex 1
Indicators used to assess alignment of legislation with GDPR

GDPR Articles	Alignment indicators
Article 2, 4 – Material scope and definitions	Does the law include a broad definition of personal data, including information that can indirectly identify a person and online identifiers and location data? Is the definition technologically neutral i.e does it apply to both automated and non-automated processing (filing systems)? Are the circumstances in which the law applies expansive enough to include automated decision-making and profiling? Does the law set out to whom it applies and contain clear definitions of those persons i.e. controllers and processors or equivalent? Does the law clearly define the circumstances and activities to which it applies i.e. broad definition of processing and profiling? Does it extend to data sharing? Does the law contain additional protections for special categories of sensitive data and define what constitutes 'sensitive data'? Does the definition of sensitive data include personal data revealing race, ethnic origin, political beliefs and opinions, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, sexual orientation, criminal convictions and offences? Does the law exempt certain activities from its application i.e. data processing for law enforcement, national security, purely for personal/household purposes, defence, public health and security, the protection of judicial independence and proceedings, breaches of ethics in regulated professions, the protection of the individual, or the rights and freedoms of others, or the enforcement of civil law matters?
Article 3 – Territorial scope	Is the territorial scope of the law clear? Does the law apply to personal data of nationals processed outside of the jurisdiction, including where a foreign organisation is offering nationals' goods or services or monitoring their behaviour?
Article 5 - Fundamental principles relating to processing	Does the law contain general principles to guide data use and collection pertaining to each of the principles set out in the GDPR, including the following or equivalent: • Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • Accuracy and updating • Storage limitation • Integrity and confidentiality – guaranteeing data security using appropriate technical or organisational measures • Accountability (of data controllers)? Does the law make the data controller responsible for ensuring compliance with these principles? Does the law make the data controller responsible for demonstrating compliance with these principles?
Article 6 – Lawfulness of processing	Does the law require certain conditions to be met for a processing of personal data to be lawful? Does the law require the data subject to provide consent to processing for specific purposes? Does the law provide for other conditions or exceptions absent consent in which the processing of personal data is lawful? Are these conditions or exceptions clear, reasonable and proportionate? Can the conditions or exceptions be overridden by the interests, rights or freedoms of the data subject, especially where the data subject is a child?
Articles 4, 7 and 8 - Consent	Does the law define consent, including requirements for it to be freely given, specific, informed and an unambiguous indication of the data subject's wishes? Does the definition of consent require a clear, affirmative action signifying agreement to the processing of personal data? Does the law specify how the request for consent should be presented i.e. in an intelligible and easily accessible form, using clear and plain language? Does the law allow consent to be withdrawn at any time and require the data subject to be informed of this right before giving consent? Does the law require it to be as easy to withdraw as to give consent? Does the law make special provisions for obtaining consent from children i.e. provide an age of consent not lower than 13 and procedure for gaining authority from person with parental responsibility for children under the age of consent? Do children receive the same privacy protections and rights as adults?
Article 9, 10 – Special categories of personal data	Does the law impose specific and stricter requirements concerning the processing of special categories of data i.e. information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, sexual orientation, criminal convictions and offences? Does the law require a legal or official authority for the processing of data relating to criminal convictions and offences? Are the requirements or conditions for processing of sensitive personal data same or similar to those set out in the GDPR?
Articles 12-23 – Individual rights	Does the law guarantee rights of the individual, including: • The right to be informed about the collection and use of their personal data • The right to access personal data • The right to have inaccurate or incomplete personal data rectified and to receive notification thereof

GDPR Articles	Alignment indicators
	• The right to have personal data erased and to receive notification thereof • The right to request restriction or suppression of their personal data e.g. the ability to store but not use personal data • The right to obtain and reuse personal data across different services in a structured, machine-readable and commonly used format • The right to object to the processing of personal data in certain circumstances • Rights in relation to automated decision making and profiling, including the right not to be subject to solely automated decisions, including profiling, which have a legal or similarly significant effect Does the law set out the grounds, conditions and requirements for the exercise of each right? Under what circumstances, does the law allow these rights to be restricted e.g. where is it necessary to safeguard national security, defence or public security in a democratic society? Is the data controller required to inform data subjects about their rights? Does the law set out how to make a valid request to exercise each right and the time periods for response and compliance with the request? Does the law set out circumstances in which the data processor or controller can refuse to comply with such a request e.g. if it is manifestly unfounded, repetitive or excessive? Does the law set out whether a fee can be charged for processing the data request and set limitations on the amount of the fee?
Article 24, 25, 30, 32 – Obligations of data controllers	Does the law require the data controller to implement appropriate technical and organisational measures in order to integrate necessary safeguards to ensure compliance with the law, safeguard individual rights and implement data protection principles e.g. pseudonymisation? Does the law require these measures to ensure a level of security appropriate to the risk? Does the law require the above measures to be reviewed and updated where necessary? Does the law make provision for a code of conduct or certification mechanism to demonstrate compliance with this obligation? Does the law require data controllers to maintain a record of processing activities under its responsibility and stipulate what the records should contain?
Article 28, 30, 32 – Obligations of data processors	Does the law require the data processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk? Does the law require data controllers to only use data processors who provide sufficient guarantees to implement appropriate technical and organisational measures to comply with the law? Does the law require processing of personal data to be governed by a contract between the data controller and processor and set out what the contract should stipulate, including requiring the processor to take appropriate measures to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the GDPR? Does the law require the data processor to obtain the authorisation of the controller to engage another processor? Does the law provide for an approved code of conduct or certification mechanism by which a processor may demonstrate sufficient guarantees of appropriate technical and organisational measures? Does the law require data processors to maintain a record of processing activities carried out on behalf of a controller and stipulate what the records should contain?
Article 33 and 34 – Data breach notifications	Does the law define a personal data breach and include in this definition both accidental and deliberate causes? Does the law require the data controller to record personal data breaches? Does the law require the data controller to report personal data breaches? Are exceptions to the duty to report clear, reasonable and proportionate e.g. the data breach is unlikely to impact the rights and freedoms of individuals? Does the law require the breach to be reported without undue delay and where feasible not later than a certain number of hours e.g. 72 hours? Does the law require the data processor to report personal data breaches to the data controller as soon as it becomes aware? Does the law require individuals to be notified of the breach where it is likely to result in a high risk to the rights and freedoms of those persons? Does failure to notify a personal data breach carry with it the possibility of a fine and/or use of other corrective powers?
Articles 35-36 – Data protection impact assessment and prior consultation	Does the law require the data controller to carry out data protection impact assessments in particular circumstances i.e. when using new technologies; when there is a high risk to the rights and freedoms of natural persons taking into account the nature, scope, context and purposes of the processing; when processing special categories of data on a large scale, including relating to criminal convictions and offences; and when conducting systematic and extensive evaluations of personal aspects of natural persons based on automated processing and profiling producing legal effects? Does the law stipulate what the impact assessment should contain and how the results should be reported? Does the law require the data controller to seek the views of potential data subjects, where feasible? Where the assessment indicates a high risk to personal data, does the law require prior consultation with and authorisation from a supervisory authority? Does the law impose penalties for failure to comply with this obligation?
Articles 37-39 – Data Protection Officers	Does the law require some organisations to appoint a data protection officer (DPO) i.e. public authorities, except courts acting in their judicial capacity; processing operations requiring regular and systematic monitoring of data subjects on a large scale; processing operations of special categories of data or data relating to criminal convictions and offences? Does the law set out the qualifications, tasks, responsibilities and resources of this person and require him or her to be bound by secrecy and confidentiality concerning the performance of his or her tasks?

GDPR Articles	Alignment indicators
	Does the law require the DPO to be involved in a timely manner in all issues relating to the protection of personal data and be given the required independence to perform his or her tasks? Does the law authorise the DPO to report to the highest level of management?
Articles 40-43 – Codes of conduct and certification	Does the law require the supervisory authority to draw up a code of conduct and specify what it should contain? Does the law encourage use of the code of conduct by all public and private bodies and organisations as a means of verifying and demonstrating compliance with the law and any accompanying regulations? Does the law set up a certification scheme whereby the supervisory authority is empowered to monitor compliance with the code of conduct and certify organisations as compliant with it? Does the law make certification voluntary? Does the law require certification to be renewed within a specified period of time?
Articles 44-49 – International transfers	Where transferring personal data to an organisation in another country or an international organisation, does the law require data controllers and processors to verify and demonstrate that the intended recipient of the data has adequate safeguards in place to ensure the same level of protection of individuals afforded by the law? Does the law specify how an organisation in another country or an international organisation can demonstrate that they have adequate safeguards in place, including: • Binding corporate rules conferring enforceable data protection rights on data subjects and establishing a complaint procedure in accordance with the law, • A legally binding data protection agreement with template transfer clauses as established by the first country's supervisory authority, • A legally binding data protection agreement reviewed and authorised by the first country's supervisory authority, • A certificate of compliance from the second country's supervisory authority demonstrating the organisation's compliance with an approved code of conduct and notified to the first country's supervisory authority, or • A decision of the first country's supervisory authority that the organisation has adequate safeguards in place ('adequacy decision')? Does the law contain institutional arrangements for organisations to apply to the supervisory authority for a decision on the adequacy of safeguards of an organisation in a second country? Does the law contain institutional arrangements for the supervisory authority to review and approve: 1) certificates of compliance from another supervisory authority; and 2) data protection agreements between national and foreign organisations? Does the law provide for any derogations from the prohibition on transfers of personal data outside of the country i.e. with an individual's informed consent, for the performance of a contract between the individual and the organisation? Does the law provide a complaint and enforcement procedure to deal with breaches of personal data by an organisation in another country or an international organisation?
Articles 51 to 60, 69 – Supervision	Does the law establish an independent public authority to be responsible for monitoring and supervising the application of the law and to protect the fundamental rights and freedoms of natural persons? Does the law require the authority to act independently and remain free from external influence, including refraining from taking external instructions? Does the law include clear rules for the selection, appointment, and dismissal of the head and members of the supervisory authority? Does the law specify the duties of the head and members of the supervisory authority? Does the law include provisions to deal with serious misconduct of members of the supervisory authority? Does the law establish the roles and responsibilities of the supervisory authority, including: • Drawing up and approving a code of conduct, • Certification of data controllers/processors, • Drafting standard contractual clauses, • Approving binding corporate rules, • Rendering adequacy decisions for cross-border personal data transfers, • Consulting with and authorising data controllers in relation to data protection impact assessments, • Recording infringements, • Annual reporting of activities, including a list of infringements and measures taken, and • Cooperation with other supervisory authorities and international organisations? Does the law set out the authority's investigative and corrective powers in relation to personal data breaches e.g. to order the provision of information, to carry out investigations, to notify alleged infringements of the law, to obtain access to all personal data, information, equipment and premises of the controller and processor, to adopt decisions, to issue warnings, reprimands and orders, to order a temporary or definitive limitation on processing, to order rectifications, to withdraw a certification, to impose administrative fines and the suspension of data flows? Does the law set out the authority's authorisation and advisory powers e.g. to consult with data controllers under a prior consultation procedure, to issue opinions to the public, parliament, government and other public bodies, to draft codes of conduct, to issue certification and approve criteria therefore, to adopt data protection clauses, to approve binding corporate rules? Does the law empower the authority to impose a range of sanctions, including reprimands, administrative fines, suspension of data flows and bans on processing of data (both temporary and permanent)? Does the law establish a board for the supervisory authority and set out its composition, voting procedures, powers, tasks and responsibilities? Do the board's tasks include:

GDPR Articles	Alignment indicators
	• Monitor and ensure correct application of the law, in cooperation with the head of the authority, • Issue guidelines, recommendations and best practices relating to the protection of personal data, • Draw up codes of conduct and establish data protection certification mechanisms, including criteria for certification, • Promote cooperation and exchange of information between supervisory authorities, • Maintain a database of decisions taken by the authority and national courts pursuant to the law, • Promote training programmes for public and private sector bodies and between supervisory authorities, and • Draw up annual report regarding the protection of natural persons pursuant to the law? Does the law require the board to act independently when performing its tasks and exercising its powers? Does the law require the board to report annually to the public, including on its exercise of powers? Does the law establish rules for the election, term of office and dismissal of members/chair of the board? Does the law establish the tasks of the chair of the board, including convening meetings and preparing agendas, ensuring the timely performance of tasks of the board, and notifying decisions adopted by the board to the head of the authority?
Articles 50, 60 to 67 – Cooperation and mutual assistance	Does the law require the supervisory authority to cooperate with supervisory authorities in other countries and to facilitate mutual assistance in order to contribute to the effective enforcement of data protection legislation? Does the law define the term 'mutual assistance'? Does the law set out the modalities of mutual assistance, including timelines for response to requests and the format in which requested information should be supplied? Does the law set out circumstances in which the supervisory authority can refuse to comply with a mutual assistance request?
Articles 77 to 84 – Remedies	Does the law give individuals the right to lodge a complaint with the supervisory authority, without prejudice to any other administrative or judicial remedy? Does the law require the supervisory authority to keep the complainant informed on the progress and outcome of the complaint within a specified period of time (e.g. 3 months), including the possibility of a judicial remedy? Does the law give complainants a right to an effective judicial remedy against a supervisory authority, without prejudice to any other administrative or judicial remedy: • where the authority does not handle a complaint or inform the data subject within three months on the progress or outcome of a complaint, and • against a legally binding decision of a supervisory authority concerning them? Does the law give complainants a right to an effective judicial remedy against a data controller or processor, without prejudice to any available administrative or non-judicial remedy, where he or she considers that his or her rights under the law have been infringed as a result of the processing of his or her personal data? Does the law give data subjects the right to have a not-for-profit organisation constituted in accordance with the law and active in the field of data protection rights and freedoms lodge a complaint on his or her behalf and represent him or her in the exercise of rights to an effective judicial remedy? Does the law give any person who has suffered material or non-material damage as a result of an infringement of the law the right to receive compensation from the controller or processor for the damage suffered? Does the law stipulate that a processor is only liable for damage where it has acted outside the law or contrary to the lawful instructions of the controller? Does the law state that, where more than one controller or processor are involved in the same processing resulting in a breach of the law, both shall be held liable for the entire damage to ensure effective compensation of the data subject? Does the law require the authority to ensure that the imposition of administrative fines is effective, proportionate and dissuasive in each individual case? Does the law set out the factors that the authority should take into account when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case i.e. the nature, gravity and duration of the infringement, the nature, scope and purpose of the processing, the intentional or negligent character of the infringement, any mitigation action taken by the controller or processor, the degree of responsibility of the controller or processor in light of technical and organisational measures implemented, any relevant previous infringements, the degree of cooperation with the authority, the categories of personal data affected, and any other aggravating or mitigating factor? Does the law set a cap on the amount of administrative fines for breaches of the law, including a monetary amount and a percentage of annual worldwide turnover in the case of an undertaking? Does the law set a cap on the amount of an administrative fine for failure to comply with an order of the authority?
Article 85-91 – Provisions relating to specific processing situations	Does the law require data controllers and processors to reconcile the right to protection of personal data with the right to freedom of expression and information, including by providing for exemptions and derogations if necessary? Are the Authority's powers in relation to journalistic activities and freedom of expression limited by safeguards? Does the law allow public bodies and authorities to disclose personal data in official documents for the performance of a task carried out in the public interest in accordance with law in order to reconcile public access to official documents with the right to protection of personal data? Does the law contain safeguards and derogations relating to data processing for archiving in the public interest or for scientific, historical research or statistical purposes?

GDPR Articles	Alignment indicators
	Does the law contain rules to reconcile obligations of professional secrecy or other secrecy obligations with the power of the supervisory authority to obtain access to all personal data, information, equipment and premises of controllers and processors? Does the law contain special rules relating to data processing carried out by churches and religious associations? Are exemptions subject to appropriate safeguards to protect the rights and freedoms of data subjects?
Supplementary questions on data sharing	Does the law contain provisions facilitating public and/or private sector data sharing, including data matching? Does the law require data controllers to undertake privacy impact assessments before sharing data in situations where: 1) there is a high risk to the rights and freedoms of natural persons; 2)when processing special categories of data on a large scale; and 3) when conducting systematic and extensive evaluations of personal aspects of natural persons based on automated processing and profiling producing legal effects? Does the law require the data controller to undertake prior consultation with the supervisory authority where a high level of risk is indicated? Does the law require sharing of personal data between data controllers to be governed by a contract? Does the law set out what a written agreement between data controllers should stipulate e.g. the roles of each party, the purpose of the sharing, the data to be shared, the basis of the sharing, appropriate organisational and technical measures in place to guarantee the rights of data subjects, limitations on recipients of the shared data, data quality, security and retention, keeping records, and apportionment of liability for personal data breaches? Does the law require sharing of personal data between a data controller and a data processor to be governed by a contract? Does the law set out what the contract should stipulate e.g. requiring the processor to take appropriate measures to ensure the security of processing, obliging it to assist the controller in allowing individuals to exercise their rights under the GDPR, and keep records? Does the law require the supervisory authority to establish a code of practice or guidelines for public sector data sharing?

Source: Prepared by the author.

UNITED NATIONS

ECLAC Series

Studies and Perspectives-The Caribbean

Issues published

A complete list as well as pdf files are available at
www.eclac.org/publicaciones

94. 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, Amelia Bleeker (LC/TS.2020/126, LC/CAR/TS.2020/4), 2020.
93. The use of technology and innovative approaches in disaster and risk management: a characterization of Caribbean countries' experience, Luciana Fontes de Meira, Omar Bello (LC/TS.2020/106, LC/CAR/TS.2020/3), 2020.
92. Preliminary overview of the economies of the Caribbean 2019–2020, Dillon Alleyne, Michael Hendrickson, Sheldon McLean, Maharouf Oyolola, Machel Pantin, Nyasha Skerrette and Hidenobu Tokuda (LC/TS.2020/56, LC/CAR/TS.2020/2), 2020.
91. Caribbean synthesis report on the implementation of the Lisbon Declaration on Youth Policies and Programmes, Catarina Camarinhas, Dwynette D. Eversley (LC/TS.2020/7, LC/CAR/TS.2020/1), 2020.
90. Proposal for a revitalized Caribbean Development and Cooperation Committee – Regional Coordinating Mechanism for Sustainable Development (CDCC-RCM): repositioning CDCC-RCM as the mechanism for sustainable development in Caribbean small island developing States (SIDS), Artie Dubrie, Omar Bello, Willard Phillips, Elizabeth Thorne, Dillon Alleyne (LC/TS.2020/6, LC/CAR/TS.2019/13), 2020.
89. Promoting debt sustainability to facilitate financing sustainable development in selected Caribbean countries: a scenario analysis of the ECLAC debt for climate adaptation swap initiative, Sheldon McLean, Hidenobu Tokuda, Nyasha Skerrette, Machel Pantin (LC/TS.2020/5, LC/CAR/TS.2019/12), 2020.
88. A preliminary review of policy responses to enhance SME access to trade financing in the Caribbean, Sheldon McLean, Don Charles (LC/TS.2020/4, LC/CAR/TS.2019/11), 2020.
87. Gender mainstreaming in national sustainable development planning in the Caribbean, Gabrielle Hosein, Tricia Basdeo-Gobin, Lydia Rosa Gény (LC/TS.2020/2, LC/CAR/TS.2019/10), 2020.
86. A review of Caribbean national statistical legislation in relation to the United Nations Fundamental Principles of Official Statistics, Amelia Bleeker, Abdullahi Abdulkadri (LC/TS.2020/1, LC/CAR/TS.2019/9), 2020.
85. Industrial upgrading and diversification to address competitiveness challenges in the Caribbean: the case of tourism, Michael Hendrickson, Nyasha Skerrette (LC/TS.2019/119, LC/CAR/TS.2019/8), 2019.

STUDIES AND PERSPECTIVES

Issues published:

94. 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
Amelia Bleeker

93. The use of technology and innovative approaches in disaster and risk management: a characterization of Caribbean countries' experience
Luciana Fontes de Meira
Omar Bello

92. Preliminary overview of the economies of the Caribbean 2019–2020,
Dillon Alleyne
Michael Hendrickson
Sheldon McLean
Maharouf Oyolola
Machel Pantin
Nyasha Skerrette
Hidenobu Tokuda

91. Caribbean synthesis report on the implementation of the Lisbon Declaration on Youth Policies and Programmes
Catarina Camarinhas
Dwynette D. Eversley

ECLAC
Economic Commission for Latin America and the Caribbean (ECLAC)
Comisión Económica para América Latina y el Caribe (CEPAL)
www.eclac.org

LC/TS.2020/126