LEGAL AND REGULATORY REVIEW REPORT

FOR

PROVISION OF CONSULTING SERVICES FOR DRAFTING THE HARMONIZED DATA PROTECTION AND PRIVACY LEGISLATION IN THE EASTERN CARIBBEAN CURRENCY UNION (ECCU)

REF NO.: LC-OECS COMMISSION-202351-CS-QCBS

Macmillan Keck
Attorneys & Solicitors
The Evolution of Digital

4 Boulevard Helvétique (1st Floor)
1205 Geneva Switzerland
Att'n: Rory Macmillan

T: +41 79 752 3622
rory@macmillankeck.pro

16 July 2025

Contents

1 Introduction 1
2 International good practices review 3
2.A Who and what are being regulated 4
2.A.1 Personal data 4
2.A.2 The data subject 6
2.A.3 Processing 6
2.A.4 Data controllers and data processors 6
2.B Scope of applicability and exemptions 8
2.B.1 Grace period 8
2.B.2 Automated and non-automated processing 8
2.B.3 Territorial connections 9
2.B.4 Personal use and journalistic, artistic and literary purposes 10
2.B.5 Processing by or on behalf of the public sector 10
2.B.6 Small businesses 11
2.B.7 Authorizing the making of additional exemptions 12
2.C Principles governing processing of personal data 12
2.C.1 Lawfulness of processing 12
2.C.2 Enumerated bases for lawful processing 13
2.C.3 Specific bases for processing sensitive personal data 16
2.C.4 Additional protections for children and others lacking legal capacity 16
2.C.5 Purpose specification and limitation 17
2.C.6 Data minimization 18
2.C.7 Data retention limitation 18
2.C.8 Fairness, transparency and mandated disclosures 18
2.C.9 Data quality 19
2.C.10 Accountability and data protection audits 19
2.C.11 Limitations on direct marketing activities or other commercial purposes 20
2.C.12 Privacy by design or default 20
2.D Individual rights concerning personal data 22
2.D.1 Right to know whether personal data are being processed 22
2.D.2 Right to access and review personal data being processed 22
2.D.3 Right to rectify personal data 23
2.D.4 Right to have personal data deleted 23
2.D.5 Right to port data to another data controller 24
2.D.6 Right not to be subject to decisions based on automated processing 25
2.D.7 Right to object to processing of personal data 26
2.E Data security 27
2.E.1 General data security requirements 27
2.E.2 Personal data breach notification requirements 28
2.E.3 Mandatory Data Protection/Privacy Impact Assessments (DPIAs) 30
2.F Cross-border transfers and processing of personal data 31
2.F.1 Restrictions on extraterritorial transfers of personal data 31

2.F.2 Approval of foreign jurisdictions for transfers 32
2.F.3 Assurance of safeguards 32
2.F.4 Exceptions or derogations from the general restriction 33
2.F.5 Enhanced requirements for sensitive personal data 34
2.F.6 Personal data localization requirements 34
2.F.7 Regional cross-border frameworks for transfer of personal data 35
2.G Institutions 37
2.G.1 Establishment or designation of a data protection authority 37
2.G.2 Functions of a data protection authority 37
2.G.3 Independence of the data protection authority 38
2.G.4 Funding of the data protection authority 39
2.G.5 Registration requirements 40
2.G.6 Appeals or judicial review 41
2.H Enforcement 42
2.H.1 Investigations 42
2.H.2 Compliance and enforcement orders 43
2.H.3 Administrative fines 43
2.H.4 Civil remedies 43
2.H.1 Criminal penalties 44
2.I Summary of the elements of a data protection framework 46
2.I.1 Scope of applicability 46
2.I.2 General elements of data protection law 46
2.I.3 Principles governing processing of personal data 46
2.I.4 Individual rights concerning personal data 47
2.I.5 Data security 47
2.I.6 Cross-border data transfers of personal data 47
2.I.7 Institutions 48
2.I.8 Penalties and enforcement 48
3 Legal and regulatory review of regional instruments 48
3.A Data protection 49
3.A.1 OECS Model Bill 49
3.A.2 Policy Considerations for the Development of Data Protection and Privacy Legislation in the Eastern Caribbean Currency Union (ECCU) 57
3.B Sector-specific regional legislation 59
3.B.1 Cybersecurity and cybercrimes 59
3.B.2 Consumer protection 59
3.B.3 Freedom of information requests 60
3.B.4 Health 60
3.B.5 Education 60
3.B.6 Financial Services 60
3.B.7 National identification 65
3.B.8 Passports 66
3.B.9 Civil Registration 66

3.B.10 Electronic communications 66
3.B.11 Electronic transactions 67
3.B.12 E-signatures 69
4 Legal and regulatory review of national legislation 70
4.A Anguilla 71
4.A.1 Data protection 71
4.A.2 Cybersecurity and cybercrimes 71
4.A.3 Consumer protection 71
4.A.4 Freedom of information requests 71
4.A.5 Health 71
4.A.6 Education 72
4.A.7 Financial services (including digital financial services) 72
4.A.8 National identification (including digital and functional forms) 74
4.A.9 Passports 74
4.A.10 Civil registration 74
4.A.11 Electronic communications 76
4.A.12 Electronic transactions 77
4.A.13 E-signatures 79
4.B Antigua and Barbuda 80
4.B.1 Data protection 80
4.B.2 Cybersecurity and cybercrimes 84
4.B.3 Consumer protection 86
4.B.4 Freedom of information requests 86
4.B.5 Health 87
4.B.6 Education 88
4.B.7 Financial services (including digital financial services) 90
4.B.8 National identification (including digital and functional forms) 91
4.B.9 Passports 92
4.B.10 Civil registration 92
4.B.11 Electronic communications 95
4.B.12 Electronic transactions 96
4.B.13 E-signatures 97
4.C Dominica 99
4.C.1 Data protection 99
4.C.2 Cybersecurity and cybercrimes 99
4.C.3 Consumer protection 99
4.C.4 Freedom of information requests 99
4.C.5 Health 99
4.C.6 Education 102
4.C.7 Financial services (including digital financial services) 104
4.C.8 National identification (including digital and functional forms) 106
4.C.9 Passports 106
4.C.10 Civil registration 106

4.C.11 Electronic communications 108
4.C.12 Electronic transactions 109
4.C.13 E-signatures 111
4.D Grenada 113
4.D.1 Data protection 113
4.D.2 Cybersecurity and cybercrimes 115
4.D.3 Consumer protection 117
4.D.4 Freedom of information requests 118
4.D.5 Health 118
4.D.6 Education 120
4.D.7 Financial services (including digital financial services) 121
4.D.8 National identification (including digital and functional forms) 123
4.D.9 Passports 124
4.D.10 Civil registration 125
4.D.11 Electronic communications 126
4.D.12 Electronic transactions 127
4.D.13 E-signatures 129
4.E Montserrat 131
4.E.1 Data protection 131
4.E.2 Cybersecurity and cybercrimes 131
4.E.3 Consumer protection 132
4.E.4 Freedom of information requests 132
4.E.5 Health 133
4.E.6 Education 134
4.E.7 Financial services (including digital financial services) 135
4.E.8 National identification (including digital and functional forms) 136
4.E.9 Passports 136
4.E.10 Civil registration 136
4.E.11 Electronic communications 137
4.E.12 Electronic transactions 138
4.E.13 E-signatures 140
4.F Saint Kitts and Nevis 141
4.F.1 Data protection 141
4.F.2 Cybersecurity and cybercrimes 144
4.F.3 Consumer protection 145
4.F.4 Freedom of information requests 146
4.F.5 Health 148
4.F.6 Education 149
4.F.7 Financial services (including digital financial services) 151
4.F.8 National identification (including digital and functional forms) 153
4.F.9 Passports 153
4.F.10 Civil registration 153
4.F.11 Electronic communications 153

4.F.12 Electronic transactions 154
4.F.13 E-signatures 156
4.G Saint Lucia 157
4.G.1 Data protection 157
4.G.2 Cybersecurity and cybercrimes 161
4.G.3 Consumer protection 163
4.G.4 Freedom of information requests 163
4.G.5 Health 164
4.G.6 Education 165
4.G.7 Financial services (including digital financial services) 167
4.G.8 National identification (including digital and functional forms) 169
4.G.9 Passports 170
4.G.10 Civil registration 171
4.G.11 Electronic communications 172
4.G.12 Electronic transactions 174
4.G.13 E-signatures 176
4.H Saint Vincent and the Grenadines 177
4.H.1 Data protection 177
4.H.2 Cybersecurity and cybercrimes 181
4.H.3 Consumer protection 182
4.H.4 Freedom of information requests 184
4.H.5 Health 185
4.H.6 Education 185
4.H.7 Financial services (including digital financial services) 187
4.H.8 National identification (including digital and functional forms) 189
4.H.9 Passports 189
4.H.10 Civil registration 190
4.H.11 Electronic communications 191
4.H.12 Electronic transactions 192
4.H.13 E-signatures 194
5 Conclusions of the data protection gap analysis 195
5.A Weaknesses of the data protection laws 195
5.B Barriers to cross-border data flows 196
5.B.1 Lack of provisions on cross-border data 197
5.B.2 Varying levels of maturity 198
5.B.3 Differences among national laws 198
5.C Implications for the digital economy 199
6 Considerations for regional and national legal frameworks 199
6.A Legal drivers in design of a data protection framework 200
6.A.1 Rights, obligations and powers 200
6.A.2 Implications for institutional design 201
6.B National and regional allocation of functions 203
6.C Standalone or multi-domain authorities 204

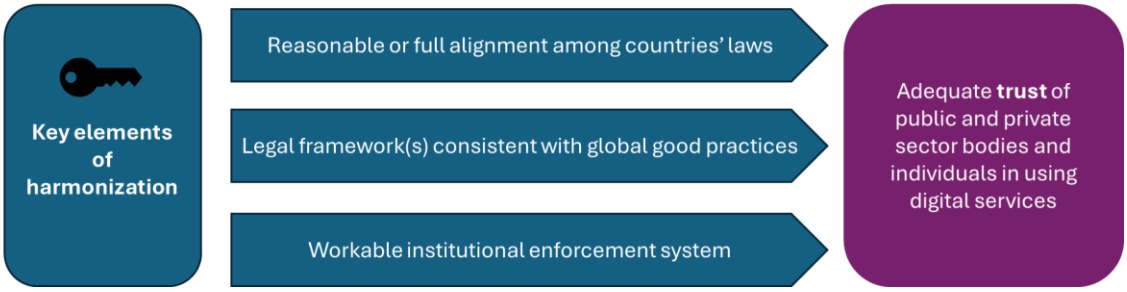
7 Relevant existing regional frameworks 204
7.A Introduction 204
7.B OECS Framework 205
7.C The ECCB/ECCU and ECSRC frameworks 207
7.D ECTEL framework 208
7.E Consumer protection 209
7.F New framework under a regional data protection agreement 210
7.G Model law for willing countries 210
7.H Overview of the frameworks 210
8 Conclusions 212
8.A Findings 212
8.A.1 Gap analysis 212
8.A.2 Considerations in approaching the gaps 212
8.A.3 Relevant existing regional frameworks 212
8.B Recommendations 213
8.B.1 Option 1 – Regional authority with satellite offices 213
8.B.2 Option 2 – Combination of a regional and national authorities 214
8.B.3 Option 3 – National authorities with regional coordination 216
8.B.4 Summary of options 218
9 Annex: Matrix of legal instruments reviewed 220
9.A Regional framework 220
9.B Anguilla 221
9.C Antigua and Barbuda 221
9.D Dominica 222
9.E Grenada 223
9.F Montserrat 224
9.G Saint Kitts and Nevis 225
9.H Saint Lucia 226
9.I Saint Vincent and the Grenadines 227

1 Introduction

This legislative and regulatory gap analysis report is Macmillan Keck's second deliverable under our assignment to draft harmonized data protection and privacy legislation for the Eastern Caribbean Currency Union (ECCU).

We approach the notion of harmonized data protection and privacy (we generally refer to these notions together as data protection) with the understanding that the ultimate goal is to promote a healthy regional digital economy. This requires personal data to be subject to protection and to flow unimpeded among ECCU member countries, i.e., the trusted free flow of personal data within the region. For example, a service provider (e.g., a bank) should be able to serve its customers in different countries without having to incur cost, time and effort examining the differences in each country's laws, or to design its data processing, storage and administrative systems or conditions of service differently for different jurisdictions in the region. Similarly, a public body or private firm dealing with information about people (citizens, residents or customers) should be able to outsource its processing activities without itself or the outsourced processing firm having to make different arrangements because of the jurisdiction in the region in which the public body or private firm, the outsourced processing firm, the people or the processing are located. The standards of data protection must also support levels of trust sufficient for public and private sector bodies and members of the populations to embrace the use of digital products and services.

Figure 1. Features of a harmonised data protection framework



We thus regard harmonization in this context as comprising three key elements:

- ***Reasonable alignment:*** There is a reasonable level of alignment among all applicable legislation and how it is applied in the region, including among national legislation, and among national and regional legislation. A reasonable level of alignment would mean that the legislation does not impede development of a regional digital economy whether because inconsistencies among them create significant confusion or conflict, or because legislation expressly limits transfers of personal data outside their respective jurisdictions.
- ***Good international practice:*** The substantive obligations, rights, powers and procedures in the applicable legislation (national, regional or combination) generally align with international good practice in data protection legislation.
- ***Institutional effectiveness:*** There is a workable institutional arrangement for coherent and effective enforcement of data protection legislation, whether through cooperation among national authorities, the authorization of a single regional authority having powers across all jurisdictions, or a combination of these.

This report is based on our review and assessment of the relevant countries' laws and regulations identified and obtained by our local team members in the region in accordance with the Terms of Reference, as well as documents supplied to us by the ECCB and OECS Commission. Stakeholder consultations that will follow in the next period after this delivery may generate additional information and context.

In section 2 of this report, we review global practices in data protection, covering a range of examples of national and regional laws, regulations, treaties, conventions, guidelines, and model laws on data protection and data privacy. We refer to "good practice" rather than "best practice" because there remains significant

divergence in approaches and opinions on data protection internationally, and different approaches may be more or less appropriate in different contexts. As a result, it is not in our view possible to declare any one approach definitively "best practice." Section 2 thus illustrates examples of a variety approaches, concluding with a summary of the cluster of key elements found in a good practice data protection framework.

In Section 3 we provide an overview of the regional legal frameworks. We review both applicable data protection laws as well as other sectoral legal frameworks.

Section 4 is our gap analysis focused on national laws. We review the state of current laws in the ECCU member states affecting personal data and provide a gap analysis against international good practice. For each ECCU member state that has enacted a generally applicable data protection law (some have not), we review that law.

Data protection provisions (e.g., consent requirements, authorizations to collect data, privacy and security requirements, breach notifications) do not necessarily exist only in generally applicable data protection legislation. They may be present in legislation governing particular sectors of the economy. For example, a health sector law may require the consent of a patient to collect data about them, may authorize the processing of such data, and may provide for the confidential and secure treatment of such data by healthcare professionals. We therefore also review in section 3 the legislation applying to the most significant areas of the economy in each country in order to assess how they affect the processing of data about members of the population, including authorization and conditions of processing, protection of privacy and security of personal data.

We also review a broad range of national legislation with a view to identifying what existing provisions of law and regulation may be inconsistent with a new generally applicable data protection law (national or regional) such that such existing provisions may need to be amended or repealed or taken into account in drafting new generally applicable data protection legislation. This review enables us to identify gaps in each country across all significant areas of legislation in light of the international practice described in Section 2.

In Section 5 we consider the harmonization of the ECCU members states' data protection frameworks. First, picking up from the conclusion in section 4, we look together at all ECCU members combined, illustrating their gaps together. We then look beyond alignment of each country with international good practice to the strategic regional objective of a regional digital economy. We consider the degree to which the national laws expressly impede the transfer of data outside their respective jurisdictions in order to understand barriers to flows of personal data within the ECCU. We also consider the degree to which inconsistencies and conflicts among the various laws' substantive provisions and institutional arrangements might impede the flow of personal data and so undermine development of a smoothly functioning regional digital economy. Lastly, we consider the institutional arrangements and the benefits and challenges of having multiple national authorities, a single regional authority, or a combination of these.

We then consider the past efforts towards regional harmonization. We review the OECS Model Bill that was prepared in 2016 and served as a model for these national laws with a view to whether it would be a helpful instrument to use in renewing the efforts towards harmonization. We conclude that, with the progression of time, the OECS Model Bill is now significantly out of date and has too many gaps to serve this function. In addition, we review the Policy Considerations for the Development of Data Protection and Privacy Legislation in ECCU issued in 2024 (the "ECCU Policy Considerations") and its contribution to harmonization. We find it to be a helpful, high level guiding signpost in building the policy momentum.

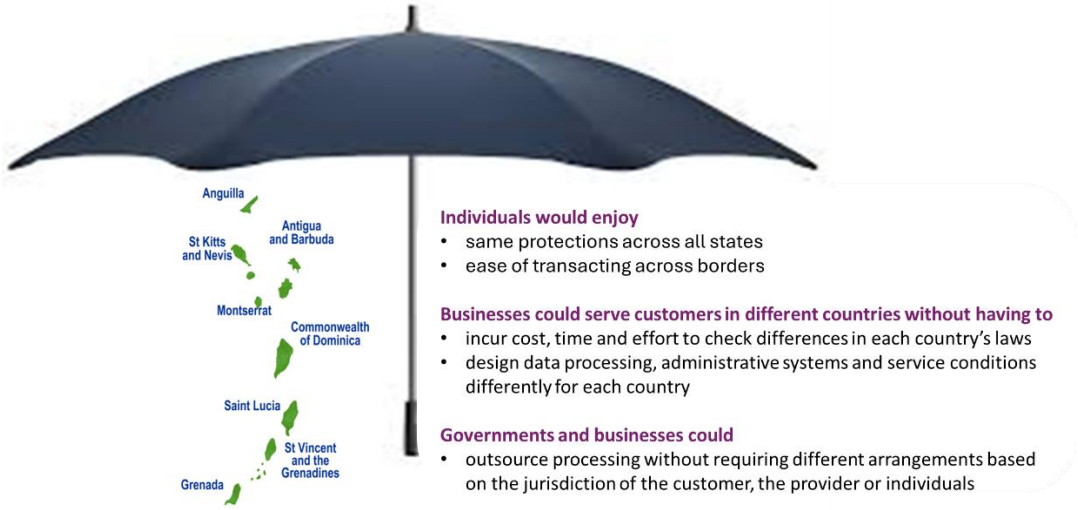
In Section 5, we bring together our conclusions from the review of existing laws. In Section 6, we turn to thinking about solutions. We reflect on legal and functional dimensions of data protection in the context of a regional economy to inform the options. We then discuss in Section 7 whether and how existing frameworks in the region could be used to introduce, or serve as examples for, an effective data protection framework, exploring the benefits and drawbacks of each.

Section 8 provides our conclusions, offering three options for structuring regional harmonization. The first involves a regional regulatory authority with satellite offices in each country. The second involves a combination of national authorities handling national cases but a regional authority leading on cases that

involve multiple countries. The third relies on national authorities with a regional body facilitating the designation of one of them as a lead authority in cases involving multiple countries. The selection of the preferred option will depend on readiness to grant power and budget to a regional authority, national sovereignty, and appetite for establishing new or leveraging existing institutions.

In the Annex at the end of the report, we provide a matrix of all the legislative instruments reviewed in the study.

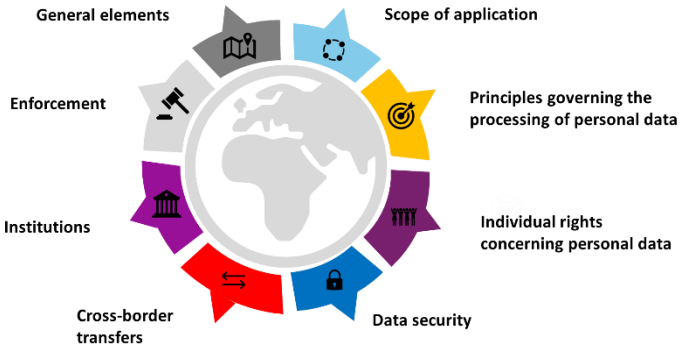
Figure 2. The benefits of harmonisation for all stakeholders



2 International good practices review

This section of the report sets out international good practices in data protection legislation, drawing on a range of national and regional legal frameworks. It outlines the key components of effective data protection laws, highlighting the benefits and rationales behind specific legislative choices, and illustrates how these practices are embodied across various instruments. These include prominent frameworks such as the EU's General Data Protection Regulation (GDPR), Trinidad & Tobago's Data Protection Act (DPA), Jamaica's Data Protection Act (DPA), and Brazil's General Data Protection Law (LGPD), alongside legislation from Africa and Asia, including South Africa's Protection of Personal Information Act (POPIA), Kenya's Data Protection Act (DPA), and Malaysia's Personal Data Protection Act (PDPA). For economy presentation, we have not set out all of the relevant provisions of all of these laws (this would be extremely lengthy and uninteresting to the reader), but we have varied the references to them in order to convey the generality of good practice.

Figure 3. Basic elements of data protection legislation

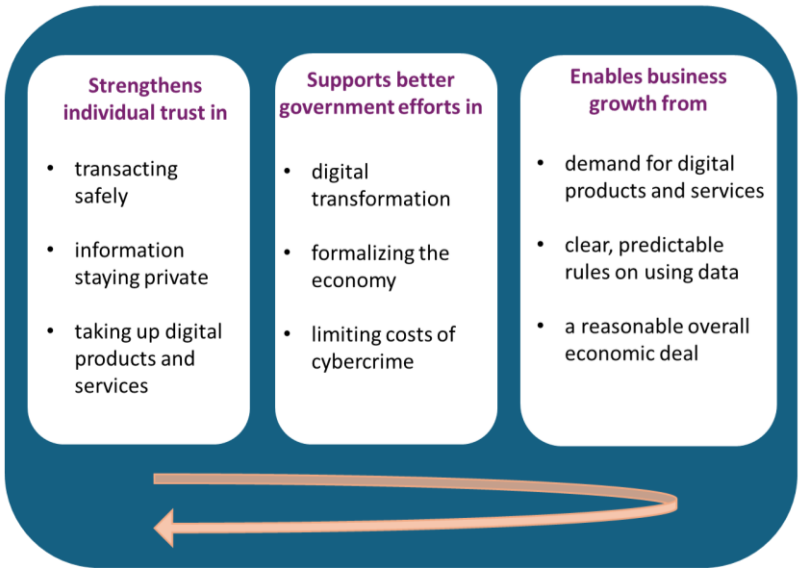


Additionally, this section refers to the data protection laws of the United States, Australia, Canada and New Zealand, as well as international treaties, conventions, guidelines, and model laws such as the HIPCAR Privacy and Data Protection Model Policy. At the client's request, we refer on occasion to provisions in the U.S. American Privacy Rights Act (APRA). This bill was tabled before the legislature in the US but not enacted into law. Nevertheless, the APRA bill had useful and innovative elements that we think are worth taking into account. The fact that it has not been adopted is, in our view, more reflective of the degree of

debate in the US about whether to adopt a generally applicable data protection law than the quality of that bill.

Through this process, our goal is to develop a data protection harmonization framework that incorporates lessons and effective approaches from global best practices while adapting them to the unique cultural, economic and legal context of the ECCU region and its member states. From time to time, we offer our views on where it may be helpful to take a simpler approach in small countries with less resources.

Figure 4. Enabling and safeguarding the digital economy



2.A Who and what are being regulated

Before addressing substantive provisions of data protection legislation, it is useful to begin with what is being regulated: what activity (processing) applied to what information (personal data) relating to whom (data subjects) carried out by whom (controllers and processors). These key concepts are often embodied in defined terms that are typically found at the beginning of data protection laws.

2.A.1 Personal data

Personal data

The word "data" can encompass an unlimited range of information. Many types of data potentially trigger legal protections and confidentiality obligations in a variety of contexts. These include copyrighted materials, patents, trade secrets, national security or other government secrets, individuals' medical information, and lawyer-client communications subject to legal privilege.

Data protection legislation cuts across these and all other forms of data to focus on "personal data" or "personal information," which (although definitions vary) is typically defined broadly as any information relating to an identified or identifiable individual.

The concept of "identified or identifiable individual" is typically defined in data protection legislation. For example, the EU's GDPR defines an "identifiable natural person" as:

> *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.*

Kenya's DPA similarly defines "identifiable natural person" as

> *a person who can be identified directly or indirectly, 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 or social identity.*

Although not typical, some instruments set out non-exhaustive examples of personal data. For example, South Africa's POPIA includes in the definition a long list of examples of information that would qualify as "personal information." It includes not only common concepts such as attributes about a person (race, religion, sex) and identifiers but also "personal opinions, views or preferences" and confidential correspondence. While these may well fall within the interpretation of a statutory definition in practice, they are less typically included in the statutory definition itself.

Anonymization

The linkage to an identified or identifiable individual is an essential element of personal data. One way of protecting privacy is to anonymize or de-identify personal data. When data are anonymized, all linkages to an identified or identifiable individual are permanently and irrevocably removed. Accordingly, anonymized data are typically not considered "personal data" and are generally treated as outside the scope of a data protection instrument. Recital 26 of the EU's GDPR makes this point expressly:

> *The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.*

Anonymization is different from de-identification of data, where identifying information is replaced with coded information that can in turn be de-coded so that the individual can be re-identified. As a result, de-identification would not qualify as anonymized.

However, in recent years, it has become increasingly clear that anonymization is difficult to achieve, and that anonymization processes may not truly remove all linkages to the identifiable individual. Several studies have shown that by combining data points about an individual, particularly from multiple large permanently anonymized data sets, it is sometimes possible to re-identify them.[1] Other approaches may be more effective at protecting privacy, such as differential privacy, a process that introduces "noise" to data sets which results in errors if deanonymization of personal data is attempted.

Sensitive personal data

Many data protection instruments specify certain kinds of personal data that, due to their nature, merit additional protection and obligations. These are generally referred to as "sensitive personal data" or a similar term. For example, South Africa's POPIA refers to "special personal information."

Sensitive personal data typically include personal attributes about an individual's body and behaviors (biometrics, health status, sexuality), lineage (race, ethnicity), or spiritual beliefs, philosophy and opinions (religion, political beliefs). They may also include other personal data which could be used to infer these attributes (e.g., location data indicating a place of worship, output of wearable devices indicating health status, etc.).

The enhanced protections around sensitive personal data reflect the concern that these personal data may be embarrassing or uncomfortable to the data subject if disclosed, or risk being used for undesirable profiling or discriminatory treatment adverse to members of a potentially vulnerable group.

The EU's GDPR formulation of sensitive personal data is typical:

[1] See, e.g., Rocher, L., Hendrickx, J.M. & de Montjoye, Y. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun 10, 3069 (2019). https://doi.org/10.1038/s41467-019-10933-3. The study is discussed in Hern, A, *'Anonimised' data can never be totally anonymous, says study*, The Guardian, 23 July 2019, available at https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds

> *[…] personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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 […].*

Some instruments, including South Africa's POPIA and Malaysia's PDPA also include as sensitive personal data, any data relating to the commission or alleged commission of criminal acts. Other instruments, including Malaysia's PDPA and Kenya's DPA allow for additional categories of personal data to be subsequently designated as sensitive personal data by a Minister or regulator.

Additionally, other data protection instruments identify specific attributes related to an individual's participation in the digital economy and online activities as sensitive. For instance, the proposed US APRA bill defined 18 categories of sensitive information, including, among others, personal data related to an individual's media (e.g., photos, videos, calendar data), private communications, login credentials, online activity profiles, video content consumption, neural data, and military service status.

Furthermore, certain instruments, such as New Zealand's DPA, do not prescribe fixed categories of "sensitive" personal information. Rather, any personal information can be sensitive, even highly sensitive, depending on the particular context and surrounding circumstances, including cultural perspectives.

The different treatment of sensitive personal data creates considerable complexities, particularly where different lawful bases of processing apply. In the case of small jurisdictions where there are limited resources for all data controllers across the country to devote to the details of data protection, we tend to consider that having robust data protection for all personal data, with a common set of standards, is sufficient, and that it is not necessary to have different provisions applying to general personal data and sensitive personal data. An obligation to ensure that the controller uses measures appropriate in light of the sensitivity of the personal data should suffice.

2.A.2 The data subject

The individual about whom a piece of personal data relates is often referred to as a "data subject." By reference to the definition of "personal data" (see above), a data subject must be an identified or identifiable individual.

2.A.3 Processing

Data protection legislation concerns various types of actions taken with respect to personal data, typically referred to together under the umbrella term "processing." This typically encompasses the entire lifecycle of personal data handling. Kenya's DPA sets out a typical definition:

> *'processing' means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as*
>
> *(a) collection, recording, organisation, structuring;*
>
> *(b) storage, adaptation or alteration;*
>
> *(c) retrieval, consultation or use;*
>
> *(d) disclosure by transmission, dissemination, or otherwise making available; or*
>
> *(e) alignment or combination, restriction, erasure or destruction.*

The sheer breadth of this must be understood for what it is. Literally, any handling of any information about an individual is processing personal data and falls under the law, except where excluded from the scope (see section 2.B).

2.A.4 Data controllers and data processors

Having discussed the type of data typically addressed in data protection legislation (personal data) and the regulated activity (processing), we turn to the two principal actors to whom data protection obligations typically apply: data controllers and data processors.

Data controllers

Data controllers are those persons or entities which are ultimately responsible for the processing of personal data – those who, alone or jointly, determine the purpose of and means for processing personal information. Examples of a data controller would be a website that collects personal information from a visitor's computer, a bank that requires account holders to provide identifying information, or a government entity that collects information about people to provide public services to them. Data controllers are the subject of most of the obligations regarding processing of personal data.

Typically, then, the rights of the data subject (discussed later in this report) to information, access, rectification and erasure, and to object to the processing of personal data, are rights against the data controller. The data controller is also typically responsible for notifying the authorities and data subjects about data breaches. In some cases where the data protection law provides or other laws (e.g., tort) apply, the data controller may be liable for damage resulting from unlawful processing.

Data controllers are sometimes referred to with different names in different countries' laws (e.g., "controller," "personal information controller," "data user," "responsible party") but the essential nature of the role is relatively uniform across most data protection legislation.

Data processors

It is common to outsource information technology activities, including data processing, to specialist firms, organizations and individuals. These are typically referred to as "data processors", more specifically those persons or entities that are not directly under the control or authority of data controllers but that carry out processing of personal data at the direction of or on behalf of a data controller. For example, while a bank collecting personal information about account holders would be a data controller, if the bank outsources operation of the software used to access and store the records, this would be the data processor. Data processors are referred to with different names in different countries' laws ("processor," "operator"). For example, Jamaica's definition reflects this notion:

> *data processor", in relation to personal data, means any person, other than an employee of the data controller, who processes the data on behalf of the data controller;*

Additionally, the Malaysia PDPA definition is again instructive:

> *'data processor', in relation to personal data, means any person, other than an employee of the data controller, who processes the personal data solely on behalf of the data controller, and does not process the personal data for any of his own purposes;*

Data processors might not have a direct relationship with the data subject. They may be acting under instructions from the data controller and may be subject to requirements and limitations from a contract with the data controller. As their responsibilities and scope for decision-making are narrower and defined for them by the controller, their data protection obligations and liabilities are also narrower. Nevertheless, because data processors are handling personal data, it is common to give them certain legal responsibilities, including directly obligating them to adhere to certain general data security requirements, as well as in some countries to give notifications in the case of data breaches (see Sections 2.E.1 and 2.E.2). For example, Brazil's LGPD states that:

> *The processor shall carry out the processing according to the instructions provided by the controller, which shall verify the obedience of her/his own instructions and of the rules applicable to the subject and the situation at hand.*

If a data protection framework applied only to data security and breach notifications, one might not need the two concepts of controller and processor. But there are numerous privacy protections that go beyond the functions of merely processing data to the wider business activities and administrative organization, involve decisions about compliance and often a relationship with the data subject. The distinction between data controller and data processor serves to allocate responsibility.

Frequently, data protection legislation imposes obligations on data controllers who are then responsible for assuring compliance with their contracted data processors. For example, the CCS Data Protection and Privacy rules state:

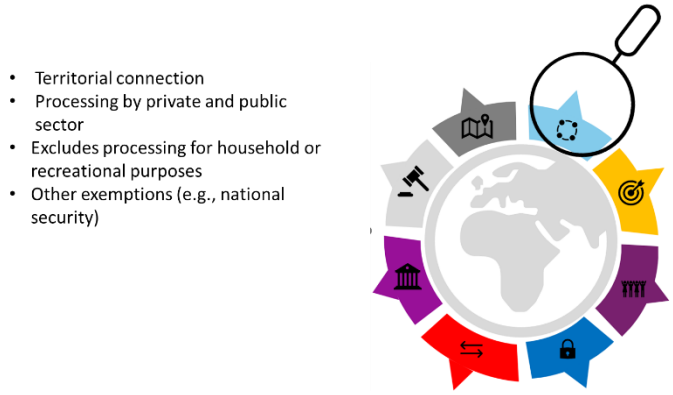
> *Where any other person processes personal information on behalf of the Data Controller, the Data Controller shall ensure that the person: (a) has sufficient controls in place to implement the security measures that must be taken; (b) actually takes the measures so identified by the data controller.*

2.B Scope of applicability and exemptions

Given the breadth of what is encompassed in processing personal data, it is important to limit the scope of application. The scope of data protection legislation is typically limited so as to exclude areas that would be excessive or impractical to regulate. The scope is thus limited:

- delaying the application of some or all obligations for a grace period;
- applying to automated means of processing (e.g., on computers, servers and other electronic devices) but not non-automated means (e.g., in paper form);
- applying only where there are sufficient connections with the territory of the jurisdiction; and
- excluding certain types of processing activities by or on behalf of the State that are important to national security, the functioning of open society, or small business.

Figure 5. Scope of application



These can be expressed as limitations of scope or as exemptions or exclusions. Some legislation has proposed exclusions for small businesses.

2.B.1 Grace period

Many data protection laws have provided that all or part of the law will only enter into force after a period, often two years. The goal of introducing data protection legislation is not to catch data controllers unprepared. Rather, the obligations should be implemented over time, allowing for awareness campaigns and outreach to the private and public sector. Compliance with the data protection principles, individual rights, data security requirements and limitation on cross-border transfers will require significant investment in technology, expertise and administrative measures.

As a threshold matter, then, we recommend that the obligations under the new legislation are not made immediately effective. In the case of OECS member states, if they will be required to introduce national legislation to establish the data protection provisions with the force of law in their respective states, any grace period could take this time period into account.

2.B.2 Automated and non-automated processing

Data protection instruments generally limit the types of processing activities that are subject to data protection obligations. This is because some types of processing are unlikely to cause harm to data subjects, are an inherent part of an individual's freedom or are necessary for a government in order to protect its citizens.

For example, these instruments typically apply to processing by both automated and non-automated means. However, processing by non-automated means is generally limited to those instances when personal data is meant to be included in a "filing system." For example, South Africa's POPIA states:

> *This Act applies to the processing of personal information . . . entered in a record by or for a responsible party making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof[.]*

2.B.3 Territorial connections

Data protection legislation typically requires a minimum level of connection to a geographic or political territory for the obligations, protections and rights to apply to processing of personal data about a data subject. These provisions are an implicit acknowledgement that there are limitations, both practical and legal, to the extraterritorial application of domestic law to geographically remote entities and activities. Data protection legislation typically only applies if there is a sufficient connection between the territory and:

- the data controller and/or data processor;
- the processing activity; or
- data subjects whose data are being processed.

Territorial connections of data controllers and data processors

Data protection legislation typically applies where the data controller or data processor is resident in or "established" in the territory. For example, the EU's GDPR states:

> *This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*

Similarly, Jamaica's DPA states:

> *This Act applies to a data controller in respect of any personal data only if the data controller – (a) is established in Jamaica or in any place where Jamaican law applies by virtue of international public law, and the personal data are processed in the context of that establishment.*

Territorial connections of processing activities

Data protection legislation typically also applies where the processing takes place within the territory. Some instruments exclude from this the mere transmission through the territory. For example, South Africa's POPIA states:

> *This Act applies to the processing of personal information . . . where the responsible party is . . . not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.*

Similarly, Jamaica's DPA states that this Act applies where [a data controller]:

> *(b) though not established in Jamaica— (i) uses equipment in Jamaica for processing the personal data otherwise than for the purpose of transit through Jamaica;*

Territorial connections of data subjects

The third basket invokes connections to the location of the data subjects whose personal data are being processed. Data protection legislation typically applies where the data subject is physically located within the territory. For example, Kenya's DPA states:

> *This Act applies to the processing of personal data […] by a data controller or data processor who . . . [is] not established or ordinarily resident in Kenya, but process[es] personal data of data subjects located in Kenya.*

However, applicability based solely on the location of the data subject would often result in impractical overreach. For example, where a person in the territory (e.g., Portugal) browses a website outside the territory (e.g., in Singapore), it would be unworkable for a foreign data controller (e.g., in the United States) operating the and having no specific intentions for residents of the territory (i.e., Portugal) to become subject to data protection obligations of the territory just because the website picks up information about the individual. Accordingly, many jurisdictions only apply the legislation on the basis that data subjects are located in the territory if the data controller is actively targeting, marketing to or monitoring them. For example, the EU's GDPR provides:2

> *This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, 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 Union; or*
>
> *(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*

2.B.4 Personal use and journalistic, artistic and literary purposes

Data protection legislation also typically exempts certain types of processing from the scope of application, such as processing for personal use, journalistic, artistic and literary purposes, and national security.

To align with global norms, we recommend excluding processing of personal data by individuals for purely personal, household, family, or recreational purposes. Activities such as organizing amateur sport teams or planning family reunions are not likely to cause harm and regulating them would be a massive intrusion into the private lives of individuals. For example, APEC's Privacy Framework specifically excluded from the definition of "personal information controller":

> *an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.*

Similarly, Jamaica's DPA provides:

> *Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes) are exempt from the data protection standards and the provisions of Parts II and III.*

Following international precedents, we recommend providing exemptions for processing carried out for journalistic, artistic, or literary purposes, with the caveat that such exemptions may be subject to reasonable limitations to balance privacy and freedom of expression. However, in general, these activities are important beneficial uses of personal data for society that should be preserved, subject to some protection.

2.B.5 Processing by or on behalf of the public sector

National security, defense and public safety

It is common to exclude from data protection legislation processing by or for public authorities that involves national security, defense and public safety. Essentially governments do not wish to be constrained when attending to such urgent and vital matters of collective good which they regard as outweighing the need to protect individuals. Although such matters are often excluded from the general data protection legislation,

[2] An alternative, less common approach, is adopted in New Zealand's DPA of 2020, which applies to: *[…](b) an overseas agency (B), in relation to any action taken by B in the course of carrying on business in New Zealand in respect of personal information collected or held by B: (c) an individual (C) who is not ordinarily resident in New Zealand, in relation to any action taken by C in respect of— (i) personal information collected by C while present in New Zealand, regardless of where the information is subsequently held by C or where the individual to whom the information relates is, or was, located: (ii) personal information held by C while present in New Zealand (but not collected by C while present in New Zealand), regardless of where the individual to whom the information relates is, or was, located.*

it is reasonably common to allow such exemptions on condition that the exceptions are necessary and proportionate or authorized by law. For example, the APEC Privacy Framework states:

> *Exceptions to these Principles […] including those relating to national sovereignty, national security, public safety and public policy should be:*
>
> *(a) limited and proportional to meeting the objectives to which the exceptions relate; and,*
>
> *(b)(i) made known to the public; or, (ii) in accordance with law."*

Data protection legislation also sometimes provides a residual general data protection obligation so that the exceptions only apply so long as there are safeguards to protect personal data. For example, South Africa's POPIA states:

> *This Act does not apply to the processing of personal information . . . by or on behalf of a public body—*
>
> *(i) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defense or public safety; or*
>
> *(ii) the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information;*

Processing by or for the State generally

Some countries' data protection legislation also expressly or impliedly limits the scope or exempts processing by the public sector more broadly. For instance, Malaysia's PDPA applies only to processing personal data for commercial purposes, expressly or implicitly excluding most government processing of personal data. We do not consider this to be good practice unless sufficient alternative governance arrangements are made to secure the protection of personal data where it is the State that is the controller or processor. Numerous national, regional and local organs of government will hold extensive personal data about the whole population. The State's powers to provide or deny access to key public services, and its centrality in ensuring or undermining rights and liberties, make privacy and security of personal data held by public authorities vitally important. We recommend therefore that as a general matter data protection legislation apply both to the public and private sectors.

Exemptions are often provided for processing carried out in connection with national or public security, detection, investigation and prevention of criminal activity, and other sensitive government functions. Some countries nevertheless take the view that there may be reasons not to apply the legislation in full to the public sector. The GDPR permits EU Member States to make laws restricting data protection obligations for a range of public functions. However, these must "respect the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society."

2.B.6 Small businesses

In order not to impede entrepreneurial activity with the burden of regulation, some legislation exempts from the scope of their application to small businesses. For example, the US APRA bill (which has not been enacted) provided that it does not apply to a small business:

> *(i) that has average annual gross revenues for the period of the 3 preceding calendar years (or for the period during which the entity has been in existence, if such period is less than 3 calendar years) not exceeding $40,000,000, indexed to the Producer Price Index reported by the Bureau of Labor Statistics;*
>
> *(ii) that, on average for the period described in clause (i), did not annually collect, process, retain, or transfer the covered data of more than 200,000 individuals for any purpose other than initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product; and*

(iii) that did not, during the period described in clause (i), transfer covered data to a third party in exchange for revenue or anything of value, except for purposes of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product or facilitating web analytics that are not used to create an online activity profile.

Similarly, Australia's data protection authority exempts small businesses from the application of its Act. However, it provides that organizations operating in specific sectors and engaging in particular processing activities that create vulnerabilities for data subjects are not exempt. These include health service providers, entities trading personal information, credit reporting agencies, and businesses that have voluntarily opted into the DPA.

2.B.7 Authorizing the making of additional exemptions

Some instruments permit a regulator or other government entity from issuing further specific exemptions. For example, Malaysia's PDPA states:

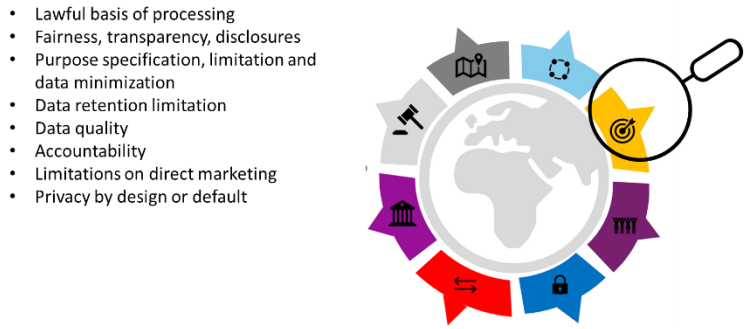
> *The Minister may, upon the recommendation of the Commissioner, by order published in the Gazette exempt—*
>
> *(a) the application of any of the Personal Data Protection Principles under this Act to any data user or class of data users; or*
>
> *(b) any data user or class of data users from all or any of the provisions of this Act.*

However, such approaches are not common, and we would generally recommend not leaving open the question whether particular users or classes of data could be exempted, but to define it clearly in the legislation upfront.

2.C Principles governing processing of personal data

Data protection instruments typically require that processing of personal data within the scope of the instrument be governed by a collection of commonly included governing principles, sometimes referred to as the "data protection principles." These are the core of most data protection frameworks. They often reflect the Fair Information Practice Principles (FIPPs), a set of longstanding, internationally recognized personal data protection principles.

Figure 6. Principles governing processing



2.C.1 Lawfulness of processing

In many jurisdictions, data protection instruments require that processing of personal data be carried out lawfully, meaning that the basis for processing must be one that is expressly sanctioned by law. This lawful requirement is sometimes articulated alongside requirements for transparency or fairness. For example, the EU's GDPR states:

> *Personal data shall be . . . processed lawfully, fairly and in a transparent manner in relation to the data subject;*

In some instruments, this lawfulness principle is articulated as a requirement that processing have a "lawful purpose" rather than a lawful basis (see Section 2.C.5 on purpose specification and limitation). For example, Malaysia's PDPA states:

> *Personal data shall not be processed unless . . . the personal data is processed for a lawful purpose directly related to an activity of the data controller;*

Similarly, Jamaica's DPA provides that personal data shall be processed fairly and lawfully;

Some instruments adopt both conventions. For example, Kenya's DPA states:

> *Every data controller or data processor shall ensure that personal data is . . . processed lawfully, fairly and in a transparent manner in relation to any data subject;*
>
> *[. . .]*
>
> *A data controller or data processor shall collect, store or use personal data for a purpose which is lawful, specific and explicitly defined.*

The requirement that a data controller have a lawful basis is viewed by some as unnecessarily restrictive. Some jurisdictions do not require the existence of a lawful basis for data processing, viewing it as an activity that organizations are at liberty to engage in subject to regulatory restrictions. For instance, California's Consumer Protection Act (CCPA) establishes various rights for consumers and applies various obligations to and restrictions on those responsible for data processing but does not require an affirmative legal basis to engage in processing in the first place.

Countries that do require a lawful basis usually set out a common set of bases for processing of personal data that would be considered lawful, which we explore below. Often, the law will provide that the data subject's consent to the processing is the primary lawful basis, in the absence of which there are several other lawful bases on which the controller may rely. The weakness of consent as a genuinely legitimate basis for processing has created doubt about the overall approach of requiring a lawful basis for processing.

2.C.2 Enumerated bases for lawful processing

Where a lawful basis for processing is required, a data controller may process personal only if the processing satisfies one of the lawful bases set out in the legislation. This requirement typically applies irrespective of whether the personal data is obtained from the data subject, a third party or from publicly available sources.

Consent

"Consent" stands out as a critical and unique basis for lawful processing of personal data, worthy of separate consideration. Many data protection instruments describe consent separately from the other enumerated bases, an indication of its special status.

Consent may be viewed as the ultimate exercise of autonomy by the individual, and requiring his or her consent might be thought to confer important individual rights, rebalancing power away from large data processors such as governments, internet companies and service providers. However, consent is not without controversy. Many commentators have questioned whether data subjects are ever effectively informed of what is happening to data about them when they give their consent. Few people actually read disclosures made by data controllers or truly understand the implications and risks of assenting to personal data processing. People disclose data about themselves to many parties and it is next to impossible to know how and to what ends such data will be transferred, aggregated and processed. It is also increasingly widely recognized that individuals give consent believing that the alternative is to forego the service that processes such data, i.e., they perceive themselves as not having any real choice. Some say that "consent is broken."

Consent as a legal basis for processing may then, counterintuitively, place an unfair burden on the individual if it opens the door and legitimizes unrestricted processing of personal data about them.

Given the weaknesses of the consent in legitimizing processing, the other principles of data protection that also apply are all the more important. These include data minimization, limits on data retention and transfer, fairness and transparency. Additionally, instead of continuing to rely on consent as a fundamental basis for legitimizing data processing, there may be a need to shift the burden to the organizations that carry out the data processing, giving them clear responsibilities as to the collection, use and transfer of personal data. These might include a duty to collect, use and transfer personal data only when it benefits the data subject, a duty to employ privacy-enhancing technologies, or a fiduciary obligation of loyalty to the interest of the data subject. Elements of these approaches are reflected in India's recent Digital Personal Data Protection Act, 2023.

Despite these critiques, consent remains the only basis for processing in which the data subject is expressly and voluntarily giving permission to the data controller to have personal data processed, and this remains a significant feature.

Consent is typically required to be given narrowly in relation to each specified purpose for data processing. Consent for one processing activity cannot necessarily be viewed as a blanket consent for all processing activities. For example, the EU's GDPR states:

> *Processing shall be lawful . . . if . . . the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*

Some data protection instruments define or otherwise create requirements for valid consent, typically requiring that consent be voluntary, freely given, and evidenced by an affirmative action. The last point importantly invalidates consent based on pre-checked boxes or default settings that a data subject must alter if he or she does wish to opt out. For example, Jamaica's DPA defines consent is as follows:

> *Consent […]*
>
> *(a) means 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;*
>
> *(b) includes any such expression of consent given by— (i) the legal personal representative of the data subject; (ii) any individual to whom the data subject delegates, in writing in such form and manner as may be prescribed, the right to give or withhold consent to the processing; (iii) in the case of a minor, (subject to section 5(a)(i)), a parent or legal guardian of the minor; or (iv) in the case of an individual who by reason of any mental impairment is unable to act, the person entitled to act for that individual under section 5(a)(ii); and*
>
> *(c) may be withdrawn in the same manner in which it may be given under paragraph (a).*

Kenya's DPA defines consent as follows:

> *'consent' means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject;*

Data protection instruments also typically provide data subjects with the ability to withdraw consent once it is given. For example, the EU's GDPR states:

> *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

Other common bases for processing

Data protection instruments typically enumerate several other bases for processing of personal data in the absence of consent of the data subject:

Necessary for performance of a contract

Data protection instruments typically permit data controllers to process personal data of a data subject when the processing is necessary for performance of a contract to which the data subject is a party. This basis often extends to processing to facilitate the consummation of a contract to which the data subject would be a part. For example, Malaysia's PDPA states:

> *. . . a data controller may process personal data about a data subject if the processing is necessary—*
>
> *(a) for the performance of a contract to which the data subject is a party;*
>
> *(b) for the taking of steps at the request of the data subject with a view to entering into a contract;*

Compliance with a legal obligation

Data protection instruments typically permit data controllers to process personal data of a data subject when the processing is necessary for compliance with a legal obligation to which the data controller is subject. For example, Kenya's DPA states:

> *A data controller or data processor shall not process personal data, unless . . . the processing is necessary . . . for compliance with any legal obligation to which the controller is subject;*

Protection of vital interests

Data protection instruments typically permit data controllers to process personal data of a data subject when necessary to protect an interest that is essential to his or her life, i.e. a "vital interest" and in some jurisdictions also the vital interest of a third party. For example, the EU's GDPR states:

> *Processing shall be lawful . . . if . . . processing is necessary in order to protect the vital interests of the data subject or of another natural person;*

Performance of a task in public interest

Data protection instruments typically permit data controllers to process personal data of a data subject when the processing is necessary for the performance of an official task in public interest carried out by a public authority, i.e., government activities. For example, South Africa's POPIA states:

> *Personal information may . . . be processed if . . . processing is necessary for the proper performance of a public law duty by a public body;*

Legitimate interests

Data protection instruments often permit data controllers to process personal data of a data subject if it is necessary to further the legitimate interests of the data controller or a third party. For example, South Africa's POPIA states:

> *Personal information may . . . be processed if . . . processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied . . .*

Other instruments expressly limit this basis by requiring that any "legitimate interests" be balanced against the fundamental rights of the data subject. For example, the EU's GDPR states:

> *Processing shall be lawful . . . if . . . processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child . . .*

Even with these express limitations, the concept of "legitimate interests" is vague and potentially vulnerable to abuse. Accordingly, guidance (whether in legislation or from a regulatory authority) is useful with respect to this basis for processing. While this is still an evolving concept, examples of "legitimate interests" are found in the recitals to the EU's GDPR include processing:

- when "the data subject is a client or in the service of the controller"
- when "controllers that are part of a group of undertakings or institutions affiliated to a central body" […] "transmit […] personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data;" and
- "to the extent strictly necessary and proportionate for the purposes of ensuring network and information security."

Some data protection laws require the controller to comply with specific conditions precedent to process personal data on the basis of legitimate interest. For example, Canada's Consumer's Privacy Protection Act states that:

Prior to collecting or using personal information under subsection (3), the organization must (a) identify any potential adverse effect on the individual that is likely to result from the collection or use; (b) identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them; and (c) comply with any prescribed requirements.

2.C.3 Specific bases for processing sensitive personal data

Data protection legislation often sets out a more limited, or even entirely separate, set of lawful bases relating to processing of sensitive personal data. For example, Kenya's DPA permits processing of sensitive personal data when "the processing relates to personal data which is manifestly made public by the data subject" or is necessary for "the establishment, exercise or defence of a legal claim."

Some laws make distinctions in the type of consent required for processing sensitive personal data. For example, both the EU's GDPR and Malaysia's PDPA include "explicit consent" as a basis for processing of sensitive personal data, while Jamaica's DPA requires that the consents need to be in writing. However, in practice, given that consent must typically be informed and unambiguous anyway, it is not always clear how this differs from the generic consent that is a basis for lawful processing of other personal data.

Some countries have particular requirements for particular types of data. For instance, Kenya's DPA also sets out limited bases for the processing of health data:

(1) Personal data relating to the health of a data subject may only be processed–

(a) by or under the responsibility of a health care provider; or

(b) by a person subject to the obligation of professional secrecy under any law.

(2) The condition under subsection (1) is met if the processing–

(a) is necessary for reasons of public interest in the area of public health; or

(b) is carried out by another person who in the circumstances owes a duty of confidentiality under any law.

Other countries restrict the communication or shared use of sensitive personal data, specifically health data, between data controllers, when the aim is obtaining economic advantage. For example, Brazil's LGPD states:

Communication or shared use between controllers of sensitive personal data referring to health in order to obtain an economic advantage is prohibited, except in hypotheses related to the provision of health services, pharmaceutical assistance and health insurance, as long as the paragraph 5 of this article is observed, including auxiliary diagnostic and therapeutic services, in benefit of the interests of the data subject and also to allow:

I - data portability of data when requested by the data subject; or

II - the financial and administrative transactions resulted from the use and provision of the services referred to in this paragraph.

2.C.4 Additional protections for children and others lacking legal capacity

Data protection instruments often set out additional protections for the processing of personal data of children and persons lacking the legal capacity to consent. These may require data controllers to obtain the consent of a child's parent or guardian, particularly when the lawful basis for processing is consent. For example, South Africa's POPIA states:

The prohibition on processing personal information of children, as referred to in section 34, does not apply if the processing is—

(a) carried out with the prior consent of a competent person;

(b) necessary for the establishment, exercise or defence of a right or obligation in law;

> *(c) necessary to comply with an obligation of international public law;*
>
> *(d) for historical, statistical or research purposes to the extent that—*
>
> *(i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or*
>
> *(ii) it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or*
>
> *(e) of personal information which has deliberately been made public by the child with the consent of a competent person.*

Kenya's DPA is even more restrictive, always requiring parental consent among other requirements:

> *(1) Every data controller or data processor shall not process personal data relating to a child unless–*
>
> *(a) consent is given by the child's parent or guardian; and*
>
> *(b) the processing is in such a manner that protects and advances the rights and best interests of the child.*
>
> *(2) A data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child.*

Brazil's LGPD emphasizes that personal data shall be processed in their best interest:

> *The processing of personal data belonging to children and adolescents shall be done in their best interest, pursuant to this article and specific legislation.*

Some jurisdictions seek to provide greater flexibility for children using internet services, recognizing that children are often active online. For instance, the EU's GDPR allows countries to accept the consent of children below 16 years old, with many countries treating consent of children of 13 years and above as valid, for the purposes of providing them with "information society services" (e.g., email and other messaging, social media, search, ecommerce). Some jurisdictions do not require parental consent to process personal data relating to a child for the purpose of the child obtaining online preventive or counselling services because this could be a barrier to a child seeking protection from parental abuse.

2.C.5 Purpose specification and limitation

In addition to requiring a lawful basis for processing, data protection instruments typically require that any collection of personal data be carried out for a specific and express purpose. This purpose must be "lawful" or "legitimate," and in most cases must be also disclosed to the data subject (see Section 2.C.8 on mandatory disclosures). To prevent "function creep," a term used to describe a situation where data originally collected for one purpose is used for other purposes, any further processing must also be within the scope of the original purpose for which it was collected, or if it is not strictly within the scope of the original purpose, then the further processing should not be "incompatible" with it. If that is not the case, then an independent lawful basis and lawful or legitimate purpose must be established. For example, Jamaica's DPA states:

> *personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with those purposes.*
>
> *[. . .]*

Similarly, South Africa's POPIA states:

> *Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.*
>
> *[. . .]*

Further processing of personal information must be in accordance or compatible with the purpose for which it was collected . . .

2.C.6 Data minimization

Once a lawful basis for processing has been determined and a lawful or legitimate purpose has been specified, data protection instruments typically require that processing of personal data, including their collection, be relevant to that purpose. This data minimization principle limits processing to only what is necessary. However, there are several subtle variations in how this is articulated.

For example, the APEC Privacy Framework states:

The collection of personal information should be limited to information that is relevant to the purposes of collection . . .

South Africa's POPIA takes this principle a step further, prohibiting processing that is "excessive":

Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

Many laws take this data minimization principle significantly further. While all irrelevant personal data processing should be unnecessary, some personal data processing may be relevant (and even not "excessive") but still not strictly necessary. Under a principle referred to as the "proportionality principle" or the "minimum necessary principle," many laws limit collection and other processing to the minimum extent necessary to achieve a specified purpose. For example, the EU's GDPR states:

Personal data shall be . . .adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed . . .

2.C.7 Data retention limitation

Data retention limitations are closely related to, and perhaps even an extension of, the data minimization principle. In general, these limitations require that personal data be retained by a data controller or data processor only for as long as they are needed to fulfil the specified purpose of the processing. This prevents unnecessary storage of personal data beyond its usefulness. Exceptions are typically made for legal or contractual obligations of the data controller or data processor to retain personal data, the data subject's consent to retention and, in some cases, journalistic, research and artistic purposes. For example, Kenya's DPA states:

A data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is–

(a) required or authorised by law;

(b) reasonably necessary for a lawful purpose;

(c) authorised or consented by the data subject; or

(d) for historical, statistical, journalistic literature and art or research purposes

2.C.8 Fairness, transparency and mandated disclosures

Data protection instruments typically require that data processing be fair and transparent. Many instruments set out fairness and transparency as a general requirement. For example, the EU's GDPR states:

Personal data shall be . . . processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

In addition to this general requirement, and often instead of it, many instruments set out specific mandatory disclosures that must be made to data subjects when their data is collected or subsequently processed for a new purpose. Some instruments require such disclosures to the data subject even if the personal data is obtained from a third party or from publicly available sources.

Where consent is the basis for personal data collection, such disclosures to the data subject, particularly regarding the nature of the personal data collected and the intended uses of such data, is essential for consent to be meaningful. Where no consent is required or obtained, such transparency can at least provide clear and accessible explanations to ensure public trust and prevent misconceptions.

These mandatory disclosures typically set out relevant information regarding processing such as the identity of the data controller, purpose for collection of personal data, third parties to whom it may be disclosed and individual rights available to the data subject (see Section 2.D regarding individual rights).

2.C.9 Data quality

Data protection instruments often require that data controllers actively maintain the quality of the personal data they are processing by ensuring that personal data are accurate, complete and up to date. For example, the OECD Privacy Guidelines state:

> *Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.*

South Jamaica's DPA similarly states:

> *Personal data shall be accurate and, where necessary, kept up to date.*

2.C.10 Accountability and data protection audits

The accountability principle is a cornerstone of data protection frameworks, requiring data controllers to take responsibility for ensuring that personal data is processed in compliance with relevant laws and regulations. Accountability can be expressed through several measures and internal data governance practices. A key method for ensuring accountability is the regular conduct of independent data protection audits, which help assess compliance, identify risks, and address any potential violations. In addition to audits, data controllers should implement robust data governance practices, maintain detailed records of processing activities, and conduct Data Protection Impact Assessments (DPIAs) for high-risk processing (see Section 2.E.3).

These mechanisms collectively reinforce a data controller's responsibility to protect personal data and maintain transparency in their operations, and actively demonstrate their compliance, all of which promotes trust. For example, EU's GDPR requires data controllers to maintain written documentation and overview of procedures by which personal data are processed. Records of processing activities must include significant information about data processing, including data categories, the group of data subjects, the purpose of the processing, and the data recipients. This must be made available to authorities upon request. Some countries authorize the data protection authority to carry out audits. For example, Kenya's DPA requires that:

> *The Data Commissioner may carry out periodical audits of the processes and systems of the data controllers or data processors to ensure compliance with this Act.*

Other frameworks mandate the appointment of a Data Protection Officer (DPO), whose role is to oversee and ensure compliance with the data protection regulations. This is often only required for controllers (and sometimes processors) that are engaged in large scale of processing personal data. The EU's GDPR requires them to appoint a DPO if they are public authorities, or are engaged in processing that involves large-scale, regular, and systematic monitoring of individuals (e.g., online behavior tracking), or special categories of personal data. Some countries have a general DPO requirement for all controllers. For example, Malaysia's revised PDPA states that:

> *A data controller shall appoint one or more data protection officers who shall be accountable to the data controller for the compliance with this Act.*

The DPO requirement is intended to ensure that someone has a clear, primary responsibility to ensure compliance, and that the data protection authority has a point person to contact for communications with the authority. We tend to find this unnecessary in small jurisdictions where organizations may be constrained for resources. Dedicating a senior position only to data protection may be excessive intervention

into internal organizations of entities that are one way or another responsible for compliance. Data protection authorities will also have ways to find out which entities are involved in significant scale of data processing.

2.C.11 Limitations on direct marketing activities or other commercial purposes

Data protection legislation often includes limitations on the ability of data controllers to use personal data to carry out direct marketing activities targeting the data subject. Some laws prohibit all direct marketing activities unless a data subject has expressly opted in. For example, South Africa's POPIA states:

> *The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject—*
>
> *(a) has given his, her or its consent to the processing; or*
>
> *(b) is, subject to [certain requirements], a customer of the responsible party.*

Other countries are less restrictive and frame these limitations as part of a right of a data subject to object (see Section 2.D.7 regarding the individual right to object). Other times affirmative action on the part of a data subject is necessary to trigger such limitations. For example, Malaysia's PDPA states:

> *A data subject may, at any time by notice in writing to a data controller, require the data controller at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing.*

Other countries take a broader approach and limit not just direct marketing but all "commercial activities" relating to the data subject. For example, Kenya's DPA states:

> *A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person–*
>
> *(a) has sought and obtained express consent from a data subject; or*
>
> *(b) is authorised to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.*

2.C.12 Privacy by design or default

The range of potential risks to privacy and security of data is as wide as the variety of types of processing is vast. Data protection laws cannot possibly address all of them. They thus establish general obligations to provide for privacy and security commensurate with risk. This requires them to consider the nature of the processing and the risks it may pose, and to plan accordingly.

Some data protection instruments require data controllers to implement "privacy by design" or "privacy by default" in their processing. These terms refer to the implementation of privacy measures and technologies in a data system that eliminates or reduces the collection of personal data and protects against processing that does not respect privacy. By embedding these measures and technologies directly into the architecture of the data system, data controllers can mitigate unnecessary or undesired processing of personal data without losing the functionality of the data system.

For example, the OECD Privacy Guidelines state:

> *A data controller should [h]ave in place a privacy management programme that:*
>
> *i. gives effect to these Guidelines for all personal data under its control;*
>
> *ii. is tailored to the structure, scale, volume and sensitivity of its operations;*
>
> *iii. provides for appropriate safeguards based on privacy risk assessment;*
>
> *iv. is integrated into its governance structure and establishes internal oversight mechanisms;*
>
> *v. includes plans for responding to inquiries and incidents;*

vi. is updated in light of ongoing monitoring and periodic assessment.

Similarly, the Kenya DPA states:

> *A data controller or data processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose is processed, taking into consideration–*
>
> *(a) the amount of personal data collected;*
>
> *(b) the extent of its processing;*
>
> *(c) the period of its storage;*
>
> *(d) its accessibility; and*
>
> *(e) the cost of processing data and the technologies and tools used*

As illustrated in these provisions, controllers and processors are typically expected to consider and make judgment calls in light of various factors when planning their data processing in order to ensure privacy and security of the data. One example of the planning of appropriate privacy measures relates to data scraping.

Data scraping involves the large-scale extraction of information, including personal data, from publicly accessible websites, online platforms, or digital services. It typically relies on automated tools, such as bots or scripts, to gather personal data including names, email addresses, photographs, contact details, user profiles, or social media activity, often without informing or obtaining permission from the individuals concerned. Scraping technologies become increasingly sophisticated and widely deployed, particularly to gather personal data for training AI models, and for data brokerage.

Some data protection authorities have drawn attention to this practice and provided guidance to data controllers as to their obligations under data protection laws.[3] Data controllers will typically be considered responsible for protecting personal data that they host, including on publicly available websites. They must protect such data from unlawful or excessive collection and any processing inconsistent with their original purpose. Therefore, data controllers who do not implement safeguarding tools and measures risk breaching their legal obligations.

Data controllers can implement a combination of technical and organizational measures to address the risk of data scraping. These protections can be integrated into the design and operation of systems and processes that process personal data.

- *Technical measures* include restricting access to personal data through tiered permission structures, monitoring systems for abnormal or high-frequency requests, and deploying tools such as robots.txt files or metadata configurations to discourage automated scraping. Data controllers can also use rate limiting, CAPTCHAs, advanced bot detection systems, IP address filtering, session-based access controls, and content obfuscation techniques to reduce the exposure and accessibility of personal data.
- *Organizational measures* include robust data access governance policies, conduct privacy impact assessments to identify and address scraping-related vulnerabilities, and provide regular training to relevant personnel on data protection risks.

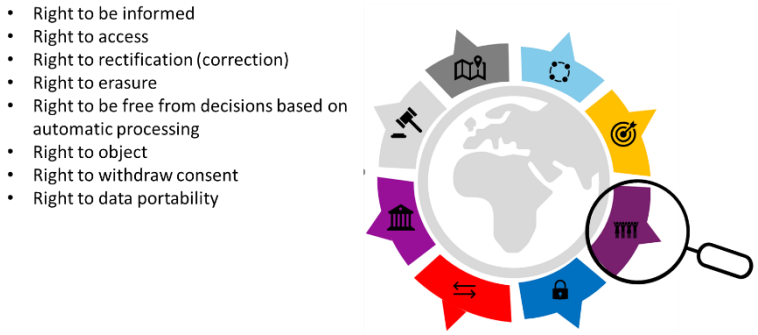
In parallel, data controllers have a duty to provide avenues through which data subjects can exercise meaningful control over their personal data. This includes offering clear options to limit the visibility of personal information, opt out of access by third parties, and understand the potential for their data to be reused for purposes beyond their original context.

[3] See for example Concluding joint statement on data scraping and the protection of privacy issued in 2024 by 16 data protection authorities.

2.D Individual rights concerning personal data

Data protection instruments generally include a suite of individual rights available to data subjects to exercise with respect to personal data held by data controllers. These rights give data subjects a degree of control over how their personal data are processed and a means of ensuring they are accurate and complete. In this subsection we describe the most common individual rights.

Figure 7. Individual rights



2.D.1 Right to know whether personal data are being processed

Data protection instruments typically provide data subjects with an individual right to ascertain whether a particular data controller is processing his or her personal data. For example, the EU's GDPR states:

> *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed . . .*

Similarly, South Africa's POPIA states:

> *A data subject, having provided adequate proof of identity, has the right to . . . request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject;*

2.D.2 Right to access and review personal data being processed

Data protection legislation typically provides data subjects with an individual right to access and review any personal data held by a particular data controller. This allows the data subject to receive a copy of the personal data which he or she may review and retain at no or a nominal cost. For example, the EU's GDPR states:

> *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data . . .*
>
> *[. . .]*
>
> *The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.*

However, other data protection instruments permit less robust access, allowing a data controller to provide a mere description or a record of the personal data rather than a full copy. For example, South Africa's POPIA states:

> *A data subject, having provided adequate proof of identity, has the right to . . . request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information—*
>
> *(i) within a reasonable time;*

(ii) at a prescribed fee, if any;

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable.

Some data protection legislation provides detailed information regarding the personal data retained by a data controller upon the payment of a prescribed fee. For example, Jamaica's DPA states:

> *[an individual is entitled] (c) upon payment of the prescribed fee— (i) to have communicated to that individual in an Intelligible form— (A) the information constituting any personal data of which the individual is the data subject; and (B) any information available to the data controller as to the source of those personal data;*

Data protection legislation also often sets out procedures and timeframes for making such requests and obtaining access, as well as exceptions when such access is not feasible or appropriate.

2.D.3 Right to rectify personal data

Data protection legislation typically provides data subjects with an individual right to have any inaccurate personal data held by a data controller rectified to make it accurate. The scope of such potential inaccuracies is often widely defined to include out-of-date, misleading and incomplete personal data. For example, Kenya's DPA states:

> *A data subject has a right . . . to correction of false or misleading data;*
>
> *[. . .]*
>
> *A data subject may request a data controller or data processor . . . to rectify without undue delay personal data in its possession or under its control that is inaccurate, out-dated, incomplete or misleading;*

Similarly, the EU's GDPR states:

> *The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.*

With the right to access and review personal data, data protection legislation often sets out procedures and timeframes for challenging the accuracy of personal data and requesting rectification, as well as exceptions when such rectification is not feasible or appropriate.

2.D.4 Right to have personal data deleted

Data protection legislation often, but not always, provides data subjects with an individual right to have personal data held by a data controller deleted. When included, this right is usually tightly circumscribed, allowing it to be exercised in limited circumstances. These may include when personal data was obtained unlawfully, the data controller no longer has a valid basis to retain the data, or retention of the data is no longer necessary to fulfill the original purpose for processing. However, there is a lot of variation among the valid circumstances for exercising such a right and no consensus practice has emerged. The EU's GDPR states:

> *The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:*
>
> *(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*
>
> *(b) the data subject withdraws consent on which the processing is based . . . and where there is no other legal ground for the processing;*

> *(c) the data subject [makes permitted objections to the processing];*
>
> *(d) the personal data have been unlawfully processed;*
>
> *(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;*
>
> *(f) the personal data have been collected in relation to the offer of information society services [to a child].*

Kenya's DPA states:

> *A data subject has a right . . . to deletion of false or misleading data about them;*
>
> *[. . .]*
>
> *A data subject may request a data controller or data processor . . . to erase or destroy without undue delay personal data that the data controller or data processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.*

In some cases, this right is combined with the right to rectification, permitting the data subject to either rectify or have the personal data deleted. For example, South Africa's POPIA states:

> *A data subject may, in the prescribed manner, request a responsible party to–*
>
> *(a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.*
>
> *(b) destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain in terms of [records retention limitations].*

2.D.5 Right to port data to another data controller

Data portability refers to the ability to easily move, copy or transfer personal data about an individual from one technological environment to another. Data protection legislation sometimes, but not always, provides data subjects with an individual right to have personal data held by one data controller to be ported to another data controller. This is intended to empower the data subject to be able to switch providers, and is partly driven by competition policy goals. In the commercial context, portability reduces the risk that a data subject is locked into the services a single provider by virtue of the provider having accumulated useful or necessary personal data.

There are two mechanisms by which a data subject can exercise this right. First, a data subject may have the right to receive personal data in a commonly used format, allowing the data subject to transfer the personal data to another data controller. Second, a data subject may have the right to direct a data controller to directly transfer personal data to another data controller, if technically feasible. For example, Kenya's DPA states:

> *(1) A data subject has the right to receive personal data concerning them in a structured, commonly used and machine-readable format.*
>
> *(2) A data subject has the right to transmit the data obtained under sub-section (1), to another data controller or data processor without any hindrance.*
>
> *(3) Where technically possible, the data subject shall have the right to have the personal data transmitted directly from one data controller or processor to another.*

However, not all jurisdictions include data portability rights. Establishing the processes and infrastructure required for porting personal data creates implementation challenges and costs. These may create significant economic burdens for businesses. Companies, particularly smaller ones, would often need to invest in upgrading their systems to ensure secure and interoperable data transfers, potentially diverting resources from core operations and discouraging innovation, especially for startups and small businesses. In addition, a firm may have already invested significantly to attract customers, develop a relationship and

knowledge of the customer that represents economic value to the firm built from the investment. Some sectors may benefit more than others from portability where there are not other "stickiness" factors impeding the individual from switching providers. For these reasons, we tend to take the view, especially in smaller countries with lower resources, that it would be prudent to verify that the anticipated likely usage of portability and the anticipated likely benefit of it to the individual and the market are proportionate to the burden of the obligation before imposing it. This can be achieved by authorizing the data protection authority to issue regulations on data portability rather than establishing data portability as an immediately applicable data subject right within the data protection legislation itself. For example, Nigeria's DPA states that:

> *The Commission may make regulations establishing a right of personal data portability.*

2.D.6 Right not to be subject to decisions based on automated processing

As more personal data processing incorporates automatic elements to generate decisions, computer algorithms to sort, analyze and make decisions about data subjects. With the rise of machine learning and artificial intelligence, many of these algorithms are themselves generated by computers, making these mechanisms and preferences unknowable to individuals. There are several risks inherent in the use of these algorithms, including:

- The decisions may be made based on erroneous, or out-of-data personal data.
- No algorithms are perfect, and a decision may reflect an inherent error in the algorithm itself.
- The algorithm may be generating the decision based on data that historically reflects imbalances across society, resulting in discrimination effectively (if indirectly) based on as race, ethnicity, religion or gender (known as "profiling"). In some cases, such decisions might not be permitted by law if the decision were made by a person.

For these reasons, data protection legislation often provides data subjects with an individual right not to be subject to decisions based on automated processing of personal data that result in legal consequences for the data subject. This right is typically articulated to specifically include profiling as an example of such automated decisions, and some instruments limit this right to profiling activities. Exceptions to this right typically include such decisions taken with the data subject's consent, when such decisions are necessary for execution of a contractual obligation of the data controller, or where authorized by law. For example, Kenya's DPA states:

> *(1) Every data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject.*
>
> *(2) Sub-section (1) shall not apply where the decision is–*
>
> *(a) necessary for entering into, or performing, a contract between the data subject and a data controller;*
>
> *(b) authorized by a law to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or*
>
> *(c) based on the data subject's consent.*

Jamaica's DPA states:

> *(2) An individual is entitled at any time, by notice in writing to the data controller, to require the data controller to ensure that no decision to which this section applies is based solely on the processing, by automatic means, of personal data in respect of the data subject for the purpose of evaluating matters relating to the data subject (for example, the individual's performance at work, creditworthiness, reliability, or conduct).*
>
> *(3) In any case where a data controller who has not received a notice under subsection (2) in respect of an individual takes a decision to which this section applies— (a) the data controller shall, as soon as is reasonably practicable, inform the individual that the decision was made on the basis*

described in subsection (2); and (b) the individual is entitled to, within thirty days after receiving the information under paragraph (a), by notice in writing require the data controller to reconsider the decision or make a new decision otherwise than on that basis.

South Africa's POPIA states:

(1) Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.

(2) The provisions of subsection (1) do not apply if the decision—

(a) has been taken in connection with the conclusion or execution of a contract, and—

(i) the request of the data subject in terms of the contract has been met; or

(ii) appropriate measures have been taken to protect the data subject's legitimate interests; or

(b) is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

2.D.7 Right to object to processing of personal data

Many data protection instruments provide data subjects with an individual right to object to the processing of personal data. When such an objection is validly made, the data controller will typically need to cease any such processing. The right to object will typically only apply in very specific conditions, and these conditions vary widely across data protection instruments.

Some instruments, such as the EU's GDPR and South Africa's POPIA, include a right to object to processing for the purposes of direct marketing (see Section 2.C.11 regarding limitations on direct marketing). Others, such as the EU's GDPR and South Africa's POPIA, limit some objections to situations where the processing is based on specific lawful bases, such as the "legitimate interests" of the data subject or a third party or a "public interest" basis. Still others, such as Malaysia's PDPA, require a showing of distress or damage or a violation of other rights of the data subject.

This right is often framed very broadly but allows the data controller to overcome the objection. For example, the EU's GDPR states:

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on ['public interest' or 'legitimate interest' bases], including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims

Similarly, Kenya's DPA states:

A data subject has a right . . . to object to the processing of all or part of their personal data;

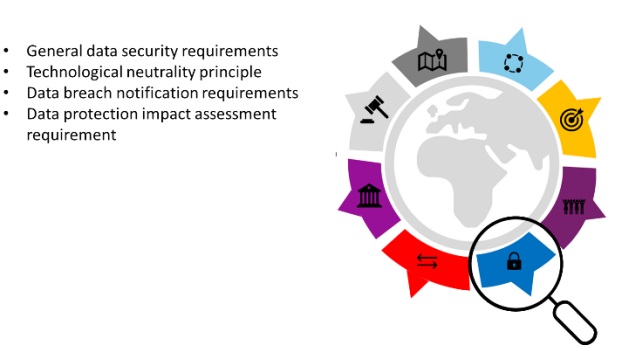
[. . .]

A data subject has a right to object to the processing of their personal data, unless the data controller or data processor demonstrates compelling legitimate interest for the processing which overrides the data subject's interests, or for the establishment, exercise or defence of a legal claim

2.E Data security

A critical aspect of data protection is the security of personal data held by controllers and processors. Data security is an essential element in the protection of privacy, but is also an end in itself to prevent other potential harms from misuse of information. Threats to personal data are wide-ranging, including unauthorized access or disclosures by hackers, accidental disclosures due to human or technical error, loss of data from natural or man-made disasters or loss of data integrity from viruses or technical failures. Ultimately, it is impossible to render a complex computerized system that is connected with others completely immune to threats. However, controllers and processors can implement technical and administrative processes and safeguards to mitigate these threats to personal data and further mitigate the harm caused when breaches occur.

Figure 8. Data security



2.E.1 General data security requirements

Data protection legislation typically requires data controllers to adhere to general data security requirements. These requirements are usually not detailed, technical prescriptions, but rather a reflection of general measures that data controllers and processors must adopt, often in proportion to their size or nature, scope and scale of personal data being processed.

In some laws, data security requirements are stated only as a general principle. For example, the OECD Privacy Guidelines state:

> *Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.*

Many data protection laws set out the types of risks and measures that a data controller should consider. For example, the EU's GDPR states the following general principle:

> *Personal data shall be . . . processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (integrity and confidentiality').*
>
> *[...]*
>
> *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 organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *(a) the pseudonymization and encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.*

Similarly, Canada's Consumer Privacy Protection Act sets out a list of factors to consider for the appropriate implementation of data security measures:

> *In addition to the sensitivity of the information, the organization must, in establishing its security safeguards, take into account the quantity, distribution, format and method of storage of the information.*
>
> *Scope of security safeguards (3) The security safeguards must protect personal information against, among other things, loss, theft and unauthorized access, disclosure, copying, use and modification and must include reasonable measures to authenticate the identity of the individual to whom the personal information relates.*

While many laws, including the EU's GDPR, impose data security requirements directly on data processors, others instead impose an obligation on data controllers to ensure that data processors have met data security requirements, sometimes through contractual requirements. For example, Malaysia's PDPA states:

> *Where processing of personal data is carried out by a data processor on behalf of the data controller, the data controller shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, ensure that the data processor-*
>
> *(a) provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and*
>
> *(b) takes reasonable steps to ensure compliance with those measures.*

Similarly, South Africa's POPIA states:

> *A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the [required] security measures . . .*

2.E.2 Personal data breach notification requirements

Data protection legislation typically requires data controllers to notify a data protection authority or similar body when there is a breach of personal data. Further requirements to notify data subjects directly, where feasible, also generally arise when data subjects are likely to be significantly and negatively affected by the breach. There are a range of views about the usefulness and design of data breach notification requirements.

Data breach notifications serve at least two important purposes. One is to inform data subjects about vulnerabilities such as identity theft and fraud resulting from unlawful access to data about them. This is important, however, only to the extent that the data breach notification will have the effect of informing the individual and he or she will be able to act on it. Low thresholds for requiring breach notifications may result in notification fatigue, with individuals paying no attention to them. And where individuals cannot do much about the breach to reduce their risks, the utility of the notification to individuals may be weaker and limited to reputational impact (although reputational impact can of course be a significant incentive to organizations to invest in robust data security).

Data breach notifications may also serve to inform the data protection authority and cyber security authorities about the sorts of data breaches that are occurring, the kinds of vulnerabilities that organizations face, particular patterns among hackers, and the kinds of remedies that might usefully be deployed. They may even make it possible to introduce standards across a variety of organizations and even vertical sectors that would reduce the risk of data breaches across the economy. This regulator-informing function of data breaches can be particularly helpful in ensuring that the data protection authority is close to the facts. It also gives the data protection authority a view of the manner in which controllers and processors are or are not securing their system, and compliance with obligations to do so.

The benefit to data protection authorities of breach notifications depends on the good flow of data between organizations subject to data protection law and the data protection authority. This has implications for the extent of data breach notification requirements, including the threshold at which they should apply, and penalties that apply to noncompliance. For instance, where data breach notifications may reveal evidence

of an organization's lack of data security measures (that effectively permitted the breach), notification may effectively be self-incriminating. A low threshold for requiring notifications may then be counterproductive, as organizations may seek to conceal their own inadequate conduct that itself may have been a breach.

There is, then, a trade-off between the benefits of more breach notifications to data protection authorities and the risk that the more of them there are, the more the incentive to make them may be undermined. This may argue for requiring reporting only the more significant breaches to the data protection authority.

The OECD Privacy Guidelines capture the general principal:

> *A data controller should . . . [p]rovide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.*

Required breach notifications must generally be made promptly. The EU's GDPR sets a deadline of "72 hours after having become aware of [the breach]" for notification to the regulator and a notification "without undue delay" to data subjects when required. South Africa's POPIA requires both notifications, when applicable, "as soon as reasonably possible after the discovery of the [breach]." Jamaica's DPA requires data controllers to notify each data subject, whose personal data is affected by the breach upon "becoming aware of, or having reason to become aware of, the contravention or breach". The 72-hour period has become quite common in countries' laws.

Typically, data processors are only obligated to notify data controllers when a breach occurs in data systems under their control. The data controller is then responsible for notifications to the regulator and possibly the affected data subjects. For example, Kenya's DPA states:

> *Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller without delay and where reasonably practicable, within forty-eight hours of becoming aware of such breach.*

Some laws specify that notifications to the data protection authority must include specific information. For example, Brazil's LGDP required that:

> *The controller must communicate to the national authority and to the data subject the occurrence of a security incident that may create risk or relevant damage to the data subjects. §1 The communication shall be done in a reasonable time period, as defined by the national authority, and shall contain, at the very least:*
>
> *I – a description of the nature of the affected personal data;*
>
> *II – information on the data subjects involved;*
>
> *III – an indication of the technical and security measures used to protect the data, subject to commercial and industrial secrecy;*
>
> *IV – the risks related to the incident;*
>
> *V – the reasons for delay, in cases in which communication was not immediate; and*
>
> *VI – the measures that were or will be adopted to reverse or mitigate the effects of the damage.*

Additionally, Jamaica's DPA requires that data controllers notify the data protection authority *within seventy-two hours after becoming aware of the contravention or security breach (as the case may be).*

Some data protection laws also authorize the authority to require data controllers to publicize a personal data breach more broadly in certain circumstances. For example, South Africa's POPIA states:

> *The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.*

2.E.3 Mandatory Data Protection/Privacy Impact Assessments (DPIAs)

Some data protection instruments require data controllers to conduct mandatory DPIAs. Like the requirement to introduce technical and administrative measures to ensure data minimization (see Section 2.C.6), the requirement to carry out a DPIA seeks to go beyond a results-based approach to regulation. DPIAs are intended to ensure that organizations integrate data protection considerations into their product development, management, service delivery and customer relationship management systems.

DPIAs can be costly and there is a risk that they be carried out in a formulaic way that does not achieve the desired goal. Thus, we recommend avoiding using them in a manner that would just result in a compliance-focused 'tick-the-box' approach. It will be important to ensure that they involve careful consideration of material risk to data subjects, and result in genuine efforts to design and manage systems to mitigate or avoid such risks.

This will take careful effort, knowledge and understanding, and likely require close engagement with the data protection authority to ensure that such assessment processes are indeed worth the effort. Thus, we recommend that they be introduced step-by-step for larger organizations which can consult with the data protection authority in the process, and which will enable a learning process that can be disseminated over time across the wider economy of data controllers.

Where such an impact assessment indicates a high risk to the rights and freedoms of data subjects, we recommend the data controller be required to consult with the data protection authority prior to processing to ensure that it puts appropriate measures and safeguards in place. We recommend applying a threshold to such organizations based on the number of data subjects on which data will be collected, and introducing such requirement after a sunrise period of a few years that will allow the data protection authority to show such organizations the kind of process it expects them to engage in.

The EU's GDPR states:

> *Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data . . .*
>
> *[. . .]*
>
> *A data protection impact assessment . . . shall in particular be required in the case of:*
>
> > *(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*
> >
> > *(b) processing on a large scale of [sensitive personal data], or of personal data relating to criminal convictions and offences . . .; or*
> >
> > *(c) a systematic monitoring of a publicly accessible area on a large scale.*

Jamaica's DPA describes the nature of a DPIA as follows:

> *(3) The data protection impact assessment form prescribed under subsection (1) shall require at least the following information—*
>
> > *(a) a detailed description of the envisaged processing of the personal data and the purposes of the processing, specifying, where applicable, the legitimate interest pursued by the data controller;*
> >
> > *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
> >
> > *(c) an assessment of the risks to the rights and freedoms, of data subjects, referred to in subsection (5); and*

> *(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights and legitimate interests of data subjects and other persons concerned.*

If a DPIA indicates that the envisaged processing would result in a high risk, the data controller may need to consult with a data protection regulator. For example, Kenya's DPA states:

> *The data controller or data processor shall consult the Data Commissioner prior to the processing if a data protection impact assessment prepared under this section indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject.*

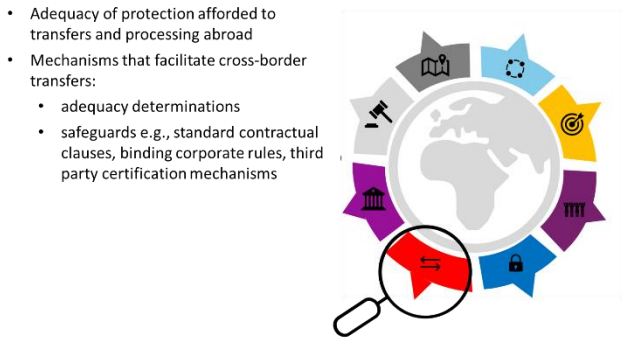
Trinidad and Tobago's Data Protection Act requires public bodies to prepare an impact assessment for certain types of activities described as:

> *[…]any proposed enactment, system, project, program or activity where such enactment, system, project, program or activity would or would reasonably be expected to substantially or materially impact personal information.*

2.F Cross-border transfers and processing of personal data

With the rise of the internet and cross-border digital and cloud services, populations in open societies have become accustomed to data moving seamlessly across political borders. However, the cross-border movement of personal data by data controllers and data processors raises data protection, privacy and sovereignty issues that have led many jurisdictions to place restrictions on such movement. This is an important area, as the benefits of using data for economic and social development will in many cases depend on the ability to transfer the data in and out of countries in the region to allow them to be processed abroad with other data from other countries and where there is sufficient computing capability.

Figure 9. Cross-border transfers and processing



2.F.1 Restrictions on extraterritorial transfers of personal data

Due to uncertainty regarding data protection standards in foreign jurisdictions and the difficulty of enforcing any measures abroad, data protection laws frequently limit extraterritorial transfer of personal data. The perceived risk is that if data are transferred abroad, they may not be subject to the same level of protection as is assured domestically. This risk is perceived to be all the more serious due to the ease of transferability of data. In some countries, the restrictions on transfer may be viewed as having a national security dimension, with concern at the risk of surveillance by other countries' governments. In other countries, such as India, some level of data nationalism and concerns about neo-colonialism may be in play as organizations from wealthier dominant economies have access to data about their citizens.

It is important for the development of the digital economy that restrictions on extraterritorial transfers of personal data do not undermine the vital importance of enabling such transfers in order to put the data to productive use. Any limitations should not be so restrictive that they stifle investment and innovation or participation of the population in the global digital ecosystem. It is thus important to avoid extensive administrative procedures to obtain the approval of the data protection authority for international transfers lest such processes or weak understanding or prejudices lead to delayed or poor decisions. Rather, robust safe harbours that allow cross-border transfers under specified conditions should apply.

Jurisdictions commonly limit extraterritorial transfers unless certain conditions that are intended to ensure the protection of the data when abroad are met. It is useful to think of these conditions in three baskets:

- approval of specified foreign jurisdictions as destinations for transfers;
- assurance of transfer-specific safeguards; and
- exceptions to or derogations from the general restriction.

We discuss each of these in turn.

2.F.2 Approval of foreign jurisdictions for transfers

Some data protection legislation provides for approval by a regulator, agency, Ministry or other government entity of a foreign jurisdiction that is considered to have adequate data protection standards, including laws, enforcement capability and restrictions on onward transfers to other jurisdictions. Typically, once a jurisdiction has been approved in this manner, all transfers of personal data to that jurisdiction are permitted, so long as the transfer otherwise complies with the requirements of the data protection law regarding processing. For example, the EU's GDPR includes procedures for jurisdiction-specific "adequacy decisions" by the Commission to enable extraterritorial transfers:

> *A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country . . . or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.*

However, in our experience, the assessment of the adequacy of a foreign country's laws is a potentially extensive, time-consuming and costly process. It should not be necessary to wait for the data protection authority to designate permitted destination jurisdictions for all transfers, although there may be a benefit to the data protection authority indicating from time to time those countries that do and do not have adequate laws. For these reasons, we tend to suggest that transfers be permitted if the third country provides adequate protection, but that this not depend on the data protection authority deciding this upfront.

2.F.3 Assurance of safeguards

As an alternative to jurisdiction-specific approvals, data protection laws often allow extraterritorial transfers to be made if safeguards are in place with respect to the transfer. These safeguards frequently include binding corporate rules within a group company or contractual commitments that include adequate data protection provisions.

For example, South Africa's POPIA states:

> *A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless . . . the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that—*
>
> *(i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and*
>
> *(ii) includes provisions that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country.*

Some laws provide parameters that shall be taken into consideration when assessing the level of data protection in a foreign country or international organization. For example, Brazil's LGPD states that the following elements shall be considered:

> *I – the general and sectorial rules of legislation in force in the receiving country or international organization;*
>
> *II – the nature of the data;*

> *III – the compliance with the general principles of personal data protection and data subjects' rights as provided in this Law;*
>
> *IV – the adoption of security measures as provided in regulation;*
>
> *V – the existence of judicial and institutional guarantees for respecting the rights concerning personal data protection; and*
>
> *VI – other specific circumstances relating to the transfer.*

Under some instruments, a data controller must provide proof of these safeguards to a regulator or other body before implementing the transfer. For example, Kenya's DPA states:

> *A data controller or data processor may transfer personal data to another country only where–*
>
> *(a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;*
>
> *(b) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws*

We do not tend to recommend requiring the controller to provide proof to the authority before making a transfer because this is impractical and may lead to significant delays impeding processing. Given the inherent difficulty of enforcing any data protection abroad, the data protection authority should, however, have clear powers to compel data controllers to report on the protections in place and basis on which cross-border transfers are made.

2.F.4 Exceptions or derogations from the general restriction

Even when the destination jurisdiction's laws are not adequate and there are not sufficient alternative safeguards, data protection legislation often includes exceptions or derogations from the general restriction on cross-border transfers. Such transfers are usually permitted when the data subject consents to the transfer, if the transfer is necessary to perform a contract between the data controller and the data subject or between the data subject and a third party, or if the transfer is necessary to protect the vital interests of the data subject, among other circumstances. These are similar to some of the lawful bases of processing (see Section 2.C.1). For example, the EU's GDPR states:

> *In the absence of an adequacy decision . . . or of appropriate safeguards . . . a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:*
>
> *(a) the data subject has explicitly consented to the proposed transfer . . .*
>
> *(b) the transfer is necessary for the performance of a contract between the data subject and the controller . . .*
>
> *(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;*
>
> *(d) the transfer is necessary for important reasons of public interest;*
>
> *(e) the transfer is necessary for the establishment, exercise or defence of legal claims;*
>
> *(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;*
>
> *(g) the transfer is made from a register. . . intended to provide information to the public . . .*

Similarly, South Africa's POPIA states:

> *A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless—*
>
> *[. . .]*

(b) the data subject consents to the transfer;

(c) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

(e) the transfer is for the benefit of the data subject, and—

(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

(ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

2.F.5 Enhanced requirements for sensitive personal data

Some data protection instruments include enhanced requirements for the extraterritorial transfer of sensitive personal data. For example, Kenya's DPA includes a range of exceptions and derogations from the general restriction on exterritorial transfers of personal data. However, these do not apply to extraterritorial transfers of *sensitive* personal data which must be based either on data subject consent or confirmation to the regulator of appropriate safeguards:

> *The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.*

We do not generally recommend this tighter approach for sensitive personal data because it adds complexity and is unnecessary: if the ordinary safeguards are in place and sufficient for personal data generally, they ought to suffice for sensitive personal data as well. At most, we would suggest that the data protection authority review the nature of such information from time to time and carry out a cost-benefit analysis of adding any additional restrictions to the transfer of such information. The difficulty of distinguishing sensitive from non-sensitive personal data and the utility of allowing all data to be aggregated and processed outside the country will often outweigh the perceived risks of doing so, particularly if the protections above are in place.

2.F.6 Personal data localization requirements

Although it is not common, some data protection laws require that personal data remain, and be stored on servers and in data centers located within the territory. Some countries alternatively require merely that a copy of the personal data remains within the territory, with other copies free to be transferred extraterritorially (subject to any restrictions on such transfers as discussed in the previous Sections).

In general, these requirements are viewed skeptically, as they have the potential to limit or prevent public sector providers and private sector from using data processing services abroad because only those service providers that rent processing capacity within the territory would be able to provide services. This can reduce the competitive options available, in particular the ability to access service providers and infrastructure that may be more secure, higher quality, more innovative and better priced. Data localization requirements can also prevent members of the population using a range of digital services abroad to the extent that the processing would be within the territorial scope of the law (see Section 2.B.3). Data localization requirements can also serve as a disincentive for investments in the jurisdiction by foreign technology companies. The only instrument included in our best practices review that included a potential data localization requirement is Kenya's DPA. While the instrument itself does not impose a localization requirement, it empowers the Cabinet Secretary to prescribe one:

> *The Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya.*

Where a data localization restriction is provided for, we would recommend curtailing its possible use to ensure that strictly only particular situations or grounds. A concern that may drive data localization policy is to ensure that data that is vital for the operation of public services (e.g., a national digital identification system or a social security database) will not be beyond the jurisdictional ability of the government to retake control of the data. However, in such cases, one can use contractual obligations requiring the processor abroad to deliver the data back into the country within a specified notice period and at a reasonable cost.

2.F.7 Regional cross-border frameworks for transfer of personal data

At a regional level, different organizations and unions of countries have adopted varying approaches to cross-border data transfers, based on their respective national and regional authority structures.

ASEAN Model Contractual Clauses

Established in 1967, the Association of Southeast Asian Nations (ASEAN) today comprises 10 Member States. The 2016 ASEAN Framework on Personal Data Protection is a voluntary, non-binding framework that sets out data protection principles, including on cross-border transfers.

In January 2021, ASEAN Digital Ministers approved Model Contractual Clauses (MCCs). These are a set of model contractual provisions that entities can incorporate in their legal arrangements for cross-border transfers between data controllers and data processors, and between data controllers.

Use of the MCCs is voluntary and other clauses or other mechanisms are still permitted. Entities can modify or adapt the MCCs as appropriate to the circumstances. Entities need to ensure that any additional member state legal requirements are also met.

The use of the MCCs is a light mechanism but does not provide effective assurance as to compliance with the applicable laws of the members. This still depends on verifying whether any member state has additional requirements.

APEC Cross-Border Privacy Rules

The APEC Cross-Border Privacy Rules go significantly further than ASEAN in setting up a system for cross-border transfers. The Asia-Pacific Economic Cooperation (APEC) is a regional economic forum composed of 21 member economies in the Asia-Pacific region. Recognizing the importance of the secure flow of personal data across borders to support digital trade and innovation, APEC members established the Cross-Border Privacy Rules (CBPR) system. It is a voluntary certification system for businesses in the region. It requires participating businesses to implement data privacy regulations and policies consistent with the APEC Privacy Framework. It provides a common set of standards for use by such businesses in order to bridge differing national privacy laws within the region. It thereby reduces barriers to the flow of information for trade and economic cooperation.

Under the CBPR, certified businesses located in participating countries can transfer personal data to certified businesses in other participating countries, provided they comply with the privacy protection principles outlined in the framework. Only businesses are eligible to participate, not governments or individuals. The domestic laws and regulations of each participating country continue to apply.

To participate in the CBPR system, a country must nominate at least one “accountability agent”. This agent is an independent third-party organization who must be approved by both the Joint Oversight Panel and APEC’s Electronic Commerce Steering Group, with the opportunity for economies to object.

In order for a business to be certified as CBPR-compliant, the business must complete a self-assessment of its data protection policies and practices using a CBPR questionnaire or other documents provided from the accountability agent. The completed assessment is then submitted to the accountability agent, who conducts an iterative review. Accountability agents allow businesses flexibility in how they meet the requirements of the CBPR, recognizing that different businesses have different challenges and capabilities. Once the business is found to be compliant with the CBPR by the accountability agent, it is considered certified, and its details are published in a public directory. This certification demonstrates the business’s commitment to protecting personal data and can enhance its reputation in the marketplace.

Enforcement of the CBPR requirements is primarily carried out by the accountability agents. If a certified business fails to comply with the CBPR requirements, individuals can file a complaint with their local accountability agent, which can then investigate and take enforcement action against the organization. In addition, domestic regulatory authorities serve as a backstop to ensure that organizations comply with the CBPR requirements.

EU framework

The EU framework, governed by the GDPR, goes significantly further in establishing harmonization and an effective zone for cross-border transfers of personal data. The EU's authority to regulate data privacy stems from its Treaty on the Functioning of the European Union, granting it the power to legislate on matters that affect the internal market and protect fundamental rights. Data privacy is recognized as a fundamental right under Article 8 of the Charter of Fundamental Rights of the EU, which specifically addresses the protection of personal data. This right is reinforced by the EU's commitment to ensuring the free flow of personal data between member states, while maintaining strong privacy protections. As a result, the GDPR acts as the primary legal tool for standardizing data protection across the EU, ensuring consistent and robust safeguards for personal data in all member states.

The GDPR, as a "Regulation", is directly applicable and binding across all EU member states from its date of application, meaning it takes effect automatically without needing to be adopted into national law. However, it allows countries also to enact national laws with some derogations from the GDPR. In some cases, this is because the EU is limited in its legislative authority in that it does not have authority to regulate, for example, national security or freedom of the press. In some areas, the GDPR simply left countries flexibility as to how they would legislate, for example in relation to processing personal data about children. The combination of GDPR and these national laws are enforceable by national data protection authorities. This structure ensures that data protection standards are applied with a reasonable level of uniformity throughout the EU, while allowing flexibility for some differences. The strong consistency among countries is key in facilitating cross-border data transfers within the EU. Since all EU member states are held to the same high data protection standards, personal data can flow freely between them without additional restrictions.

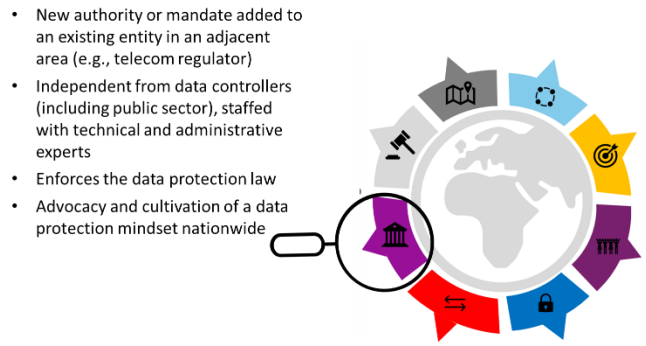
The mechanisms of coordination among national data protection authorities, and between them and the EU's regional authority (the European Data Protection Board, or EDPB) are key to the overall framework. GDPR provides, as do the respective national laws, for a "one-stop-shop" for regulatory supervision. The data protection authority of the country where a data controller or processor has its establishment has supervisory authority over cross-border processing by that controller or processor and is its sole interlocutor for such purpose. Data protection authorities in other member states must allow it to lead, although they are expected to cooperate in investigations and enforcement. If a case affects other member states (e.g., if the controller is processing personal data relating to data subjects in another member state), then the supervising authority must inform the data protection authorities of those other states of its planned decision. The other data protection authorities may make objections within a set timeframe. If the data authorities disagree, they may refer it to the EDPB for a binding decision.

2.G Institutions

2.G.1 Establishment or designation of a data protection authority

Data protection instruments typically establish a new entity or designate an existing entity to serve as a data protection authority or in a similar capacity. This entity may even be a single government official or a small body with several members. For simplicity, we refer to all such entities, individuals and bodies as a "data protection authority" or the "authority." The function of such an authority is to keep track of conduct in the country, monitoring and enforcing compliance and supporting the upholding of data subjects' rights.

Figure 10. Institutions



For example, the EU's GDPR states:

> *Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural in relation to processing and to facilitate the free flow of personal data within the Union (supervisory authority').*

Some data protection instruments merely set out the mechanism by which such an entity will be established. For example, Malaysia's PDPA's sets out the conditions for appointment of a Commissioner to fill such a role:

> *The Minister shall appoint any person as the 'Personal Data Protection Commissioner' for the purposes of carrying out the functions and powers assigned to the Commissioner under this Act on such terms and conditions as he thinks desirable.*

Similarly, New Zealand's DPA states that:

> *The Governor-General may, on the recommendation of the responsible Minister, appoint a Deputy Privacy Commissioner.*

Jurisdictions have organized their data protection authorities in various ways, depending on their available resources, the structure of other sectoral institutions, and overall governance frameworks. One approach is to create a standalone, independent authority, entirely separate from the Ministry, functioning as a distinct entity. A second option involves establishing an independent authority that, while separate from the relevant Ministry, operates within an existing statutory agency, such as a communications commission. The third option is to place the data protection office directly within the relevant Ministry, integrating it into the existing governmental structure.

2.G.2 Functions of a data protection authority

Data protection laws will often set out the functions and powers of the authority. Some of these are legal powers, and some of the functions are not. Some variation of the following will often be found in a data protection law:

- Activities that involve the exercise of legal powers:
  - hearing complaints, investigate noncompliance and make enforcement orders;
  - receiving breach notifications, audits and other required reports, and considering actions relating to them;

- where the law so authorizes, issuing legally binding regulatory instruments, whether these be regulations, directives, orders or others having direct legal effect (e.g., regarding cross-border transfers, and approving certification schemes); and
- exchanging information and coordinating the exercise (or not) of powers with other authorities outside or within the jurisdiction;

- Activities that do not require legal powers, such as:
  - issuing guidance to controllers, processors and data subjects on how types of data, types of processing, and processing in different sectors will be viewed by the authority;
  - carrying out promotion, awareness raising and training relating to data protection practices across the community of controllers, processors and data subjects; and
  - carrying out research, and developing and suggesting policy and new legislation to policymakers.

The complaints and investigation role are vitally important. Providing clear and accessible channels for individuals to file complaints and request investigations is fundamental for a data protection authority to enforce the law. This will also foster trust and accountability among organizations handling personal data. When individuals can easily report alleged data protection violations, it empowers them to safeguard their privacy rights and ensures that organizations remain vigilant in their data practices. Additionally, in many jurisdictions, data protection authorities are authorized to initiate investigations when they have reason to believe there may have been a violation even if there has been no complaint. This enhances their effectiveness by enabling proactive oversight and the ability to address systemic issues or emerging risks without waiting for external reports.

For example, Canada's Digital Charter implementation Act provides both:

> *[…]An individual may file with the Commissioner a written complaint against an organization for contravening Part 1.*
> *[…]If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Act, the Commissioner may initiate a complaint in respect of the matter.*

2.G.3 Independence of the data protection authority

Many data protection laws require that a data protection authority have independence from the political branches of government. The independence of an agency typically refers to independence from political or commercial control in performing its functions and exercising its powers, financial independence, and independent power to hire staff.

For example, South Africa's POPIA states:

> *There is hereby established a juristic person to be known as the Information Regulator, which—*
>
> *[. . .]*
>
> *(b) is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour or prejudice;*
>
> *[. . .]*
>
> *(d) is accountable to the National Assembly*

A similar position is adopted by New Zealand's DPA:

> *The Commissioner must act independently in performing statutory functions*
>
> *and duties, and exercising statutory powers, under—*
>
> *(a) this Act; and*
>
> *(b) any other Act that expressly provides for the functions, powers, or duties of the Commissioner (other than the Crown Entities Act 2004).*

The EU's GDPR sets out a more detailed set of factors required for independence:

> *(1) Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.*
>
> *(2) The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.*
>
> *[. . .]*
>
> *(5) Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.*
>
> *(6) Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.*

The overall goal of an independence requirement is to prevent an authority from being captured by political or commercial forces or agendas. Independence from the political organs of the State (such as ministries) can be particularly important because the State is almost always the controller in the country, having the largest amount and broadest range of personal data about the population. Because it is held by the State, which has strong powers over the population, it is all the more important to protect privacy and security of the data.

2.G.4 Funding of the data protection authority

Upon establishing or designating a data protection authority, a data protection instrument will typically set out how the authority will be funded. Funding is typically achieved through a combination of allocations made by the legislature and proceeds from fees or fines. For example, Malaysia's PDPA states:

> *(1) For the purposes of this Act, a fund to be known as the 'Personal Data Protection Fund' is established.*
>
> *(2) The Fund shall be controlled, maintained and operated by the Commissioner.*
>
> *(3) The Fund shall consist of—*
>
> *(a) such sums as may be provided by Parliament for the purposes of this Act from time to time;*
>
> *(b) fees, costs and any other charges imposed by or payable to the Commissioner under this Act . . .*
>
> *[. . .]*
>
> *The Fund may be expended for the following purposes:*
>
> *(a) paying any expenditure lawfully incurred by the Commissioner; . . .*
>
> *(c) paying the remuneration, allowances, benefits and other expenses of [personnel] . . .;*
>
> *[. . .]*
>
> *(f) generally, paying any expenses for carrying into effect the provisions of this Act.*

Similarly, Kenya's DPA states:

> *The funds and assets of the Office shall consist of–*
>
> *(a) monies allocated by the National Assembly for purposes of the Office;*
>
> *(b) any grants, gifts, donations or other endowments given to the Office; and*
>
> *(c) such funds as may vest in or accrue to the Office in the performance of its functions under this Act or any other written law.*

Also similarly, Brazil's LGDP states that:

> *Revenues from ANPD are: I - budget allocations, provided in the general budget of the Union, special credits, additional credits, transfers and payments that are conferred to it; II - donations, bequests, subsidies and other resources destined to it; III - amounts determined in the sale or lease of movable and immovable assets of its property; IV - amount calculated in financial market applications of the revenues provided in this article; V – (vetoed); VI - resources derived from agreements, contracts or similar instruments held with entities, bodies or companies, of either public or private law, national or international; VII - sums of the sale of publications, technical material, data and information, including for public bidding purposes.*

2.G.5 Registration requirements

Some data protection instruments require data controllers, and even data processors, to register with a data protection authority. Usually, this registration requirement only applies when certain thresholds are met, or processing involves particularly sensitive matters.

There can be advantages to a limited level of registration. It can allow the data protection authority to identify key organizations that have strategic importance in a country's digital economy and establish a regulatory relationship that would be useful in various ways. It can allow the authority more easily to identify leader organizations that would introduce and develop data protection practices, building a community of professionals that understand the issues and can share knowledge and understanding more broadly across the economy. It can facilitate enforcement, making it easier to identify those entities that should be prioritized for monitoring. The reputation of such registered organizations may also strengthen their incentives, whether vis-à-vis the public or just in the senior circles of the political and commercial spheres, to establish good data protection practices. Lastly, registration could be a means of raising funding for the data protection authority's activities through application of a registration fee.

However, as mentioned at the outset, we strongly favor avoiding unnecessary administrative processes. As explained in Section 2.A.4, any legal or natural person that collects, stores, sends, adapts or performs computing functions on any information about an individual for a purpose other than personal use, journalism and a few other purposes is engaged in processing personal data. Almost every micro and small and medium enterprise will process personal data of someone and thus be subject to the data protection law unless there are exclusions for small businesses. For this reason, it is highly impractical to require all data controllers or processors to register with the data protection authority. If this was required, it would have to devote all of its resources to registering all such controllers and processors without any benefit to doing so.

For this reason, if used at all, registration requirements should only apply to data controllers that exceed a specified, high threshold. This can refer to the important scale, wide scope and strategically significant nature of the personal data processed as well as the factors relating to the size of the data controller such as number of data subjects handled, and value of services rendered. These thresholds can be established by the data protection authority in an early round of regulations and revisited periodically.

For example, the proposed US APRA bill characterized certain data controllers as "large data holder":

> *The term "large data holder" means a covered entity or service provider that, in the most recent calendar year, had an annual gross revenue of not less than $250,000,000 and, subject to subparagraph (B), collected, processed, retained, or transferred—*
>
> *(i) the covered data of—*
>
> *(I) more than 5,000,000 individuals;*
>
> *(II) more than 15,000,000 portable connected devices that identify or are linked or reasonably linkable to 1 or more individuals; or*
>
> *(III) more than 35,000,000 connected devices that identify or are linked or reasonable linkable to 1 or more individuals; or*
>
> *(ii) the sensitive covered data of—*

> *(I) more than 200,000 individuals;*
>
> *(II) more than 300,000 portable connected devices that identify or are linked or reasonable linkable to 1 or more individuals; or*
>
> *(III) more than 700,000 connected devices that identify or are linked or reasonably linkable to 1 or more individuals.*

These entities would have stricter obligations, including publishing privacy policies from the past ten years and filing annual reports with the US Federal Trade Commission about their data handling practices.

Kenya's DPA sets out a mechanism to allow the Data Commissioner to establish thresholds for such mandatory registration:

> *(1) Subject to sub-section (2), no person shall act as a data controller or data processor unless registered with the Data Commissioner.*
>
> *(2) The Data Commissioner shall prescribe thresholds required for mandatory registration of data controllers and data processors, and in making such determination, the Data Commissioner shall consider-*
>
> *(a) the nature of industry;*
>
> *(b) the volumes of data processed;*
>
> *(c) whether sensitive personal data is being processed; and*
>
> *(d) any other criteria the Data Commissioner may specify.*

We would generally only consider registration to be advisable if there is strong confidence that it can apply only to a small number of key data controllers, and that it can be managed efficiently.

2.G.6 Appeals or judicial review

Data protection legislation typically permits data subjects, data controllers and data processors to appeal adverse decisions of the data protection authority. Occasionally, a data protection law establishes an *ad hoc* appeals body with full or quasi-judicial authority. However, more often than not the entity's recourse against the decision of a data protection authority (or an *ad hoc* appeals body) is under the typical judicial review process applicable to administrative agencies, i.e., to the relevant courts.

Malaysia's PDPA permits appeals to an Appeal Tribunal established under the PDPA, the judgments of which are to be enforced as a judgment of a court:

> *There is established an Appeal Tribunal for the purpose of reviewing any of the matters on appeal . . .*
>
> *[. . .]*
>
> *Any person who is aggrieved by the decision of the Commissioner under this Act relating to matters . . . may appeal to the Appeal Tribunal by filing a notice of appeal with the Appeal Tribunal.*
>
> *[. . .]*
>
> *A decision given by the Appeal Tribunal may, by leave of the Sessions Court, be enforced in the same manner as a judgment or order to the same effect, and where leave is so given, judgment may be entered in terms of the decision.*

Another structure providing accountability is identified in Jamaica's DPA, which provides for a Data Protection Oversight Committee to hold its Information Commissioner accountable to the public in the performance of their functions under their Act:

> *The Commissioner shall be subject to the oversight of the Data Protection Oversight Committee in accordance with Part II of the First Schedule.*

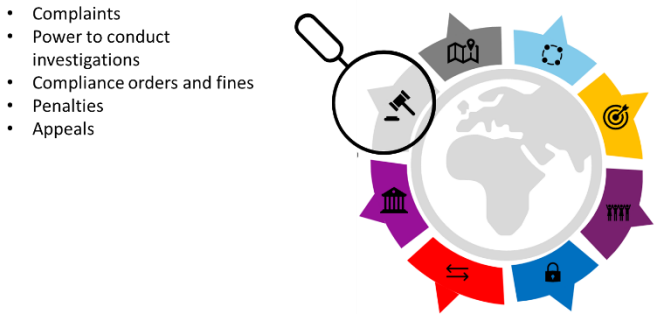
Regardless of whether a data protection authority's decisions are subject to appeals to administrative tribunals, boards, committees or other oversight mechanisms, the ultimate decision is in most jurisdictions (including Eastern Caribbean states) subject to a right of judicial review under general administrative law. This typically covers the lawfulness and the fairness of decisions. This typically includes assessing whether the data protection authority acted within its legal powers and complied with procedural requirements, such as providing notice to affected parties and giving them a genuine opportunity to be heard. It also typically examines whether the decision was necessary and proportionate to the objective pursued, and whether it respected key principles such as impartiality, non-discrimination, and legal certainty.

Judicial review thus operates as a layer of accountability and a legal check against the arbitrary exercise of administrative power, and is supported by international human rights frameworks[4]. It is reflected in many constitutional and legal systems around the world as a cornerstone of lawful and accountable governance.

2.H Enforcement

The effectiveness of a data protection law depends on the extent to which its obligations and safeguards are respected by data controllers and data processors. To uphold and enforce these legal requirements, data protection authorities are typically equipped with a range of enforcement powers that provide a structured and proportionate response to suspected violations.

Figure 11. Enforcement



Data protection authorities have enforcement powers to investigate apparent or alleged violations of data protection laws, and to address them where they find them to have occurred. When a data controller or data processor is found to have committed a serious or persistent breach of data protection obligations, a data protection authority may consider imposing penalties. These penalties give the regulatory instrument teeth and reinforce its deterrent effect. Penalties include administrative fines, civil remedies and criminal penalties.

2.H.1 Investigations

A data protection authority may conduct investigations to assess whether a data controller or data processor is acting in compliance with its legal obligations under the applicable data protection legislation. They may initiate an investigation upon receipt of a complaint, a data breach notification, intelligence gathered through monitoring activities, or on their own initiative (*ex officio*) where there are reasonable grounds to suspect non-compliance.

In the course of an investigation, a data protection authority may uncover potential violations and establish a procedural basis for any corrective or enforcement action. Investigations may involve information requests, data protection audits, document reviews, interviews with relevant personnel, forensic examinations of systems, and even physical inspections of premises. Where investigatory powers include

[4] Universal Declaration of Human Rights, Article 8: "Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law", United Nations General Assembly, Universal Declaration of Human Rights, 1948, GA Res 217A; Charter of Civil Society for the Caribbean Community, Article V: "All persons shall be equal before the law, be entitled to the equal protection of the law and to a fair and impartial hearing within a reasonable time", Caribbean Community (CARICOM), Charter of Civil Society for the Caribbean Community,1997; European Convention on Human Rights, Article 13: "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity", Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, , ETS No. 5.

access to premises, or other acts that may interfere with the rights and freedoms of individuals, data protection authorities must follow the necessary procedural safeguards under national law, such as the requirement to obtain prior judicial authorization.

2.H.2 Compliance and enforcement orders

A data protection authority will often have the power to issue compliance and enforcement orders to compel data controllers or processors to fulfill their obligations under the applicable data protection legislation. Compliance orders are generally issued to address or prevent ongoing or anticipated non-compliance. They may include warnings or reprimands directed at controllers or processors whose processing activities breach legal obligations, or directions requiring them to bring specific operations into compliance. Such orders may also obligate a controller or processor to comply with a data subject's request to exercise their rights within a specified timeframe and in a prescribed manner, or to notify affected individuals of a personal data breach.

Enforcement orders typically follow the conclusion of an investigation or arise from clear evidence of a confirmed breach. They may involve more restrictive or supervisory measures, such as compelling, suspending, or limiting certain processing activities, or requiring the implementation of additional safeguards and revisions to internal policies or practices. Orders must typically be proportionate to the nature and severity of the breach and must be issued in accordance with the procedural requirements established under national law.

2.H.3 Administrative fines

Many data protection laws empower the data protection authority to issue administrative fines for violations of obligations under the instrument. The legislation usually limits the amounts of these fines, articulated either as a monetary cap or a percentage of an undertaking's annual turnover (either domestic or worldwide) or both. For example, South Africa's POPIA states:

> *(1) If a responsible party is alleged to have committed an offence in terms of this Act, the Regulator may cause to be delivered by hand to that person (hereinafter referred to as the infringer) an infringement notice . . .*
>
> *(2) A notice referred to in subsection (1) must . . . specify the amount of the administrative fine payable, which amount may, subject to subsection (10), not exceed R10 million . . .*

Similarly, Kenya's DPA states:

> *In relation to an infringement of a provision of this Act, the maximum amount of the penalty that may be imposed by the Data Commissioner in a penalty notice is up to five million shillings, or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, whichever is lower.*

There is no widely accepted best practice with respect to administrative penalties for violations of personal data protection and privacy obligations, except that they should be sufficient to incentivize compliance.

2.H.4 Civil remedies

Many data protection instruments permit individuals to bring direct civil claims in domestic courts against data controllers and data processors to require them to respect their data subject rights and, in the case of violations, to pay damages. For example, the EU's GDPR states:

> *(1) Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.*

> *(2) Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically.*
>
> *[. . .]*
>
> *(6) Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State . . .*

Similarly, South Africa's POPIA states:

> *(1) A data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act . . . whether or not there is intent or negligence on the part of the responsible party.*
>
> *[. . .]*
>
> *(3) A court hearing proceedings in terms of subsection (1) may award an amount that is just and equitable, including—*
>
> > *(a) payment of damages as compensation for patrimonial and non-patrimonial loss suffered by a data subject as a result of breach of the provisions of this Act;*
> >
> > *(b) aggravated damages, in a sum determined in the discretion of the Court;*
> >
> > *(c) interest; and*
> >
> > *(d) costs of suit on such scale as may be determined by the Court.*

In addition, the proposed US APRA bill included a private right of action, allowing individuals to sue under many, but not all, of its operative provisions.

2.H.1 Criminal penalties

Some data protection instruments set out criminal penalties for violation of obligations imposed on data controllers and data processors. Most commonly these penalties are imposed when an entity contravenes requirements relating to processing of personal data or fails to comply with the decision or directive of a data protection authority requiring an entity to take or refrain from specific actions. Criminal penalties may consist of fines and/or imprisonment.

For example, Malaysia's PDPA states:

> *A data controller who contravenes [compliance with the Personal Data Protection Principles] commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.*
>
> *[. . .]*
>
> *A person who fails to comply with an enforcement notice [issued by the Commissioner] commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.*

Similarly, South Africa's POPIA states:

> *A data controller who contravenes the provisions [setting out the lawful bases for processing] commits an offence.*
>
> *[. . .]*
>
> *Any person who, without reasonable excuse, fails to comply with an enforcement notice commits an offence and is liable on conviction to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.*
>
> *[. . .]*

> *A person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall, on conviction, be liable to a fine not exceeding three million shillings or to an imprisonment term not exceeding ten years, or to both.*

Kenya's DPA also states:

> *A data controller who contravenes the provisions [setting out the lawful bases for processing] commits an offence.*
>
> *[. . .]*
>
> *Any person who, without reasonable excuse, fails to comply with an enforcement notice commits an offence and is liable on conviction to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.*
>
> *[. . .]*
>
> *A person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall, on conviction, be liable to a fine not exceeding three million shillings or to an imprisonment term not exceeding ten years, or to both.*

The given rationale, in our experience, for criminalizing breaches of data protection law in the countries that do so is typically that only when criminal penalties, including imprisonment, are threatened will actors take real notice of them. We do not find this to be a compelling reason to criminalize such conduct. It is foreseeable that almost every micro, small and medium enterprise and many sole proprietors will be data controllers. It is foreseeable that many will take time before they comply with the new data protection legislation. However, this is no reason to criminalize a failure to keep data secure, the collection of more data than is strictly needed for a given purpose, a failure to make breach notification. These are matters more naturally treated under general regulation and not criminal law.

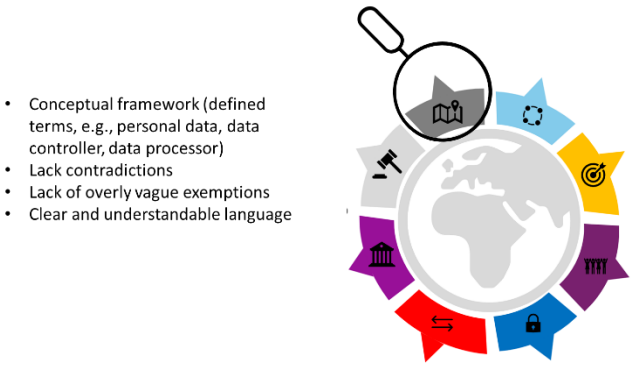
Imposing criminal liability for violations of data protection laws is generally not advisable as an international good practice, due to the potential for abuse and overreach. Criminal penalties, if applied broadly or inappropriately, can lead to disproportionate consequences for non-intentional or technical breaches. Criminalizing data protection violations risks creating a punitive environment that stifles compliance efforts, as businesses may become overly cautious, diverting resources towards legal defenses instead of improving data protection practices. Moreover, the threat of criminal prosecution can discourage cooperation with regulatory authorities, as entities might be less inclined to report violations or vulnerabilities that could expose them to criminal liability.

In this context, criminal penalties can become a blunt instrument, misused to target minor infractions rather than addressing serious violations. Instead, these penalties are better reserved for cases involving intentional, malicious activities that cause significant harm, such as hacking, data theft, or fraud. For example, under the United States' Computer Fraud and Abuse Act (CFAA), criminal sanctions are applied to unauthorized access to computer systems with malicious intent, reflecting the severity of deliberate cybercrimes. Similarly, the European Union's Directive on Attacks Against Information Systems imposes criminal penalties for attacks that intentionally disrupt or compromise critical data systems, underscoring the importance of reserving criminal liability for actions that undermine the integrity of data security.

2.I Summary of the elements of a data protection framework

In our international good practices review we identified several key elements that contribute to the effectiveness and robustness of data protection law. Regardless of cultural or country-specific requirements, there is an expectation that any new or revised legislation will align with these international best practices and include the following types of provisions. We summarize the main elements below.

Figure 12. Summary of general elements



2.I.1 Scope of applicability

- Establishment of a comprehensive general data protection law that applies broadly across the economy and explicitly addresses data protection by private entities but applying in whole or part only after an appropriate grace period.
- The law's geographic scope of application, requiring a connection between the controller, processor, or processing activities and the country.
- Exclusions of certain processing, processing of personal data for personal, recreational, household purposes, or for security, law enforcement, or public health objectives.

2.I.2 General elements of data protection law

- Limitation of exceptions applying to processing by public authorities to such exceptions as are necessary and proportionate, or subject to a similar, clear assessment (i.e., the legislation largely or fully applies to public authorities).
- Definitions of key data protection terms, including "personal data", "processing", "controller" (the entity that determines the means and purposes of processing), "processor" (the entity that processes personal data on behalf of a controller), and "data subject" (the individual whose personal data is processed).
- Requirement for a controller or processor to have a lawful basis for collecting or process personal data, such as:
    - consent provided by the data subject;
    - performance of a contract to which the data subject is a party;
    - necessity to comply with a legal obligation;
    - necessity to protect a vital interest;
    - necessity for the compliance with a legal obligation or interest of the controller or a third party;
    - necessity for the protection of a public interest; and
    - legitimate interests pursued by the controller or a third party.

2.I.3 Principles governing processing of personal data

Principles governing the processing of personal data, which require that data controllers or processors to:

- process only the minimum amount of personal data necessary for the specified purpose;
- retain personal data for a defined and limited timeframe;
- ensure fairness and transparency in processing;
- avoid processing personal data for purposes incompatible with those for which it was initially collected;
- make mandatory disclosures to data subjects; and
- maintain personal data that is accurate and up to date (data quality).

2.I.4 Individual rights concerning personal data

- Right to access and obtain copies of personal data;
- Right to request the correction of any inaccurate information;
- Right to object to data processing in specific circumstances;
- Right to request erasure of data, subject to conditions and exemptions, if it is no longer needed for the original purpose;
- Right to withdraw consent under certain conditions; and
- Right to request the direct transmission of personal data from one provider to another (data portability).

2.I.5 Data security

- Requirement for controllers and processors to implement appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of personal data under their control, including protection against accidental or unlawful destruction, loss, misuse, alteration, unauthorized disclosure, or access.
- Obligation for controllers to report any personal data breaches to the relevant authorities, and in certain cases, to the affected data subjects.
- Requirement for controllers to conduct a data privacy impact assessment when processing activities are likely to pose a high risk to the rights and freedoms of data subjects, and to implement measures to mitigate this risk.

2.I.6 Cross-border data transfers of personal data

- Establishment of clear rules regarding cross-border data transfers, including realistically achievable conditions under which personal data may be transferred abroad, including:
    - decisions on the adequacy of the destination jurisdiction's laws;
    - accountability measures;
    - binding corporate rules;
    - standard contractual clauses;
    - consent from the individual whose personal data is being transferred; and
    - government authorization.
- Absence of general restrictions on cross-border transfers of personal data or categories of personal data (data localization).

2.I.7 Institutions

- Establishment of a data protection authority or designation of an existing agency to regulate and monitor data protection and oversee the implementation of and be responsible for the enforcement of the law. Establishment of administrative processes relating to the institution's data protection duties, functions and powers.
- Ensuring that the data protection authority or other institution designated in that role:
    - has a reasonable degree of independence in the exercise of its powers;
    - has sufficient legal powers to carry out its duties, which may include setting and charging fees (if applicable), conducting investigations, implementing remedies and resolving disputes, among other things; and
    - has an appropriate level of distance from day-to-day political influence through the institution's governance structure and sources of funding (grants, fees, donor funding, etc.).
- "Forward-looking" provisions with respect to the regulation of new technologies such as facial recognition and artificial intelligence that might have a profound effect on data protection in the future. These might be included as substantive topics to be studied by the appropriate institution and implemented later through regulations or rules.

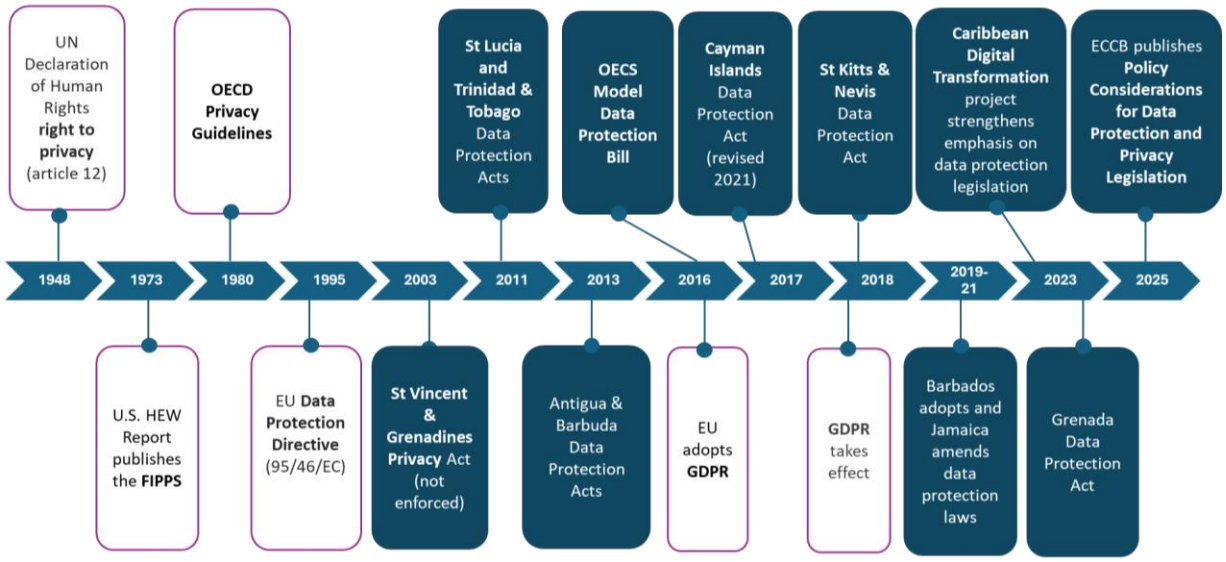
2.I.8 Penalties and enforcement

- Set up of enforcement and recourse mechanisms, allowing an individual who is aggrieved by the decision, action or inaction of a controller or processor to have the opportunity to lodge a complaint with a designated institution which could initiate an investigation on its own initiative or upon reference by the data subject.
- Provisions allowing a prosecutor or attorney general to bring criminal or civil actions, provide for alternative dispute mechanisms between data subjects and controllers, utilize the powers of an existing ombudsman or similar institution to enforce data subject rights, or allow third parties to act on behalf of groups of data subjects.

3 Legal and regulatory review of regional instruments

Having described good international practice in Section 2, we turn to our review of the legislation in the region. We start with regional legislation because many national data protection laws were based on the regional OECS Model Data Protection Act of 2016 ("OECS Model Bill"). Assessing this first enables us to refer to it when later assessing the national data protection laws.

Figure 13. Evolution of Caribbean data protection laws in context



3.A Data protection

This section reviews the OECS Model Bill and the ECCU's Policy Considerations for the Development of Data Protection and Privacy Legislation in the Eastern Caribbean Currency Union with a view to their substantive alignment with international good practice, as well as their role in developing a harmonized legal and regulatory data protection framework in the ECCU region.

3.A.1 OECS Model Bill

The OECS Model Bill was prepared as a model data protection law that OECS member states were intended to legislate into law at the national level.

The OECS Model Bill appears to borrow heavily from the Malaysia Personal Data Protection Act 2010 (PDPA), with many provisions copied nearly verbatim.

International practice in data protection law has evolved significantly since the OECS Model Bill's publication in 2016, and even more so since the Malaysian 2010 Act, particularly with the introduction of the European Union's General Data Protection Regulation (GDPR) and similar legislation in many countries. The observations below highlight provisions in the OECS Model Bill that do not align well with international good practice today.

Scope of applicability

Applicability limited to "commercial transactions"

As mentioned, much of the OECS Model Bill was based on the Malaysian PDPA of 2010 (the PDPA was subsequently amended in 2024). Malaysia's 2010 PDPA expressly excluded application to the Government of Malaysia and only applied to commercial transactions by the private sector. By contrast, the OECS Model Bill was meant to apply to both "public bodies and private bodies" (§3). However, the reliance on the borrowed language from the Malaysia PDPA, that took a different approach, led to some inconsistencies in the OECS Model Bill.

For example, the definition of "*personal data*" in the OECS Model Bill, which adopted the Malaysia PDPA definition verbatim, limits the scope of personal data to information "*in respect of commercial transactions*":

> *"personal data" means any information in respect of commercial transactions, which–*

> *(a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;*
>
> *(b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or*
>
> *(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,*
>
> *that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject;*

This definition excludes any information that is not "*in respect of commercial transactions*." This would likely exclude personal data collected by public bodies and processed for government administration, public policy, research, and scientific operations, as well as situations where personal data is collected by a government entity and subsequently shared with a private sector entity that is not engaged in "*commercial transactions*." For instance, this could involve a payment processor responsible for distributing government subsidies to designated recipients, thereby leaving critical data processing activities outside the scope of the OECS Model Bill.

In addition, ection 4(1) of the OECS Model Bill limits its application to private bodies to include only such private bodies that are conducting commercial transactions (this particular limitation would not apply to public bodies, though the issue with the definition of "personal data" described above remains):

> *With respect to a private body this Act applies to a person who processes or who has control over or authorizes the processing of any personal data in respect of commercial transactions.*

Alignment with good international practice would require removing the limitation to "commercial transactions" from the definition of "personal data" as well as the provision on applicability to private bodies.

Broad exemption for processing by regulatory authorities

Section 21(2)(e) exempts from several of the data protection principles and requirements any personal data that is processed for the purpose of discharging regulatory functions:

> *[Personal data] processed for the purpose of discharging regulatory functions shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act if the application of those provisions to the personal data would be likely to prejudice the proper discharge of those functions*

This provision allows regulatory bodies to process personal data without following some of the standard data protection requirements when doing so is necessary to ensure they can fulfil their responsibilities properly and efficiently. This exemption is overly broad and may apply to any regulatory body tasked with processing personal data, such as tax authorities, and financial regulators.

Alignment with good international practice would involve ensuring that only certain regulatory authorities that process substantial amounts of personal data from exemptions related to regulatory functions. This ensures that their data processing activities remain fully subject to the OECS Model Bill's comprehensive data protection standards, thereby safeguarding personal data based on the privacy and data protection principles.

General elements of data protection law

Definition of "personal data" is potentially limiting

Beyond the reference to "commercial transactions" described immediately above, the definition of "personal data" is potentially limiting for additional reasons. To qualify as personal data, information must meet at least one of three conditions:

> *(a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;*
>
> *(b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or*
>
> *(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.*

Conditions (a) and (b) require the involvement of "equipment operating automatically." Condition (c) requires the information to be "recorded." Neither of these two concepts is defined and their meaning is not intuitive. Their inclusion creates unnecessary complexity that serves as a potential barrier for applicability of the OECS Model Bill to processing by entities receiving personal data form the system or serving as relying parties.

Alignment with good international practice would involve simplifying the definition of "personal data" by removing the terms "recorded" and "equipment operating automatically," and revisiting the three conditions to ensure they do not create barriers to its applicability. Additionally, it would be better to refrain from an exhaustive list of specific identifiers, allowing for flexibility to include additional relevant identifiers or elements as they emerge in the future.

Anonymisation

The concept of anonymization is not addressed in the OECS Model Bill. It would be helpful if the legislation were to clarify that when data is "anonymized", it will no longer constitute personal data. While anonymization is clearly not a perfect means of protecting privacy, its flaws and the risks involved need to be balanced against the utility of allowing large sets of personal data to be put to use. It would also be better if the legislation required the data protection authority to periodically revisit the technical mechanisms for protecting personal data and issue guidance on what processes are sufficient to remove a set of data from the definition of "personal data." This issue will require ongoing, in-depth technical analysis in an evolving landscape.

Definition of "sensitive personal data" excludes important attributes

The OECS Model Bill defines "sensitive personal data" as follows:

> *sensitive personal data" means any personal data consisting of information as to the physical or mental health or condition of a data subject, his or her sexual orientation, his or her political opinions, his or her religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him or her of any offence or any other personal data as the Minister may determine by order published in the Gazette;*

While this definition includes many of the key concepts common in data protection laws, it omits some that are often afforded increased protections including race, ethnicity, biometric data, genetic data, information relating to sex life, and other attributes related to an individuals' activity in the digital economy.

In addition, there is no definition of the term "biometric data." Alignment with good international practice would involve expanding the definition of "sensitive personal data" to reflect international good practices, including incorporating biometric data. A common formulation would include personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual, including without limitation by physical measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition and deoxyribonucleic acid (DNA) analysis.

Use of the terms "data users," "public bodies," "private bodies" and "persons"

The OECS Model Bill uses inconsistent terminology around the entities responsible for determining the scope and means of processing and that are subject to obligations under the OECS Model Bill. In some places, the OECS Model Bill refers to "data users". However, other parts of the OECS Model Bill, including the individual rights section, refer to "public bodies" and "private bodies." The OECS Model Bill also sometimes refers to data users as "persons," (a term that is not defined), which may impose obligations on

such "bodies" and "persons" even if they do not qualify as data users, i.e., those entities who have control over the processing of personal data.

In addition, a related issue implicates the definition of "private body" and the use of it along with "public body" as a replacement for data user:

> *"private body" means a body, excluding a public body, that–*
>
> *(a) carries on any trade, business or profession, but only in that capacity; or*
>
> *(b) has legal personality;*

First, the definition does not include individuals, only those with a "legal personality." This may limit application to individuals who function as data users where the terms "public body and private body" are used in its place.

Second, private bodies must "carr[y] on [a] trade, business or profession." This potentially further excludes data users such as NGOs and non-profits that may process personal data but would neither qualify as public bodies or public bodies under these definitions. These entities would not be subject to the obligations specifically directed at those "public bodies and private bodies."

Alignment with good international practice would involve making the terms used to describe data users consistent in the OECS Model Bill, and generally simplifying them. It would also be appropriate to remove the limitation restricting the individuals or entities that may qualify as a private body.

No definition of "consent"

Although consent of a data subject is required in several contexts throughout the OECS Model Bill, there is no definition of consent. Reliance on consent is a hotly contested topic in many countries, and it is therefore helpful to define what it comprises. For example, consent could be defined to require that it be freely given, informed and an unambiguous indication of agreement by some affirmative action. Otherwise, something more coercive, such as a pre-checked box on an electronic form, could potentially be considered consent. Alignment with good international practice would involve adding an internationally accepted definition of "consent."

No clear concept of a "data processor"

The OECS Model Bill refers to "data processors" in two places. Once, in the definition of "data user," but only to exclude them from the definition, and another time in the section 10(2) to require data users to ensure that their data processors have adequate data security measures in place. However, there is no definition of a data processor. Defining the role of data processors in a data protection law is essential to clearly establish their responsibilities and accountability in handling personal data on behalf of data controllers. They increasingly play a key role in the digital economy by operating as cloud service providers, payment processors, and marketing agencies processing personal data on behalf of data controllers.

Alignment with good international practice would involve adding a definition of "data processor" that is consistent with international good practices, i.e., one that processes personal data on behalf of or at the direction of a data user or another data processor. The purpose of the term is typically to apply a lighter set of obligations to those that are not the primary responsible data users but to which processing is delegated or otherwise outsourced.

Relationship with other national legal instruments

In Section 5 provides that the OECS Model Bill:

> *shall not affect the operation of any enactment that makes provision with respect to the collection, holding, use, correction or disclosure of personal information and is capable of operating concurrently with this Act.*

This provision may be problematic to the extent that respective jurisdictions reflect their provision in their national laws. One of the primary functions of a generally applicable data protection law is that it sets out processes, rights and obligations which jointly establish a harmonized and consistent environment

governing the processing of personal data across the economy. This means that other legal frameworks governing personal data may be supplemented by its provisions, and that it would take precedence over any overlapping or conflicting frameworks.

However, the provision that the Act "shall not affect the operation" of any other law regarding "the collection, holding, use, correction or disclosure of personal information*"* would restrict the Act's ability to override existing law, where necessary, and preventing it from fully establishing uniform data protection safeguards across the economy.

Alignment with good international practice would involve removing entirely Section 5 of the OECS Model Bill.

Processing activities

The OECS Model Bill allows the Minister, upon the recommendation of the Information Commissioner, to establish additional exemptions.

> *The Minister may, upon the recommendation of the Information Commissioner, by order published in the Gazette exempt–*
>
> *(a) the application of any of the Personal Data Protection Principles under this Act to any data user or data processor or class of data users or data processors; and*
>
> *(b) any data user or data processor or class of data users or data processors from specified provisions of this Act.*

Alignment with good international practice would involve not authorizing a data protection authority, Minister or other government entity to subsequently designate other categories of processing activities that are exempt from the legislation on an *ad hoc* basis as this process can easily become subject to abuse. However, it would be reasonable to allow the authority to exempt data processing from specific restrictions in certain situations, such as for research and development or humanitarian purposes.

Principles governing the processing of personal data

Lawful basis of processing for public interest

The OECS Model Bill provides lawful bases of processing personal data under its "General Principle", which are largely aligned with the international good practices. It includes the lawful bases of consent of a data subject, and necessity for certain purposes. However, this provision excludes the basis of processing based on the necessity for substantial public interest, which would provide a ground for processing for public welfare, and wider societal benefits. These could include activities including fraud prevention, promoting initiatives on equality and racial and ethnic diversity and more.

Alignment with good international practice would involve amending Section 7(2) of the OECS Model Bill to explicitly include that the processing of personal data is lawful when it is necessary for a substantial public interest purpose.

Additional protections for processing personal data of children or persons with limited capacity to consent

The OECS Model Bill does not provide any additional protections for processing personal data of children and of persons lacking the legal capacity to consent.

Alignment with good international practice would involve including in the legislation additional protections for processing personal data of children and persons lacking the legal capacity to consent, in particular requiring consent of a parent or guardian, except in limited cases, such as when processing is authorized by law or is necessary to protect the vital interest of the child and persons lacking the legal capacity to consent, consistent with global best practices.

Principle of lawful, fair and transparent processing

The OECS Model Bill fails to include a principle mandating that personal data be processed in a lawful, fair, and transparent manner, as is required by established global best practices.

Alignment with good international practice would involve adding a data protection principle mandating that personal data be processed "lawfully, fairly and in a transparent manner", consistent with international good practices.

When the data controller, or its data processor, is collecting the data directly from the data subject, the disclosures would be mandatory upon collection. When the data controller, or its data processor, is obtaining the data from a third party that collected the data under a lawful basis for a specified purpose, no disclosures should be necessary, as the third party should already have disclosed to the data subject that the data would be shared with that data controller. If the data subject was not notified of such sharing when collected, or if the data is to be processed for a purpose that is beyond the original disclosed purposes, a new lawful basis for processing must be determined, and new disclosures to the data subject would be necessary.

Principle of data minimization

The OECS Model Bill requires that personal data shall not be processed unless-

[…] the personal data is adequate but not excessive in relation to that purpose.

This articulation of the data minimization principle is largely in accordance with best practice, though it omits a "minimum necessary" standard.

Alignment with good international practice would involve retaining the current provision but adding a "minimum necessary" standard rather than merely "adequate but not excessive."

Data retention principle does not have exemptions

Section 11 sets out the "retention principle" which limits personal data retention by data users:

> *(1) The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.*
>
> *(2) It shall be the duty of a data user to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.*

However, the OECS Model Bill does not set out the common exception to this requirement, allowing personal data to be further retained if required by law. For example, financial service providers are often subject to customer data retention requirements under anti-money laundering laws. Adding an appropriate exception to section 11 would permit these and other service providers to comply with their sector-specific obligations.

Alignment with good international practice would involve including exceptions to the data retention requirement consistent with international good practices, including when further retention is required by law.

Individual rights concerning personal data

No data subject right to withdraw consent

The OECS Model Bill does not include a data subject right to withdraw consent. Such a withdrawal ordinarily prevents any further processing of personal data where the basis of processing was consent in the first place.

Alignment with good international practice would involve including an individual right to withdraw consent and ensuring that consent can be withdrawn as easily as it is provided.

Automated processing

The OECS Model Bill does not include a right to object to being subject to decisions based on automated processing of personal data.

Data security

Lack of specific data security requirements

Section 10 of the OECS Model Bill sets out the obligation of a data user to process personal data securely:

> *when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard to- (a) the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction; (b) the place or location where the personal data is stored; (c) any security measures incorporated into any equipment in which the personal data is stored; (d) the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and (e) the measures taken for ensuring the secure transfer of the personal data*.

While it is not advisable for laws to mandate specific, technical security measures that may become outdated or irrelevant, it is beneficial to provide guidance on adopting technical and organizational measures to secure personal data and include non-prescriptive examples, such as pseudonymization and encryption.

Alignment with good international practice would involve expanding the existing security principle, and introducing some recommended technical measures, in alignment with international good practices.

No personal data breach notification obligations

The OECS Model Bill does not include any personal data breach obligations. Typically, data processors are required to inform data users if they experience any such breach. Data users are in turn required to notify the relevant data protection authority and, in cases where there is a high likelihood of harm to data subjects, to notify affected data subjects directly. These notifications keep the relevant authority apprised of threats to personal data security and give data subjects an opportunity to mitigate any damage from the breach, such as resetting passwords.

Alignment with good international practice would involve including mandatory breach notifications by a data processor to a data controller and by data controllers to a regulator in the case of all breaches and by data controllers directly to data subjects when the breach is likely to significantly harm the data subject, and that in light of knowledge of the breach, the data subject will be able to take steps to reduce risk of harm, such as switching to another service provider. In all cases, such notifications should be made promptly upon discovery of the breach.

No data processor liability for data security

Section 10(1) addresses data security requirements for data users. Section 10(2) addresses data security requirements for data processors, but it does not similarly make data processors directly liable for failure to adopt adequate data security measures. Rather, it is the job of data users to ensure that their data processors comply:

> *Where processing of personal data is carried out by a data processor on behalf of the data user, the data user shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, ensure that the data processor–*
>
> *(a) provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and*
>
> *(b) takes reasonable steps to ensure compliance with those measures.*

To ensure that data processors are more likely to comply with such requirements, data processors could have direct liability under the OECS Model Bill.

There are advantages to imposing direct liability on data processors for data security obligations as opposed to leaving it only to data users to take responsibility for obtaining contractual guarantees from their data processors, and for ensuring their compliance. We would recommend considering such direct liability.

No further requirements on data users when engaging data processors, including ensuring other data processor obligations

Other than the data general security requirements described above, the OECS Model Bill does not require data users to take any measures to ensure that data processors can assist them in complying with the Act. For example, data users, relying parties or other entities involved in data exchange, may need assistance from their data processors when responding to data subject access requests, resolving data breaches, making data breach notifications, or performing other functions.

Typically, data protection laws require that data users take adequate measures to ensure that data processors can perform these functions. This may include an obligation on the data user to perform due diligence prior to and after engagement or to enter into a written contract with the data processor. While the data user generally remains primarily liable for any failures of the data processor that would result in a violation of the data protection law, the data processor would be contractually liable to the data user.

Alignment with good international practice would involve setting out requirements around engaging a data processor to ensure that a data user takes adequate measures to ensure that a data processor can comply with the OECS Model Bill and assist the data user in complying with the OECS Model Bill.

No requirement to conduct a DPIA

The OECS Model Bill does not require data users to conduct DPIAs when processing personal data that are large in scale, extensive in scope, innovative, or highly sensitive. Incorporating a requirement to conduct a DPIA under certain circumstances is recognized as a good practice, since DPIAs enable data users to proactively identify and mitigate potential risks associated with their data processing activities. In addition, in instances where a DPIA reveals that the proposed processing activities may pose significant risks to individuals' privacy, data controller may be required to consult with a data protection regulator. This process promotes compliance with the Act, fosters an environment of accountability and enhances public trust in how personal data is managed and safeguarded.

Alignment with good international practice would involve introducing the requirement for DPIAs, consistent with global best practices.

Cross-border transfers of personal data

The OECS Model Bill does not address cross-border transfers of personal data. Such transfers may be required to enable commercial transactions and investments in the region.

Typically, data protection laws set out the circumstances under which cross-border transfers are permitted. These are likely to include determinations of adequacy by the Information Commissioner or the implementations of safeguards, such as binding corporate rules, third-party certification mechanisms or standard contractual clauses. A sensible cross-border framework is important to ensure confidence and continuity in processing data that needs to be transferred overseas, e.g., for outsourcing to more efficient foreign processors and cloud-based processing.

Alignment with good international practice would involve including provisions governing cross-border transfers of personal data, consistent with global bast practices, which would aim to ensure that an adequate level of protection is provided, whether by law of the foreign jurisdiction to which data is transferred or through mechanisms like binding corporate rules and contractual clauses.

Institutions

Unclear and insufficient funding resources

The OECS Model Bill does not include provisions setting out explaining the sources of the Information Commissioner's funding, whether for initial establishment or for ongoing annual expenses. Ensuring a consistent funding stream is essential for any authority to fulfill its role and enshrining this requirement in law safeguards financial allocation from arbitrary government decisions.

The OECS Model Bill does not include provisions outlining the sources of funding for the Information Commissioner, both for its initial establishment and for its ongoing operational expenses. Securing a reliable and transparent funding mechanism is crucial for the authority to effectively carry out its mandate, and embedding this requirement in law ensures that financial allocations are shielded from arbitrary government decisions.

Alignment with good international practice would typically involve setting out how the body will be funded, typically from government budget, fines and donations from for example international development agencies.

Penalties and enforcement

Disproportionate and unclear fines and penalties

Under Sections 16, 24, 27, and 44, the OECS Model Bill provides for criminal penalties for certain violations. However, imposing criminal penalties for data protection violations is not aligned with international good practices, as it creates the potential to lead to overly harsh consequences for infractions that may not warrant such severity. Data protection violations, especially in complex compliance environments, are often better addressed through administrative penalties, fines, or corrective measures rather than criminal sanctions. We would suggest not providing for criminal liability for violations and instead having a system of administrative fines, accompanied by clearly defined escalation procedures.

3.A.2 Policy Considerations for the Development of Data Protection and Privacy Legislation in the Eastern Caribbean Currency Union (ECCU)

Overview and background

The ECCB developed the Policy Considerations for the Development of Data Protection and Privacy Legislation in the ECCU ("Policy Considerations") in 2024 to update its position from its 2020 data protection and privacy policy. It addresses the evolving challenges arising from the region's continued transition towards a harmonized digital economy.

The Policy Considerations appropriately acknowledges the context and frames the policy considerations. In summary: Data has become a vital asset for businesses and nations. The growing value of data heightens privacy and security risks. The stringent sanctions in frameworks like the EU's GDPR highlights common violations and sets a global benchmark and reference point for the ECCU designing effective data protection obligations and enforcement mechanisms. Persistent cyber threats from malicious actors highlight the need for robust, proactive measures. Safeguarding citizens' privacy is a core human right, requiring a flexible, technology-neutral data protection regime. The ECCU should focus on adequate protection measures, clear scope and obligations, and effective enforcement protocols. This framework should align with international good practices, while addressing the region's specific challenges, including limited resources and increasing digital transformation. Strong regulatory enforcement should cover breach notification, penalties for non-compliance, and accountability measures.

Key elements and observations

The Policy Considerations offer a framework for addressing key elements of data protection and privacy legislation in the ECCU, which are largely aligned with global best practices:

- ***Scope:*** The Policy Considerations recognize the need to limit scope of data protection law to exclude personal and household use, as well as other exclusions consistent with international good practice (investigation of crime, threats to public security, journalistic, academic, artistic and literary expression). Helpfully, it contemplates excluding smaller controllers and processors from certain obligations. The territorial scope is also reasonably aligned with international good practice.
- ***Key definitions:*** The definitions of key terms are consistent with international good practices. It would be worth considering whether to add other definitions for completeness when preparing legislation, such as the term sensitive data (although as discussed in Section 2.A.1 it is worth considering whether this only adds unnecessary complexity).
- ***Data processing requirements:*** The Policy Considerations appropriately sets out the basic principles of data protection. It could add reference to the principles of data minimization, lawful, fairness and transparency. There could be a little misunderstanding about the characterization of "privacy by design" but this is not significant.
- ***Lawful processing of personal data:*** The recommended bases of processing are consistent with the international good practices.
- ***Rights of data subjects:*** The recommended rights of data subjects are largely consistent with international good practice. However, we do not tend to recommend establishing a generally applicable right to data portability at the start. (See Section 2.D.5 above.)
- ***Obligations of data controllers and data processors:*** Although this part is aligned with elements identified in the international good practices, it does not reflect a "risk based" approach and the principle of proportionality. These would mandate obligations and processes according to the anticipated risk of an activity on personal data. This is reflected through the generally applicable requirement for data controllers and data processors to register with the data protection authority, and the general requirement to appoint a data protection officer to the types of processing activities of the data controller. These requirements would both be highly disproportionate, unworkable, and risk causing more harm than benefit. (See Section 2.G.5.) It would be helpful to add that data users (i.e., controllers) must ensure that data processors carrying out processing on their behalf will have contractual obligations to them to comply with the law, and making them liable to data controllers for any violations.
- ***Role of data protection authority:*** The role of an authority is appropriately described. In addition, the intended relationship between regional and national legal systems and institutions will need to be clarified, including whether there would be national authorities and how they relate to the regional authority. An ECCU Data Protection Authority may need to hold different functions depending on whether it needs to harmonize and facilitate the enforcement of established national data protection instruments through national data protection authorities, or whether it would need to directly enforce national data protection frameworks within the ECCU region. (See also Section 0of this report.)
- ***Transfers outside the ECCU:*** The framework for personal data transfers is broadly consistent with international good practice. There is appropriate reference to the importance of harmonization among ECCU countries, which needs to be prioritized to serve as the foundation for flow of personal data among ECCU members, and the development of a harmonized approach between the ECCU and non ECCU countries.
- ***Enforcement measures:*** The Policy Considerations appropriately describe the importance of accountability and robust mechanisms for supervision and oversight.

Overall, these recommendations are largely consistent with international good practice and will be carefully considered and incorporated in the drafting of the harmonized data protection framework for the ECCU member states.

3.B Sector-specific regional legislation

3.B.1 Cybersecurity and cybercrimes

Currently, there are no regional cybersecurity laws. However, a soft law instrument, the Draft Regional Environmental and Social Management Framework (ESMF), has been developed as part of the Caribbean Digital Transformation Program. This framework includes provisions related to cybersecurity, data protection, and the protection of critical network infrastructure. However, it remains a draft document and has not yet been implemented or enacted within the Organization of Eastern Caribbean States (OECS).

3.B.2 Consumer protection

There is no regional framework specifically on consumer protection. However, consumer protection provisions sometimes appear in sector-specific legislation, and these may include provisions affecting treatment of personal data. For example, the Payment System and Services Bill prepared by the ECCB in 2024 includes limited provisions on consumer protection. It aims to establish a comprehensive regulatory framework for payment systems in the region, by being adopted by member states. The Bill provides for the licensing and regulation of payment service providers, oversight of payment systems, and related financial and operational matters to promote security, efficiency, and transparency in the payments industry.

The Bill outlines licensing requirements for payment service providers and addresses the processing of personal data in relation to payment services. Safeguards relevant to personal data are established in the Sections below:

- ***Central Bank confidentiality:*** Section 33 establishes the Central Bank's duty of confidentiality, prohibiting it from disclosing any information or documents obtained in the exercise of its functions under the Act, except under specific circumstances. Disclosure is permitted when necessary for performing its regulatory duties, protecting the financial integrity or security of the payment system, or sharing information with legally authorized recipients. Disclosure is also permitted if ordered by a court, for statistical purposes, or to maintain transparency among payment system participants. Additionally, information can be disclosed to fulfill international treaty obligations. This provision promotes the personal data principle of confidentiality, while allowing controlled disclosures to safeguard the financial system and uphold legal obligations.
- ***Data protection obligations of licensees:*** Section 63 establishes data protection obligations of licensees and participants in the payment system. It requires them to process personal data in a way that supports the prevention, detection, and investigation of payment fraud. Additionally, they must process data in compliance with the applicable national data protection act or any other relevant data protection laws so that consumers receive necessary information about how their data is handled. Furthermore, licensees and participants are prohibited from accessing, processing, or retaining personal data beyond what is strictly necessary for providing payment services unless they obtain the consumer's explicit consent.

This Bill upholds principles of confidentiality and non-disclosure but does not include specific provisions on data security and data subject rights. Rather than directly imposing obligations and responsibilities on entities processing personal data or granting rights to data subjects, it defers to national data protection laws. As a result, its provisions on personal data processing are limited. To ensure comprehensive data protection, accountability, and compliance with international practices, this Act would benefit from integration with a broader, generally applicable data protection framework.

3.B.3 Freedom of information requests

There is currently no regional legislation on freedom of information requests in the region.

3.B.4 Health

There is currently no regional legislation on health in the region.

3.B.5 Education

There is currently no regional legislation on education in the region.

3.B.6 Financial Services

Introduction, scope of application and definition of key terms

Banking Bill of 2015

The Banking Bill of 2015 was prepared as a draft law in order to develop a single banking space in the ECCU. State parties to the ECCB Banking Agreement of 1983 each adopted the Banking Act as national law (see Section 4 of this report).

The Banking Bill provided for the regulation of banking operations, the establishment of a unified banking space, and the collection, processing and disclosure of personal data by licensed financial institutions. The Act provided for various processes that involve processing personal data. This includes receiving information from individuals applying for licenses (Sections 3 and 7(1)). They include evaluation of whether proposed directors and officers are "fit and proper" for the role (Sections 38 and 97), as well as direct and indirect holders of shares or interests in them (Section 36(2) and 98). The Act provided for auditing of books, records and financial statements, which could include personal data (Section 61), and authorized investigators would have access to information in the course of investigations (Section 74). The Bill also provides reasons for removal of a director or officer (Section 103), which requires the assessment of various factors, including personal data.

Many of the above activities of receiving license applications, and providing, evaluating and storing personal data of shareholders, directors and other officers, as described above, would constitute forms of personal data processing.

Credit Reporting Bill of 2016

The ECCB Harmonized Credit Reporting Bill of 2016 was prepared to introduce harmonized credit reporting. It was enacted into national law in the ECCB member states law (see Section 4 of this report). The Bill provided for a comprehensive framework for a regional credit system. Its primary objectives include ensuring objective credit decisions, facilitating credit information sharing and reporting, regulating credit reporting practices, and creating a harmonized space for credit-related activities. The Bill primarily focuses on how personal data are processed by credit bureaus and regulates the collection, evaluation and overall processing of personal data. It also includes definitions of key terms:

- A "data subject" is defined as any person "whose information has, or many have, been furnished to the credit bureau by reason of a contractual relationship with a credit provider, a loan application signed by the person, or any other legitimate purpose."
- A "data subject information" covers "any information relating to the credit information or personal information of a data subject, whether such information is obtained from the data subject, whether specified public register, that may be processed under this Act or the Regulations."
- A "personal information" in relation to a data subject is "the full name, an alias or previous name, the gender, data of birth, social security number, passport number, driving license number, past and current addresses, any other contact information of the individual."

The Bill also distinguishes information as "positive information" and "negative information". Both categories of information contain information related to the financial details of individuals and can be considered as personal data.

- "positive information" means any information "relating to the current or historical status of a credit transaction between a data subject and a credit provider, including but not limited to (a) the date on which an account was opened, (b) the amount of the loan, (c) the date of the last payment, (d) any outstanding credit (e) any high credit approved, (f) the amount of payments, (g) payment history, (h) the current balance, (i)repayment patterns, (j) the utilization of credit, (k) any collateral pledged."
- "negative information" means any information : in relation to the delinquent status of a credit transaction between a data subject and a credit provider, and includes: (a) credit defaults, collections and late payments, (b) accounts compulsorily closed other than for administrative reasons, (c) voluntary or mandatory surrender of assets, (d) conviction for the offense of fraud or forgery; (e) receiverships, bankruptcies and liquidations, (f) liens, garnishment or judgments; (g) cheque kiting activity; (h) refusal to provide business financial statements, (i) any other act or information which could cause a credit application to be declined or restricted according to a credit providers' policy relating to the overdue, past due, charge odd, or delinquent status of the credit transaction between the data subject and the credit provider."
- "Process" means to "collect, keep, maintain, hold or store the credit information, or carry out any operation or set of operations on the credit information including (i) the organization or adaptation of the credit information, (ii) the retrieval, consultation or use of the credit information, (iii) the disclosure of the credit information by transmission, transfer or dissemination, and (iv) the alignment, combination, correction, erasure or destruction of the credit information."

The Credit Reporting Bill covers a wide range of personal data processing activities:

- The Central Bank, as part of its license evaluation process for credit bureaus and personnel employment, collects and assesses personal data during its review.
- Credit bureaus, in their operations and credit report preparation, process large volumes of financial and non-financial personal data. Sections 17–32 outline these activities, specifying the required safeguards credit bureaus must implement and the rights they must uphold for individuals.
- Under Sections 33–39, the Central Bank is authorized to conduct inspections, including entering and searching premises and collecting materials that may contain personal information.

The Credit Reporting Bill provided for multiple lawful bases for processing personal information within the credit reporting sector. It sets confidentiality and non-disclosure requirements for credit bureaus and mandates the implementation of security safeguards to protect sensitive data. Additionally, the Bill provided for various rights of data subjects in order to ensure greater transparency and control over their personal information.

Lawful basis for processing

Banking Bill

- As outlined in the previous section, Sections 7(1), 36(1), and 61(1) of the Bill mandate the processing of personal data belonging to directors, shareholders, and officers. This is done to meet the Bill's requirements, including evaluating license applications and conducting audits.

- Section 178 discusses the requirement for secrecy of information, and allows individuals associated with licensed financial institutions to disclose information of their customers only where a written authorization of the customer or their legal representative is given, when it is required by law or a court order, and where it is part of an intergovernmental agreement among participating governments. This section reflects the lawful basis of consent and processing of personal data under a court order.

Credit Reporting Bill

- Entities applying for a credit bureau license must submit applications containing personal information, which is processed under the lawful basis of legal compliance. The Central Bank then collects and evaluates this data to assess applicants' suitability for licensing based on the criteria set forth in the Bill.
- Section 18 mandates that credit reports cannot be accessed without the data subject's prior consent. However, credit information providers may disclose both positive and negative credit data to credit bureaus without consent, provided they notify the data subject via public notices at their business location, website, or other appropriate means. Third parties may obtain a credit report for a legitimate purpose under Section 20, but only with the data subject's consent, which may be electronic or any form providing valid evidence. Consent remains valid until the contractual relationship ends, though credit data may still be retained under Section 25. Before releasing data, credit bureaus must verify and validate the identity and consent of the data subject and use secure transmission methods to prevent tampering.

  Exceptions to the consent requirement include cases involving court orders, law enforcement investigations, insurance fraud detection, financial penalties, legal proceedings, or research and statistical use, provided the data is de-identified. These provisions uphold data protection, transparency, and lawful processing while ensuring necessary safeguards in credit reporting.
- Under Sections 33–35, the Central Bank has the authority to conduct investigations, audits, and assessments to ensure that credit bureaus comply with the Bill. This includes entering premises, requesting documents, and reviewing records as part of their duties. These inspections, audits, and investigations involve the collection and evaluation of personal data, which is lawfully processed to ensure regulatory compliance.

Obligations of the entity processing personal data

Banking Bill

Section 178 provides the requirement for secrecy of information and prohibits individuals associated with licensed financial institutions from disclosing any information regarding the identity, assets, liabilities or transactions of their customers, subject to exceptions.

Credit Reporting Bill

The Credit Reporting Bill provides for multiple obligations on entities processing personal data, aligning closely with data protection principles. These obligations ensure lawful processing, accuracy, security, and transparency while safeguarding individuals' rights over their credit information.

- Section 20 outlines key data protection obligations for credit bureaus, regulating the content, accuracy, security, and disclosure of credit reports. It mandates that all credit reports contain lawfully processed information from approved providers, ensuring validity, accuracy, and relevance. Reports must not include judgment details without specifying the amount, age, and creditor's information, nor contain sensitive personal data such as race, religion, medical history,

or political affiliation. These provisions echo the principles of data quality and accuracy principles and reinforce purpose limitation by preventing the misuse of data.

- Credit bureaus cannot generate lists of individuals with good payment histories unless for a legitimate purpose, nor omit information that may impact a data subject's ability to access credit. They must also implement reasonable procedures to ensure timeliness, sufficiency, and accuracy, alongside rigorous security measures to protect data integrity and reliability. Non-compliance with these obligations constitutes an offense under the Act.
- Credit bureaus may only provide credit reports for permissible purposes and with the data subject's consent. These purposes include credit applications, acting as a guarantor, debt collection, tenant screening, insurance underwriting, pre-employment screening, and portfolio monitoring, among others. Requesters must verify identities, submit proof of consent, securely dispose of data, and implement security controls. Credit bureaus are obligated to validate consent and identity before disclosure and ensure data integrity during transmission. These provisions reflect international good practices for handling sensitive personal data, reinforcing purpose limitation and data security.
- Section 21 focuses on data management and quality control, requiring credit bureaus to implement strict protocols to maintain data accuracy, reliability, and security. They must update records regularly, enforce quality control procedures, and take all necessary steps to ensure comprehensive and current data. Credit information may only be disclosed for permissible purposes, and failure to comply results in penalties.
- Section 22 establishes strict data security and control measures. Credit bureaus must implement technical, institutional, and procedural safeguards to prevent unauthorized access, misuse, and breaches. Additionally, they are required to maintain detailed access logs, tracking all authorized access and data processing activities.
- Section 24 emphasizes the duty of credit bureaus to maintain complete and accurate records of credit information. This ensures data integrity and transparency, prevents misinformation, and protects data subjects from errors in credit reporting.
- Section 48 reflects the confidentiality obligations on the Central Bank, restricting access to inspection-obtained information to authorized officials or individuals with explicit written permission. Unauthorized disclosure is prohibited unless required by law or with the data subject's consent. However, the Central Bank may share information with government agencies, regulators, or law enforcement when necessary for legal or public interest purposes. Even authorized individuals cannot be compelled to testify on such matters unless ordered by a court or with the data subject's consent. This provision ensures financial data remains protected while allowing controlled disclosure when legally justified.

Data subject rights

Banking Bill

Under section 178(2) individuals may request summaries of their credit ratings, which echoes the right to access.

Credit Reporting Bill

- Under Section 17(2), credit bureaus must give credit information providers a reasonable opportunity to correct any inaccurate, illegal, incomplete, or otherwise deficient information contained in a data subject's credit file. This provision aligns with the data subject's right to access and rectify personal information.

- Similarly, Section 19 allows individuals to request their credit report from a credit bureau and inquire about specific information included in the report.
- Under Section 22, upon request, credit bureaus must provide data subjects with details of who accessed their information and when. Credit bureaus are also required to develop and enforce written policies and procedures, limit access to authorized personnel through secure authentication mechanisms, and maintain compliance with security protocols through regular monitoring, audits, and employee training. Any security breaches must be promptly investigated and addressed, while credit bureaus must continuously review and improve security policies and authentication controls. Failure to comply with these security and control measures constitutes a criminal offense, making the credit bureau liable for penalties upon summary conviction.
- Section 23 grants data subjects the right to access and correct their credit information held by credit bureaus. It entitles individuals to be informed about the types of data a credit bureau supplies to its subscribers: to challenge any inaccurate information and request corrections and to receive a free copy of their credit report once per year.
- Credit bureaus must respond to access and correction requests within three days and provide clear information on data subject rights and the procedures for requesting access or corrections. Additionally, the Minister has the authority to issue regulations for correcting incomplete, obsolete, misleading, erroneous, or inaccurate credit information processed by credit bureaus.

Cross-border transfers of personal data

Banking Bill

There are only two instances where the Bill addresses broadly cross-border transfers.

Section 94 allows the Central Bank to enter into formal agreements or arrangements with foreign supervisory or resolution authorities, for the purpose of facilitating coordination, cooperation, and the exchange of information between the Central Bank and the foreign authorities. It provides that the Central Bank may only share information if it is confident that the foreign authority has a legal obligation to protect the confidentiality of the shared information in accordance with applicable laws or regulations. The sharing of data is likely to include personal data, such as financial records, credit scores, and names of customer data.

This provision reflects the principle of adequacy of protection, which is found in multiple data protection frameworks with the aim that when personal data is transferred from one jurisdiction to another, the receiving jurisdiction must offer a level of protection that is as robust as that available in the originating jurisdiction.

Additionally, Section 89 states that, in the interest of public policy and upon request by the Central Bank, licensed institutions must share personal data with the Central Bank to ensure compliance with the Act. This activity involves data sharing of information that is likely to include personal data.

Credit Reporting Bill

Section 31 regulates the cross-border flow of credit information and ensures the protection of personal data when processed outside the Currency Union. It allows a credit bureau, with the approval of the Central Bank, to outsource or subcontract credit information processing to entities operating outside the Currency Union, provided it complies with relevant regulations. However, the Central Bank will not approve the transfer of personal data outside the Currency Union if it believes that the information will not be adequately protected or will not receive the same level of protection as required by this Act. This provision emphasizes data security and regulatory oversight, ensuring that sensitive credit data is handled safely and not transferred to jurisdictions with weaker data protection standards.

Institutions and penalties

Banking Bill

While there is no specific institution established for the enforcement of data protection standards, the Central Bank generally oversees the data collection and processing to ensure compliance and risk management. The penalties for non-compliance or failure to submit the required information or provision of false data carries the penalty of $25,000 per Section 96.

Credit Reporting Bill

The Credit Reporting Bill does not establish any institutions that process personal data, other than credit bureaus. However, it establishes the credit reporting review commission through which data subjects and credit bureaus gain the right to seek a review of decisions or actions related to credit disputes. If a credit bureau fails to resolve a dispute within the prescribed time or if a data subject is dissatisfied with the bureau's decision, they may request a review. Similarly, a credit bureau that disagrees with a Central Bank decision may also seek a review. The Credit review Commission constitutes a layer of accountability on the decisions made by the credit bureaus that involve the processing of personal data.

The Bill also includes several fines relevant to the processing of personal data:

- Under Section 18(4), any person who obtains information regarding a data subject from a credit bureau under false pretenses commits an offence and is liable, on summary conviction, to a fine of not less than ten thousand dollars but not exceeding one hundred thousand dollars.
- Under Section 19(6) a credit bureau commits an offence if the credit bureau fails to comply with the requirements of purpose limitation, lawful processing, confidentiality and security and set out in sections (3)-(5) of the Act.
- Under Section 20(6), a credit bureau commits an offence if the credit bureau willfully discloses data subject information in contravention of the provisions of this section and is liable, on summary conviction, to a fine not less than ten thousand dollars but not exceeding one hundred thousand dollars.

Conclusion

Banking Bill

The Banking Bill focuses on the processing of personal data in the financial sector. While it addresses confidentiality and includes limited data subject rights, it does not include provisions on data security, data minimization, quality and transparency. The Bill could either be amended (in each ECCB member state) to encompass these areas or such matters could be addressed through data protection law. The provisions would not contradict a generally applicable data protection framework aligned with international good practice.

Credit Reporting Bill

The Credit Reporting Bill reflects key principles, rights, and obligations found in comprehensive data protection laws aligned with international good practices. Recognizing that credit bureaus process large volumes of personal data, the Bill emphasizes the need for robust security measures and data protection safeguards. It establishes frameworks for ensuring purpose limitation, transparency, and data accuracy, while also empowering individuals with various data subject rights to maintain control over their personal information. It would not conflict with a generally applicable data protection law aligned with international good practice.

3.B.7 National identification

There is currently no regional law on national identification in the region. The OECS has a Digital ID initiative and plans to create a digital identification system.

3.B.8 Passports

There is currently no regional legislation on education in the region. However, a regional framework on movement within the region is provided through the Freedom of Movement regime in the Eastern Caribbean and which is restricted to the members Eastern Caribbean Economic Union (ECEU). Established in 2010 through the signing of the Revised Treaty of Basseterre, the ECEU forms a single financial and economic space, allowing the free movement of goods, services, capital, enterprises, and people within its jurisdiction.

3.B.9 Civil Registration

There is currently no regional civil registration law in the region. Civil registration is tackled individually by member states.

3.B.10 Electronic communications

Introduction, scope of application and definition of key terms

The Electronic Communications Bill of 2006, revised in 2020, was developed for adoption as national law by member states of the Eastern Caribbean Telecommunications Authority (ECTEL) (see Section 4 of this report). It provided for the member states to repeal the prior Telecommunications Acts that they had previously adopted to adopt to harmonize telecommunications regulation across the region.

The Electronic Communications Bill aimed to facilitate electronic communications while fostering a competitive, fair, transparent, and accountable regulatory environment. One of its objectives is to ensure that licensees comply with obligations related to personal data protection, the confidentiality of communications, and net neutrality.

Several provisions in the Bill refer to the processing of personal data:

- Individuals or entities seeking an individual or class license, or frequency authorization, must submit applications to the Commission, as outlined in Sections 37-38, 47-48, and 56-57, which require the submission of personal data.
- Under Section 78, licensees must report prescribed information, including personal data, to the Commission and ECTEL. However, these authorities are prohibited from disclosing confidential commercial information without the licensee's prior written consent.
- Section 36 states that the Commission maintains a register containing details of all licensees and frequency authorizations, including personal contact information.

The collection, storage, and disclosure of personal data in the context of licensing and telecommunication services constitute personal data processing.

Lawful basis for processing

Personal data collected and assessed as part of the application process for providing licenses, frequency authorizations, and any subsequent modifications or renewals of these licenses. Personal data are also stored in records and are kept by the Commission. These various forms of processing are performed on the basis of compliance with a legal obligation under the Act.

Obligations of the entities processing personal data

The Bill provides certain obligations to entities that process personal data, which reflect data protection principles.

- Under Section 83(d) that covers consumer protection obligations, licensees shall protect data and information in a prescribed manner.
- Clause 23 of the Bill deals with secrecy and confidentiality. An oath of secrecy is to be taken by the commissioners, Chief Executive Officer, employees or members of an advisory committee.

Provision is made for the preservation of confidentiality by these persons of all matters coming to their knowledge in the performance of their duties including the business affairs of the Commission, applications to the Commission or affairs of licensees or customers. Exceptions to the duty of confidentiality include where disclosure is permitted by a court or where it is available to the public from another source.

Data subject rights

The Bill does not address any provisions for data subject rights.

Cross-border transfers of personal data

The Bill does not address cross-border transfers of personal data.

Institutions and penalties

Section 8 of the Bill provides for a national telecommunications regulatory commission and grants it the authority to carry out various functions, including advising the Minister on the development of national telecommunications policy, overseeing technical regulation, and setting technical standards for the telecommunications sector, as outlined in Section 12.

Section 109 provides for the disclosure of personal information as a crime. It restricts licensees from disclosing personal information of retail customers unless the customer provides consent, or a court order requires disclosure under this Act or another law. A violation of this rule is an offense, subject to a fine of up to $50,000, imprisonment for up to four years, or both upon summary conviction.

Conclusion

The Bill contains limited requirements for confidential processing of personal data and provides penalties for unlawful disclosures. However, it does not include any requirements for data security and minimization and secure cross border data transfers. The Bill does not contain any provisions that would contradict or be inconsistent with a generally applicable data protection law.

3.B.11 Electronic transactions

Introduction, scope of application and definition of key terms

The OECS prepared the Electronic Transactions Bill of 2011 for adoption by the OECS member states in order to establish in each national order the legal framework for electronic transactions (see Section 4 of this report). This would grant legal effect to electronic documents, records, signatures, and other related matters. The Bill also addresses the processing of personal data within the context of electronic communications between two parties, referred to as "the originator" and "the addressee." As defined in Section 2:

- "originator, in relation to an electronic communication, means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but does not include a party acting as an intermediary with respect to that electronic communication"; and
- "addressee, in relation to an electronic communication, means a person who is intended by the originator to receive the electronic communication, but does not include a person acting as an intermediary with respect to that electronic communication".

Electronic communications between an originator and addressee will often include the following personal data: their names, email addresses, metadata such as the time and location of an email, identifiers included in a signature (phone numbers, physical addresses, and other contact details may be shared directly within the email content), along with any information revealed in the context of their communication.

The definition of "authentication data" encompasses a username, password, and license key, which are considered personal data processed within the context of electronic transactions, particularly in relation to electronic signatures.

According to the definition of "electronic communications", which cover information being "generated, communicated, processed, sent, received, recorded, stored, or displayed by electronic means", personal data undergo "processing" as they are transferred by the originator and subsequently received and stored by the addressee.

However, the Bill does not impose any obligations on the originator, or the addressee of electronic communications regarding the protection, maintenance of integrity, or safety of personal data. Additionally, there are no provisions concerning data subject rights, cross-border data transfers, or relevant institutions authorized to oversee electronic communications. As a result, electronic transactions would benefit from a comprehensive data protection framework that imposes obligations, rights, and responsibilities regarding the processing of personal data.

Lawful basis for processing

Personal data involved in electronic transactions, as defined under the Bill, are processed under several lawful bases:

- Under Sections 16-21, the processing of personal data involved in the formation and enforcement of an electronic contract is performed under the lawful basis of contractual necessity. In the context of automated contracts, personal data is required to fulfill the terms and obligations outlined in the contract, such as providing services, delivering goods, or managing transactions
- Section 7 states the legal recognition of electronic communications, and Section 8 the legal recognition of electronic records. Providing personal data through electronic communications and in electronic records constitutes personal data processing based on contractual necessity and is legitimized through the lawful obligations under this Bill.

Obligations of the entity processing personal data

- Section 26(2) provides that where a security procedure has been agreed to be applied by the parties of an electronic record, the appropriateness of the security procedure can be determined by various factors, including the nature of the transaction, the level of technological modernity of the party and more. Given that electronic records are likely to contain personal data, this principle echoes the data protection principle of data security.
- Section 31 establishes the framework governing the use of electronic records and electronic signatures by the government and its agencies. It provides that when a public authority decides to perform any of the its key functions set out in subsection (1) of Section 31, by means of electronic records or in electronic form, the public authority may specify, among other factors "the control processes and procedures that may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; or (e) any other required attributes for electronic records or payments that are currently specified for corresponding paper." This requirement reflects the requirement of records to be processed with confidentiality, security and integrity.

Data subject rights

The Bill does not address data subject rights.

Cross-border transfers of personal data

Section 25 the Act addresses cross-border recognition of electronic signatures and certificates. The Bill allows parties to mutually agree on the use of a particular type of electronic signatures and certificates which are recognized as sufficient for the purpose of cross-border recognition.

Institutions and penalties

The Bill does not establish institutions not it provides for penalties relevant to processing of personal data.

Conclusion

While the Bill provides a framework for regulating electronic communications and ensuring the validity of electronic documents and signatures, it addresses inadequately the issue of protection of personal data. The Bill would not conflict with a data protection framework aligned with international good practices. It would be supplemented by its provisions, especially as it pertains to the obligation of confidentiality, data security safeguards and cross-border data transfers. It would also ensure that both originators and addresses are held accountable for the responsible processing of personal data.

3.B.12 E-signatures

Introduction, scope of application and definition of key terms

Electronic signatures are addressed within the Electronic Transactions Bill of 2011, which was prepared for adoption by contracting states (see Section 4 of this report). Specifically, Sections 22-28 provide the legal framework for the recognition of electronic signatures in the context of electronic transactions. The Bill defines the following key terms:

- Under Section 2 of the Bill, a signature is defined as a method used to identify a person and to indicate the intention of that person in respect of the information contained in a record.
- Signature creation data is unique data, including codes or private cryptographic keys or a unique configured physical device which is used by the signatory in creating an electronic signature.
- Secure electronic signature means an electronic signature that is treated as a secure electronic signature by virtue of section 28 or any other provision of this Bill.

The use of electronic signatures would typically involve processing of personal data under a data protection law.

Lawful basis for processing

Where an electronic signature is used to enter into or perform contractual obligations, the performance of the contract would constitute a lawful basis of processing the personal data embedded within these signatures (e.g., name, email address, unique identifiers). Under Section 22, where a signature is mandated by law, an electronic signature satisfies this requirement, provided it effectively identifies the individual and serves to demonstrate their intent regarding the creation of an electronic record. Consequently, the processing of personal data within the signature is justified under the lawful basis of compliance with the legal obligations outlined in this Bill.

Under Section 23 of the Bill, parties of the transaction may agree to the use of a particular method or form of electronic signature or security procedure.

Obligations of the entity processing personal data

- Section 22 provides that when the law requires a document or record to be signed, or imposes consequences for not having a signature, the requirement for a signature is satisfied for electronic records if two conditions are met: when it effectively identifies the individual and serves to demonstrate their intent regarding the creation of an electronic record. This provision echoes the

data protection principle of "integrity", as the validity of an electronic signature is conditional upon the integrity, validity and accuracy of the information to which it relates being maintained.

- Similarly, Section 27 reflects the requirements for an electronic signature to be treated as a secure electronic signature in the context of an electronic transaction. For the signature to be considered secure, it needs to be unique to the person using it, capable of identifying the person who created it, created using a method or means that is under the sole control of the person using it, linked to the electronic record it relates to in such a way that any changes to the record would invalidate the signature. Through these criteria, an electronic signature is uniquely linked to the signer and tamper-proof, protecting the integrity of the associated record.
- Section 31 establishes the framework governing the use of electronic records and electronic signatures by the government and its agencies. It provides that when a public authority performs any of the its key functions (set out in subsection (1) of Section 31), by means of electronic records or in electronic form, the public authority may specify "the control processes and procedures that may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; or (e) any other required attributes for electronic records or payments that are currently specified for corresponding paper." These requirements reflect the requirement of records to be processed with confidentiality, security and integrity.

Data subject rights

The Bill does not provide for data subject rights in relation to the right to access, correct or erasure their personal data provided in the context of e-signatures.

Cross-border transfers of personal data

Section 25 addresses the cross-border recognition of electronic signatures as it pertains to the foreign certificates and signatures in relation to their legal effectiveness. Additionally, the Bill allows parties to agree on the types of electronic signatures or certificates they prefer to utilize for their transactions.

Institutions and penalties

The Bill does not establish any relevant institutions.

Section 38 penalizes the activity of intentionally submitting or sharing false or misleading information, whether in official filings or to individuals using electronic signatures. It provides that it is an offence when a person "(a) files information required under this Bill that contains false or misleading information; or (b) provides a consumer or a user of an electronic signature with false or misleading information."

Conclusion

While the Electronic Transactions Bill provides a framework for regulating electronic signatures, electronic communications and ensuring the validity of electronic documents and signatures, it addresses inadequately most aspects pertaining to data protection. The Bill would not conflict with a data protection framework aligned with international good practices. It would be supplemented from its provisions especially as it pertains to security safeguards and cross-border data transfers. It would also ensure that both originators and addressees are held accountable for the responsible processing of personal data.

4 Legal and regulatory review of national legislation

We turn to our review of the legislation in the ECCU member states in order to carry out a gap analysis at the national level. We reviewed the national legislation of each ECCU member state across thirteen thematic areas:

- Data protection
- Cybersecurity and cybercrimes
- Consumer protection
- Freedom of information requests
- Health
- Education
- Financial Services (including digital financial services)
- National identification (including digital and functional forms)
- Passports
- Civil registration
- Electronic communications
- Electronic transactions
- E-signatures

Through our review we identified provisions related to the collection, processing, sharing, transfer, or storage of personal data or the individual rights of individuals commonly included in data protection. We also describe how these provisions might overlap, conflict, or need to be harmonized with any general regional data protection legislation, if applicable.

We applied the same evaluation approach to regional legislative and regulatory frameworks.

4.A Anguilla

4.A.1 Data protection

Anguilla does not have a framework governing the protection of personal data.

4.A.2 Cybersecurity and cybercrimes

There is currently no legislation in this area.

4.A.3 Consumer protection

There is currently no legislation in this area.

4.A.4 Freedom of information requests

There is currently no legislation in this area.

4.A.5 Health

Introduction, scope of application and definition of key terms

The Department of Health Services Act 2024 provides the legal framework for the efficient administration of health care services in Anguilla. Additionally, it provides for the dissolution of the Health Authority of Anguilla and replaces it with the Department of Health Services, under the Ministry of Health.

It covers personal data and provides certain relevant definitions: “health information” is defined as information that “(a) a health service provided to an individual; and (b) any other information prescribed for the purpose of this definition”. Also, Section 19 provides that health information is deemed “self-

identifying" if the individual's identity can be readily ascertained from the information, whereas "non-identifying" health information is data from which the individual's identity cannot be readily determined.

Although the Act does not define word "processing", it refers to activities that involve processing health information such as access, use and disclosure of health data throughout the Act. These activities constitute forms of personal data processing.

Lawful basis for processing

Hospitals and other healthcare providers process patients' personal health data, under the lawful basis of fulfilling their contractual relationship. In addition, medical providers often operate under the legal mandate of this Act when collecting and retaining patient data to satisfy their statutory record-keeping requirements.

Obligations of the entity processing personal data

Section 19(2) reflects the principle of confidentiality by prohibiting the disclosure of personal health data, unless authorized under the Act. Additionally, Section 19(4) outlines specific circumstances under which disclosure of personal data is permitted.

Data subject rights

Under Part 3, the Act provides several data subject rights:

- Section 10 provides that individuals have the right to access records that contain health information about themselves, which reflects the data subject right to access.
- Section 16 provides individuals with the right to correct or amend their information, if they believe there is an omission or error, which reflects the right to rectification. This Section also provides that individuals submit a statement of disagreement if they are denied their right to correct their data.

Cross-border transfers

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Department of Health Services, established under the Ministry of Health, is responsible for the implementation of the Act.

The Act penalizes the disclosure of personal data in violation of the provisions of the Act by placing a fine of $5,000.

Conclusion

This Act includes provisions that uphold confidentiality of personal data and provide data subject rights to individuals. However, it does not offer adequate security safeguards and requirements for transparency, data minimization and data accountability. A generally applicable data protection law would supplement this framework.

4.A.6 Education

There is currently no legislation in this area.

4.A.7 Financial services (including digital financial services)

We understand that Anguilla has enacted a Banking Act 2015 on the same basis as the other state parties to the ECCB Agreement. We have not been able to obtain a copy of the Act but it is reasonable to assume that it is the same as adopted in the other countries. The same issues mentioned there (e.g., see 4.B.7 for Antigua

and Barbuda) would be the same in Anguilla. Here, we review the other act governing financial services, the Financial Services Commission Act 2022.

Introduction, scope of application and definition of key terms

The Financial Services Commission Act Cap F28 of 2022 establishes a Commission responsible for administering financial services in Anguilla. Its duties include overseeing licensees, maintaining relationships with entities engaged in financial services, and offering guidance to both licensees and the public.

In setting out its processes, rights and obligations, the Act repeatedly uses the term "persons." While it does not explicitly define this term, it is contextually understood to encompass both individuals and legal entities. The following activities set out in the Act involve personal data processing:

- Sections 4 and 8 focus on the appointment of the members and the Director of the Commission, a process which likely involves processing of their personal information. Details about these individuals, such as their educational background, qualifications, and other personal attributes—are assessed to determine if they are "fit and proper" for their positions. Likewise, under Section 43, personal data may be processed for the purpose of removing directors and other officers of a licensee.
- Section 21 provides that the Commission may request licensees to provide specific information and documents which are likely to contain personal data.
- Similarly, Section 24 provides that the Magistrate has the right to issue a warrant and perform a search at a person's home, take possession of items and documents, make copies and request any additional information. This search and collection of relevant materials is likely to involve the processing of personal data.
- Section 26 provides that the Commission may, under specific conditions and circumstances, disclose information and documents to foreign authorities. This information is likely to contain personal data.
- Section 39 states that the Commission may appoint investigators, to conduct investigations on its behalf on issues regarding licensees "(a) the nature, conduct or financial condition of the person's business; (b) a particular aspect of the person's business; (c) the ownership or control of the person being investigated; (d) in the case of a licensee, whether there are grounds for taking enforcement action against the licensee; (e) whether the person is carrying on, or has carried on, unlicensed financial services business." Investigating these matters is likely to involve the processing of personal data.

These activities outlined above constitute forms of processing of personal data.

Lawful basis of processing

The Commission, investigators, and authorized individuals process personal data as part of the activities specified in Sections 4, 8, 21, 26, and 39, operating under a lawful basis of fulfilling legal obligations imposed by this Act.

Obligations of the entities processing personal data

The Act provides limited obligations to entities processing personal data, which reflect certain data protection principles.

- Section 22 requires the Commission to keep confidential any information or documents provided in response to a notice, meaning the Commission cannot disclose this information to any third party unless it is "(a) required or permitted to do so by the Court" or "(b) authorized under the

Act." This requirement ensures that personal information is used solely for its intended purpose and remains confidential, thus safeguarding individuals' privacy.

- Section 27 provides that information relating to a person's business or affairs, acquired by individuals in the course of their duties, under the relevant financial services laws, are considered "protected information".
- Conversely, information is not considered protected, if made publicly available or disclosed in a way that doesn't identify individuals. Protected information is prohibited from being disclosed without the consent of both the source of the information and the person to whom it relates, except as permitted by other provisions. This provision echoes the principle of confidentiality.

Data subject rights

The Act does not address any data subject rights.

Cross border transfers of personal data

- Sections 25 and 26 refer to the Commission's duty to cooperate with foreign regulatory authorities, which may include sharing documents and other information for the purpose of assisting foreign authorities. Sharing information is likely to include personal data transferred abroad.
- Section 26(7)(c) provides that the Commission must be satisfied that the foreign regulatory authority is subject to adequate legal restrictions on further disclosure of information and documents. The foreign authority is prohibited from disclosing the information to anyone other than its officers or employees engaged in supervisory functions, or from taking any action based on the information, without the Commission's written permission.

Institutions and penalties

Under Section 2, the Act establishes the Financial Services Commission.

Under Section 27, disclosing "protected information" is classified as an offense. Schedule 4—which outlines offenses under the Act—prescribes a $50,000 penalty for corporate entities violating Section 27, while individuals face a $10,000 fine, up to 12 months' imprisonment, or both.

Conclusion

Although this Act reflects the principles of confidentiality of information and prohibits the disclosure of data that is qualified as "protected information", it does not contain safeguards to personal data. The Act would benefit from provisions requiring technical and organizational safeguards of personal data, as well as structured mechanisms for safe transferring personal data across borders. However, this Act would not conflict with a generally applicable framework that would align with international good practices.

4.A.8 National identification (including digital and functional forms)

There is currently no legislation in this area.

4.A.9 Passports

There is currently no legislation in this area.

4.A.10 Civil registration

Introduction, scope of application and definition of key terms

The Registration of Births, Deaths and Marriages Act Cap R35 governs the registration of births, deaths and marriages in Anguilla and provides the framework for maintaining accurate records.

The registration of these life events is performed by the Registrar General, and by other authorized persons, and involves the processing of personal data in several instances:

- Sections 7 and 8 provide that every birth of a child or death shall be registered in the general register office and sets out the information that shall be provided according to whether the child is considered "legitimate", "illegitimate" or there was an event of a still birth, under the Act.
- Section 5 provides that births, deaths and marriages shall be registered with the Registrar General.
- Section 11 provides that children born in Anguilla shall get be given a name through baptism and that their parents shall deliver their certificate of baptism to the Registrar General.
- Section 14 provides that persons whose information is included in the births and deaths or marriages shall sign their name and provide place of abode.

The types of personal data required for the registration of births, deaths, and marriages are detailed in Schedules 1-3 of the Act. The actions of collecting, registering and maintaining personal data about these life events are forms of personal data processing.

Lawful basis

The Act provides a lawful basis for processing, inasmuch as it requires (a) individuals to furnish personal data to register births, deaths, and marriages and (b) the Registrar General to record and disclose the data in certificates (Section 17). The processing of personal data during the act of registration of the event is carried out based on the lawful basis of fulfillment of a legal obligation. Subsequent processing activities carried out by the Registrar General are performed as part of their official duties under the Act.

Subsequently, the Registrar General and relevant officials process this personal data in accordance with the statutory mandate of the Act and subsequent regulations to maintain accurate and official records of civil status.

Obligations of the entities processing personal data

The Act reflects some key principles of data protection. Specifically, the Registrar General, who is responsible for collecting, storing, sharing, and processing the personal data:

- is required to process data for the purposes of record keeping, issuing certificates and other purposes as indicated within the Act (purpose specification principle).
- shall make any corrections deemed necessary to maintain the data accurate, updated, and free from clerical errors (Section 12), as well as imposing penalties for reporting false information (under the requirements described in Section 19) (data quality principle).

Additionally, the Act provides that any person who destroys, misuses or processes information in unlawful ways, as described in Section 18, is guilty of an offence and on conviction is liable for imprisonment for a term of 5 years. This is more an expression of cybercrime law, but in some ways reflects data security and data quality principles. However, there is no specific principle of confidentiality and secrecy. Also, the Act does not require the Registrar to implement any technical or organizational measures to ensure the security of the data.

Data subject rights

- Section 12 reflects the data subject right of data rectification by stating that the Registrar General may correct any clerical errors in civil status and provide the exact procedure to do so.
- Section 7 reflects the right to access, by stating that the public may search for the indices of certified copies of registers and obtain copies.

Cross-border transfers of personal data

The Act does not address the cross-border transfer of personal data.

Institutions and penalties

The Act provides that the Registrar General and the general register office are the main entities responsible for implementing the provisions of this Act.

The Act provides for penalties for:

- failing to register a birth, death, or marriage (Section 17, penalty up to $960);
- willful destruction of a register or sheet (Section 18, imprisonment up to 5 years); and
- making false statements (fine of $1,520 or imprisonment of 6 months on summary conviction or 5 years on conviction on indictment).

Conclusion

The Act requires the provision, recording and disclosure of certain personal data in connection with births, deaths and marriages that would be regarded as "processing" of personal data under a typical data protection law. The Act indirectly (albeit thinly) reflects a few key data protection principles in relation to such processing but omits important ones such as confidentiality and data security. As a result, the introduction of a generally applicable data protection law (i.e., that did not exclude the processing under this Act) would raise the level of protection of personal data across the board in the civil registration process. Nothing in the Act contradicts or would be inconsistent with a general data protection law, and so no amendment would be required to the Act and no special accommodation would be required in the new general data protection law.

4.A.11 Electronic communications

Introduction, scope of application and definition of key terms

The Telecommunications Act Cap T6 governs telecommunication operations and services in Anguilla. It outlines the responsibilities of the Minister and the Telecommunications Commission, establishes procedures for issuing licenses and frequency authorizations, and addresses matters such as interconnection and facility access, universal services, road works, terminal equipment and technical standards, as well as testing and inspection.

The Act addresses the processing of personal data by referencing the information of "users, operators, or service providers," which may be used for network and service operations, billing and charge collection, protecting rights or property, and preventing fraudulent network use—activities that all involve personal data processing. It also contains certain limited provisions on personal data processing, Section 8 outlines the obligation to maintain confidentiality, and Section 46, criminalizes the unauthorized disclosure of personal data.

Lawful basis for processing

The Act contains a few bases for processing personal data:

- Section 8 provides that the disclosure of information obtained in connection with the operation of the network shall be kept confidential, except when permitted by the user. This information may contain personal data, and is provided by provided by the users, in compliance with their contractual obligations with operators and providers. Section 8 requires that information obtained in the course of operating a network remain confidential unless the user permits its disclosure. This information, often containing personal data, is provided by users under the lawful basis of their contractual obligations to operators and service providers.

- Section 54 states that the Governor may order telecommunications network operators and service providers to intercept communications or otherwise furnish user information in aid of law enforcement or national security. The disclosure of personal data under this provision constitutes a legal obligation pursuant to the Act, specifically for law enforcement or national security purposes.

Obligations of the entities processing personal data

Section 8 requires telecommunication operators and service providers to maintain confidentiality of user information, by limiting disclosure to operational needs or legal requirements. This provision reflects the personal data principle of confidentiality and integrity, as well as the principle of purpose limitation, by requiring personal data to be disclosed when necessary for operational needs or legal obligations.

Data subject rights

The Act does not address data subject rights.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act does not establish a new institution but refers to the Public Utilities Commission ("Commission"), established under the Public Utilities Commission Act. Section 3 of the Act outlines the functions of the Commission, and Section 38 provides the Commission with the right to entry, search and inspection.

Under Section 46, a person who intentionally discloses any communication that knows was obtained in violation of section 40(1)(e) or who intentionally uses or discloses any personal information in violation of section 8 commits an offence and is liable on summary conviction to a fine of $5,000.

Conclusion

The Act places very limited obligations on entities processing personal data of users, subscribers, and other providers and lacks most data protection safeguards, such as security measures, data subject rights, provisions for cross-border data transfers, and specific penalties for data protection breaches. A generally applicable data protection law would help fill the data protection related omission of this Act.

4.A.12 Electronic transactions

Introduction, scope of application and definition of key terms

The Electronic Transactions Act Cap E38 governs electronic transactions in Anguilla, and gives legal effect, to electronic records and signatures. It mandates the legal recognition of electronic records, ensuring that they are not denied due to their electronic nature, the requirement for retention electronic records in compliance with legal or contractual obligations, the accessibility of electronic records, and the admissibility of the same in legal proceedings.

This Act addresses the processing of personal data within the context communications of electronic records between two parties, referred to as "the originator" and "the addressee." As defined in Section 1:

- "originator, in relation to an electronic record, means a person who— (a) sends an electronic record; (b) instructs another to send an electronic record on his behalf; or (c) has an electronic record sent by his electronic agent; but does not include— (d) a person who sends an electronic record on the instructions of another; or (e) a person acting as an intermediary with respect to that electronic record;

- "addressee, in relation to an electronic record, means a person who is intended by the originator to receive the electronic record, but does not include a person acting as an intermediary with respect to that electronic record;

Electronic communications between an originator and addressee will often include the following personal data: their names, email addresses, metadata such as the time and location of an email, identifiers included in a signature (phone numbers, physical addresses, and other contact details may be shared directly within the email content), along with any information revealed in the context of their communication. According to the definition of "electronic communications", which cover information "generated, communicated, processed, sent, received, recorded, stored, or displayed by electronic means", personal data undergo "processing" as they are transferred by the originator and subsequently received and stored by the addressee.

Also, the Act defines personal data as "data which relate to a person who can be identified— (a) from those data; or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller; and includes any expression of opinion about that person and any indication of the intentions of the data controller or any other person in respect of that person"

Lawful basis for processing

- Section 2 provides legal recognition of electronic transactions and Section 3 allows information that would otherwise be required to be provided in writing to be provided electronically. Providing personal data through electronic transactions constitutes personal data processing based on contractual necessity and is legitimized through the lawful obligations under this Act.
- Section 7 provides that records, documents and information may need to be made available for inspection. Sharing information through inspections may cover personal data and is a form of personal data processing based on legal obligation from this Act.

Obligations for entities processing personal data

Under Section 31, the Governor has the authority to establish regulations that "prescribe standards" for the processing of personal data. While the Act itself does not impose direct obligations on entities processing personal data, it empowers the Governor to create such obligations through regulations. Violating these regulations would result in penalties.

Section 23 provides that information concerning an individual's private affairs or a specific business is deemed confidential. Whether pertaining to personal details or business matters, this sensitive information is protected from disclosure.

Data subject rights

Section 12 governs how to handle errors or alterations in the transmission of electronic records, offering remedies that permit parties to avoid the effects of erroneous records under certain conditions. This provision loosely mirrors the data subject right of data rectification—at least to the extent that electronic records include personal data.

Cross-border transfer of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

Under Section 32 provides that a data controller or data processor who voluntarily registers to a data protection standard and who fails to comply with that standard, is guilty of an offence and is liable on summary conviction to a fine of $50,000, or to imprisonment for 6 months, or to both; and if the offence of which they are convicted is continued after conviction that data controller or processor commits a further offence and is liable to a fine of $5,000 for every day on which the offence is so continued.

Conclusion

The Electronic Transactions Act contains minimal safeguards for the protection of personal data. Therefore, it would not conflict with a data protection framework aligned with international good practices. It would be supplemented by its provisions especially as it pertains to confidentiality obligations, security safeguards and cross-border data transfers. It would also ensure that both originators and addressees are held accountable for the responsible processing of personal data.

4.A.13 E-signatures

Introduction, scope of application and definition of key terms

The Electronic Evidence Act of 2022 provides a framework that validates electronic signatures and regulates their use and their related procedures. It also facilitates cross-border recognition of electronic signatures and establishes obligations for entities and individuals who rely on them.

Under Section 1, "electronic signature" means data in electronic form, incorporated into or otherwise logically associated with any electronic data or communications, and adopted by a person with the intent to indicate their approval and agreement to the content. It is an attribute which constitutes personal data and has binding authority under the conditions described in the Act.

E-signatures are also covered through Sections 15-20 of the Electronic Transactions Act.

Lawful basis for processing

Section 13 of the Electronic Evidence Act requires that parties shall agree regarding the specific method of electronic signature that they would use in their transaction. The contractual obligation between the parties constitutes a lawful basis for processing the personal data embedded in the signatures.

Obligations for entities processing personal data

Sections 13 and 15 of the Electronic Evidence Act require entities using electronic signatures to ensure their reliability. In addition, Section 18 mandates that these entities verify the reliability of their signatures. Together, these provisions loosely echo the data protection principles of data accuracy and data integrity.

Data subject rights

The Act does address data subjects' rights.

Cross-border transfers of personal data

Section 19 of the Electronic Transactions Act outlines the process for recognizing foreign electronic signatures and certificates, specifying that they must meet equivalent reliability standards.

Institutions and penalties

Under the Electronic Evidence Act, the Governor has the authority to establish standards for the reliability of electronic signatures and to introduce any necessary regulations. The Act also imposes penalties on entities that rely on electronic signatures but fail to verify their reliability or adhere to certificate limitations under Section 18. Additionally, Section 35(2) provides that regulations made under this Act may classify certain violations as offenses and prescribe penalties—up to the maximum fine and imprisonment term specified for any offense under the Act.

Conclusion

Both the Electronic Transactions Act and the Electronic Evidence Act focus on the legal recognition and validation of electronic signatures. However, they lack most safeguards regarding protection of personal data. Most importantly, a generally applicable data protection law would fill these omissions and would not conflict with the existing framework.

4.B Antigua and Barbuda

4.B.1 Data protection

Overview

Antigua and Barbuda's legal framework on protection of personal data is governed by the Data Protection Act of 2013 ("Act"), which passed into law through Law No. 10 of 2013. The Act covers the processing of personal data by both private and public sector entities. It also provides that the Information Commissioner appointed under the Freedom of Information Act, 2004 shall be the responsible authority for overseeing and enforcing the Act. This Act largely mirrors the OECS model Bill of 2016.

While the Act establishes certain key rights and obligations regarding protection and processing of personal data, it does not include some key elements from the international good practices outlined in Section 2 of this report.

Scope of applicability

The section below is generally consistent with international good practices, applying to both private and public entities, and defining personal data to include automated processing. However, the Act's scope is overly restrictive, covering only a limited range of processing activities. To fully align with global standards, the scope should be expanded.

Applicability limited to "commercial transactions"

Similar to the OECS Model Bill, this Act restricts the definition of personal data to information "related to commercial transactions." A detailed analysis and recommended approach regarding this limitation are provided in the context of the OECS model Bill, as discussed in Section 3.A.1of this report.

Broad exemption for processing by regulatory authorities

Similar to the OECS Model Bill, Section 19(2)(e) of the Act exempts from several of the data protection principles personal data that is processed for the purpose of discharging regulatory functions. (See Section 3.A.1 of this report.)

General elements of data protection law

Some of the definitions contain contradictions, lack clarity, and would require revision to align with international good practices.

Definition of "personal data" is potentially limiting

As with the OECS Model Bill, the Act definition of personal data may limit the application of the Act. (See Section 3.A.1 of this report.)

Definition of "sensitive personal data" excludes important attributes

As with the OECS Model Bill, the Act's definition of sensitive personal data omits attributes that should be afforded additional safeguards when being processed. (See Section 3.A.1of this report.)

Use of the terms "data users," "public bodies," "private bodies" and "persons"

As with the OECS Model Bill, the Act uses the terms "data users", "private bodies", "private bodies" and "persons" inconsistently. This drafting approach creates limitations, confusion and shall be revised. (See Section 3.A.1of this report.)

No definition of "consent"

As with the OECS Model Bill, the Act does not define "consent". (See Section 3.A.1of this report.)

No clear concept of a "data processor"

As with the OECS Model Bill, the Act does not define "data processor". (See Section 3.A.1of this report.)

Relation with other national legal instruments

As with the OECS Model Bill, Section 4 of the Act concerning its effect on other laws may confuse matters. (See Section 3.A.1of this report.)

Principles governing the processing of personal data

The Act reflects data protection principles in its Sections 5-11, addressing lawful bases, security, purpose limitation, and data quality. However, the current formulation of these principles could be improved.

Principle of lawful, fair and transparent processing

As with the OECS Model Bill, the Act does not include a principle mandating that personal data be processed in a lawful, fair, and transparent manner, as is required by established global best practices. (See Section 3.A.1of this report.)

Principle of data minimization

As with the OECS Model Bill, the Act does not explicitly include a "minimum necessary" standard for processing of personal data. (See Section 3.A.1of this report.)

Lawful basis for public interest

As with the OECS Model Bill, the Act does not include a lawful basis on necessity for substantial public interest. (See Section 3.A.1of this report.)

Additional protection for processing personal data of children or persons with limited capacity to consent

As with the OECS Model Bill, the Act does not include additional protections for the processing of personal data for children and persons lacking the legal capacity to consent. See Section 3.A.1of this report.)

Limitations on data retention do not have exceptions

As with the OECS Model Bill, Section 9 sets out the "*retention principle*", but limiting personal data retention by data users too tightly. (See Section 3.A.1of this report.)

Individual rights concerning personal data

Sections 12-16 of the Act outline the key data subject rights and sets out the circumstances and timelines, under which they shall be exercised. While they are largely aligned with international good practices, the Act does not provide the rights of data subjects to withdraw consent, oppose the processing of their personal data with automated means, and delete their personal data. (See Section 3.A.1of this report.)

Data security

The Act has several significant omissions, notably the lack of requirements for data processors and data controllers to provide notifications in the event of a data breach.

Lack of specific data security requirements

Section 8 of the Act outlines the obligation of a data user to process personal data securely –

"when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard to- (a) the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction; (b) the place or location where the personal data is stored; (c) any security measures incorporated into any equipment in which the

personal data is stored; (d) the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and (e) the measures taken for ensuring the secure transfer of the personal data".

As with the OECS Model Bill, the Act could provide greater specificity to support effective security frameworks for safeguarding personal data. (See Section 3.A.1of this report.)

No personal data breach notification obligations

As with the OECS Model Bill, the Act does not include any personal data breach obligations. (See Section 3.A.1of this report.)

No requirements on data users when engaging data processors

As with the OECS Model Bill, the Act does not require data users to take any measures to ensure that data processors can assist them in complying with the Act. (See Section 3.A.1of this report.)

No data processor liability for data security

Section 8(1) addresses data security requirements for data users. Section 8(2) addresses data security requirements for data processors, but, as with the OECS Model Bill, it does not make data processors directly liable for failure to adopt adequate data security measures. (See Section 3.A.1 of this report.)

No requirement for Data Privacy Impact Assessments (DPIAs)

As with the OECS Model Bill, the Act does not mandate that data users conduct Data Protection Impact Assessments (DPIAs). (See Section 3.A.1of this report.)

Cross-border data transfers of personal data

As with the OECS Model Bill, the Act does not include provisions on cross-border data transfers. (See Section 3.A.1of this report.)

Institutions

Our internal research and contacts attempted by our local team members were not able to locate an online presence or physical establishment of the Information Commissioner.

Lack of provisions on the funding of the Commissioner

As with the OECS Model Bill, neither the Act nor the Freedom of Information Act that establishes the Information Commissioner provides for the funding of the Commissioner. (See Section 3.A.1 of this report.)

Penalties and enforcement

Limited scope of data subject complaints to the Commissioner

The Act does not establish a clear mechanism for data subjects to file complaints with the authority when they suspect or experience a violation of a data user's obligations under the Act. The complaints provisions under the Freedom of Information Act, which the Commissioner also administers, would not be suitable for data protection complaints, as those relate to cases involving the denial of access to information. We recommend amending the Act to introduce a mechanism that allows data subjects to file complaints regarding violations of any provision of the Act by data controllers. This mechanism should also outline the process the Commission must follow upon receiving such complaints, consistent with international good practices.

Disproportionate and unclear fines and penalties

We would also discourage the use of criminal offences for data protection violations. (See Section 3.A.1 of this report.)

Introduction, scope of application and definition of key terms

The Electronic Crimes Act 2013 of Antigua and Barbuda aims to prevent and punish electronic crimes within the jurisdiction. The Act covers various offences which can affect personal data, including access and interference, sending offensive messages, misuse of encryption, electronic terrorism and identity theft.

The Act does not include an explicit definition of personal data, but defines "data" as: "representations of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including electronic program, text, images, sound, video and information within a database or electronic system."

This broad definition does not differentiate between personal and non-personal data and so the Act's prohibitions and obligations apply to what are commonly referred to in data protection laws as "personal data."

Also, despite not explicitly defining the term "processing", the Act references numerous activities performed on computer systems that deal with data, including: "collect", "access", "damage", "tracking", "modify."

Lawful basis for processing

In the Act's various offences (Sections 3-15) of accessing, misusing, forging, interfering with data "without lawful excuse or justification", the requirement for authorization echoes the data protection principle of consent, which is a basis of lawful processing. The offences outlined in the Act occur when such consent is not present.

Additionally, information and personal data collected and processed in the context of an investigation, as provided in Sections 16-25 , are processed in accordance with the lawful basis of lawful obligation under the Act. It could be also argued that, according to the nature of the data and the investigation, the processing is performed on the basis of national security and public interest.

Broadly, these provisions seek to ensure that processing is aligned with established legal requirements under the Act.

Obligations of the entity processing personal data

Although the Act does not provide affirmative general data processing obligations (only criminal prohibitions), it reflects some notions often included in data protection laws:

Section 10: Establishes the parameters that constitutes child pornography as a crime and fees and penalties.

Section 8: This Section titled "violation of privacy" makes it an offense to intentionally or without lawful excuse capture, publish, or transmit images of a person's private area or an image of a person in a vulnerable position without their consent, under circumstances that violate their privacy. The penalties for this offense are either a fine up to one hundred thousand dollars or imprisonment for up to two years (summary conviction), or a fine up to two hundred and fifty thousand dollars or imprisonment for up to five years (conviction on indictment). Additionally, if the victim is disabled or mentally incapacitated and unable to consent, the offender faces the same penalties as specified, regardless of the victim's capacity to consent. While this provision provides a narrow interpretation of privacy, it reflects the principle of personal integrity and confidentiality, which is aligned with the internationally recognized data protection principles.

Data subject rights

The Act does not address data subject rights.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Enforcement

The Act does not establish a relevant authority or institution. However, it provides penalties for the following offences that can relate to the processing of personal data:

- Identity theft: under Section 5 a person shall not make use of any electronic signatures, passwords or identifying features of another person. This offence attracts a fine not exceeding $200,000 or imprisonment for a term not exceeding 3 years or both (summary conviction), or a fine not exceeding $500,000 or imprisonment for a term not exceeding 7 years or both (conviction on indictment)
- Misuse of encryption: a fine not exceeding $100,000 or imprisonment for a term not exceeding 2 years or both (summary conviction) or a fine not exceeding $250,000 or imprisonment for a term not exceeding 5 years or both (conviction on indictment).

Conclusion

This Act broadly addresses two forms of processing that would relate to typical data protection law. The first is prohibiting certain forms of data processing, particularly those that were performed without lawful authority or having other criminal aspects. The second is to affirmatively require certain procedures (e.g., judicial order) for police and other authorized persons to obtain data (which would include personal data) in the context of investigations and prosecution. In doing so, the Act establishes a framework for combating cybercrimes and incorporates some minimal provisions that align with data protection principles. However, it does not include many typical data protection provisions, e.g., security standards and institutional structures, which are essential for effectively safeguarding personal data involved in the prohibited or authorized processing activities.

A generally applicable data protection framework that aligns with international good practices would address these gaps in providing the necessary supplementary measures to ensure robust protection of personal data.

4.B.2 Cybersecurity and cybercrimes

Introduction, scope of application and definition of key terms

The Electronic Crimes Act 2013 (amended by Act No. 25 of 2018) of Antigua and Barbuda aims to prevent and punish electronic crimes within the jurisdiction. It covers various offences (Sections 3-15) including unauthorized access and interference to computer systems, sending offensive messages, misuse of encryption, electronic terrorism and identity theft. Additionally, it facilitates the collection of electronic evidence crucial for criminal investigations. To achieve these goals, the Act establishes rules and protocols for data handling and processing. It also enforces strict criminal penalties for specified offenses to deter malicious activities and promote responsible use of computer technologies.

The Act defines the term “data” as: “representations of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including electronic program, text, images, sound, video and information within a database or electronic system.” This broad definition does not differentiate between personal and non-personal data.

Also, despite not explicitly defining the term “processing”, the Act references numerous activities performed on computer systems that deal with data, including: “collection”, “access”, “damage”, “tracking”, “modifying.”

Lawful basis for processing

In the Act's various offenses—such as accessing, misusing, forging, or interfering with data "without lawful excuse or justification"—the need for authorization aligns with the data protection principle of consent, a key foundation for lawful processing. Essentially, these offenses arise whenever consent is not granted, thereby underscoring the importance of ensuring proper authorization before handling data.

Additionally, both personal and non-personal data collected and evaluated during investigations are processed under the lawful basis of fulfilling obligations set out in the Act. Depending on the scope of the investigation, it can also be argued that the processing is conducted in the interest of national security or public welfare.

Broadly, these provisions seek to ensure that processing is aligned with established legal requirements under the Act.

Obligations of the entity processing personal data

Although the Act does not provide affirmative general data processing obligations (only criminal prohibitions), it reflects some notions which are often included in data protection laws:

- Section 10: Establishes the parameters that constitute child pornography as a crime and provides fees and penalties.
- Section 8: This Section titled "violation of privacy" makes it an offense to intentionally or without lawful excuse capture, publish, or transmit images of a person's private area or an image of a person in a vulnerable position without their consent, under circumstances that violate their privacy. The penalties for this offense are either a fine of up to one hundred thousand dollars or imprisonment for up to two years (summary conviction), or a fine up to two hundred and fifty thousand dollars or imprisonment for up to five years (conviction on indictment). Additionally, if the victim is disabled or mentally incapacitated and unable to consent, the offender faces the same penalties, regardless of the victim's capacity to consent. While this provision refers to privacy through the scope of bodily intimacy, and not as a generally applicable right, it reflects the intention of personal integrity and personal autonomy, which is aligned with the internationally recognized data protection principles.

Data subject rights

The Act does not address data subject rights.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act does not establish an authority or institution. However, it provides penalties for the following offences, which may involve the processing of personal data:

- Section 5 defines identity theft as an offence, and states that a person shall not make use of any electronic signatures, passwords or identifying features of another person. This offence attracts a fine not exceeding $200,000 or imprisonment for a term not exceeding 3 years or both (summary conviction), or a fine not exceeding $500,000 or imprisonment for a term not exceeding 7 years or both (conviction on indictment).
- Section 8 states that any person who intentionally and without lawful excuse or justification publishes or transmits an image of a private area of another person, or an image of a person in a vulnerable position, without their consent, commits the offense of violation of privacy. However, this provision interprets privacy in a narrow sense, focusing on bodily privacy rather than

encompassing the broader right to privacy as recognized in international data protection frameworks. A person committing this offence is liable for summary conviction to a fi ne not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding two years, or to both; or (b) on conviction on indictment to a fi ne not exceeding two hundred and fifty thousand dollars or to imprisonment for a term not exceeding five years, or to both.

Conclusion

This Act broadly addresses two forms of processing related to typical data protection law. The first is prohibiting certain forms of data processing, particularly those that were performed without lawful authority or having other criminal aspects. The second is to affirmatively require certain procedures (e.g., judicial order) for police and other authorized persons to obtain data (which would include personal data) in the context of investigations and prosecution. In doing so, the Act establishes a framework for combating cybercrimes and incorporates some minimal provisions that align with data protection principles. However, it does not include many typical data protection provisions, e.g., security standards and institutional structures, which are essential for effectively safeguarding personal data involved in the prohibited or authorized processing activities.

A generally applicable data protection framework that aligns with international good practices would address these gaps in providing the necessary supplementary measures to ensure robust protection of personal data.

4.B.3 Consumer protection

Introduction, scope of application and definition of key terms

The Consumer Protection and Safety Act, Cap 97 covers issues related to consumer protection in Antigua and Barbuda. However, it does not include any provisions relevant to the processing of personal data.

Additionally, limited consumer protection provisions are included in the Electronic Transaction Act, which will be analyzed in the Section titles "Electronic Transactions" below. Under Section 36 of the Electronic Transactions Act, a person using electronic communications to sell goods or services to consumers is required to provide accurate clear and accessible information about themselves including inter alia (a) the legal name of the person, its principal geographic address and an electronic means of contact or telephone number. Aside from this Section, no other provisions relate to the processing or obligations related to personal data.

4.B.4 Freedom of information requests

Introduction, scope of application and definition of key terms

The Freedom of Information Act No. 19 of 2004 aims to promote the disclosure of information in the public interest, ensure the right of access to information, and establish effective mechanisms to protect that right in Antigua and Barbuda. The Act's objective of promoting transparency may seem to conflict with protecting personal data, which calls for the need for reaching a balance between confidentiality and security measures within freedom of information. However, the Act contains only minimal provisions addressing the protection of personal data.

The Act defines personal information as "data that pertains to a living individual who can be identified from that information." Personal data may be included in records held by public authorities, thereby falling under the scope of this Act. Personal data is considered to be processed when it is collected, maintained by public authorities, accessed by individuals, and incorporated into records under investigation. These activities constitute different forms of processing of personal data covered by the Act.

Lawful basis for processing

Personal data is processed under the Act based on the lawful obligation to maintain records and provide public access to them, as specified in the Act's provisions.

Obligations of the entity processing personal data

The Act imposes obligations on the public authorities to process personal data, in alignment with the following data protection principles:

- Section 12(3) states that the commissioner must issue an update Code of Practice in relation to the keeping, management and disposal of records and additionally the transfer of records to the Archives and Records office. This practice echoes the principle of data integrity and data confidentiality.
- Under section 26(1) a public authority may refuse to communicate personal data or information under specified circumstances, including where the disclosure has not been consented to. This practice reflects the principle of confidentiality and protection of personal data.

Data subject rights

- Section 12(1) establishes the obligation that every public authority must maintain its records in a manner that facilitates the right of access to information, which echoes the right to access. Section 12(1) imposes an obligation on every public authority to maintain records in a way that facilitates the right of access to information, underscoring the importance of ensuring public accessibility.
- Section 12(2) states that every public authority must establish and maintain adequate procedures that allow the correction of personal information which it holds.

Cross-border transfers of personal data

The Act mentions no provisions in relation to cross-border transfers of personal data.

Institutions and penalties

Section 35 mandates the appointment of the Information Commissioner who would be responsible for overseeing and enforcing the provisions of this Act and ensuring the maintenance of records.

In addition, Section 48 provides that a person is not allowed to perform several activities that interfere with the objectives of the Act that include: (a) obstruct access to records in violation of Part III of the Act, (b) hinder a public authority from performing duties required by Part III, (c) interfere with the work of the Commissioner, (d) destroy, mutilate, remove, or alter records with the intent to prevent disclosure of information, or (e) fail to comply with a decision or order issued by the Commissioner under sections 42 or 43. If someone violates any of these provisions, they commit an offense and are liable to a fine of up to five thousand dollars, imprisonment for up to two years, or both.

Conclusion

The focus of the Freedom of Information Act is the transparency and accountability of public authorities, as opposed to the safeguarding of personal data. Therefore, it provides limited obligations for the protection of personal information. Notably, the Act does not include any technical and organizational requirement for the protection of personal information, nor any requirements for data minimization and data retention. However, this Act would not conflict with a generally applicable data protection framework.

4.B.5 Health

Introduction, scope of application and definition of key terms

The Medical Practitioner's Act of 2009 governs the registration, licensing, and practice of medicine in Antigua and Barbuda. However, the Act does not cover topics such as the handling and protection of patients' data. Instead, it focuses on the roles and responsibilities of the Medical Council, which is tasked with receiving, processing, issuing, and revoking licenses for general practitioners, consultants, and specialists in the country (Sections 13, 13A). Individuals aiming to obtain such licenses are required to

complete a form that requests their personal data, including their name, address, contact details, and academic and professional qualifications. This information is found in Schedule I of the Act. The activity of receiving, assessing and storing this information is considered processing of personal data.

The Antigua Health Act Cap 353 also covers the thematic area of health in Antigua and Barbuda, but it does not cover the processing of personal data.

Lawful basis for processing

Under Sections 13 and 13A of the Medical Act, individuals seeking licensure as registered medical practitioners or consultants are required to provide the Medical Council with the personal data prescribed by the Act. The relevant Board for each profession then reviews this information to determine the applicants' qualifications and issues certificates accordingly. In addition, the Medical Act obligates the storage of personal data for qualified practitioners in medical records. All of these processing activities are carried out on the lawful basis of complying with a legal obligation.

Obligations of the entity processing personal data

Section 11 of the Medical Act requires Medical Council members to maintain the confidentiality of personal information obtained in the course of their duties. Likewise, Section 28 imposes an identical obligation on members of the Disciplinary Committee. Together, these provisions underscore the Act's commitment to protecting personal data. However, the Act does not address security safeguards for personal data or establish retention periods for storing personal data and records.

Data subject rights

The Medical Act does not address data subject rights.

Cross-border transfers of personal data

The Medical Act does not address cross-border transfers of personal data.

Institutions and penalties

The Medical Act establishes the Medical Council, as a responsible body for the registration and licencing of medical practitioners in Antigua and Barbuda. While it does not provide any offences directly targeted to violation of obligations regarding processing of personal data, Section 31 provides an "umbrella" offence, stating that "A person who contravenes a provision of this Act or the regulations for which no specific penalty is provided commits an offence and is liable on summary conviction to a fine of $10,000 or to imprisonment for two years or to both, or on indictment to a fine of $25,000 or to imprisonment for three years or to both."

Conclusion

The aforementioned Acts contain minimal provisions on personal data protection and also contain some data subject rights. However, they lack most key provisions and safeguards in regard to personal data, such as the requirement of security of personal data of registered practitioners, and they do not contain any provisions covering the protection of personal information of patients. Most importantly they do not contain any provisions that would conflict with or impose barriers in the implementation of a generally applicable data protection framework which would be aligned with the international good practices.

4.B.6 Education

Introduction, scope of application and definition of key terms

The Education Act Cap 145 of 1973, amended by Act No. 21 of 2020, covers the regulation, and management of educational institutions in Antigua and Barbuda. While the Act does not define the terms, "personal data", "student data" or "reports", the processing of personal information of students is mentioned in several contexts:

- Section 18 states that upon the admission of a new student, information such as their name, date of admission, names of parents or guardians as well as residence of parents or guardians are required and shall be entered into the admissions register.
- Section 26 provides that admitted students to secondary or comprehensive schools shall be assigned a personal record book or card, which shall be retained by the headmaster and may be made available to the student or their parent upon payment of a fee. This record book is likely to contain personal data.
- Section 59 provides that the following books and logs may be kept and produced for the inspection of the Minister and any authorized officer of the Ministry of Education. Among the records described in the Act, the admission register, class attendance register, logbook, teacher attendance register, visitor's book, punishment book would include personal data, such as individuals' names, descriptions of their behaviors, and other personal attributes.
- Section 48 provides the right to education officers to request the parent apprehend without warrant and deliver to the school from which he is absent or to his parent, any child found illegally absent from school.

The aforementioned activities constitute forms of processing personal data.

Lawful basis for processing

Sections 18, 26, 59, 48: As noted in the previous section, personal data is provided by students and their parents in fulfillment of their obligations under this Act, or in the context of a contract between the student or parent and the school. This data is processed by principals, school attendance officers, and government officials for various purposes outlined in the Act.

These purposes include establishing and maintaining records, performing official functions, accessing and obtaining copies of records, monitoring attendance, and carrying out other administrative duties.

Obligations of the entity processing personal data

The Act does not place any obligations to entities that process personal data.

Data subject rights

Under Section 26(4), students or their parents have the right to obtain, upon application, a copy of a record book or card upon payment of a fee. This right reflects the data subject right of access to personal data.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act does not establish an institution but provides that the Minister "may establish a National advisory Council for the purpose of advising him as to the performance of any of his responsibilities under this Act."

Conclusion

Although the Act covers the processing of personal data of students, it does not contain safeguards for the protection and processing of personal data, including a duty of confidentiality, provisions covering data retention periods, data security measures, or cross-border data transfers. A generally applicable data protection framework, aligned with international good practices, would supplement this Act's provisions.

4.B.7 Financial services (including digital financial services)

Introduction, scope of application and definition of key terms

Financial services in Antigua and Barbuda are governed by three laws: the Finance Administration Act of 2006, the Financial Services Regulatory Commission Act of 2013 and the Banking Act of 2015. Only the latter covers the processing of personal data.

The Banking Act covers the licensing of various financial institutions in the context of which personal data and other information of their shareholders, directors and officers are assessed.

- Section 3(1) requires persons (natural and legal) carrying on banking business or hold themselves as carrying on banking business in the Currency Union to obtain a license granted by the Central Bank. Under Section 7, financial institutions applying for a license to operate to submit various types of information—including personal data—to the Central Bank. The exact types of information are outlined in Schedule 1 of the Act and include name, address, qualifications, and experience of the financial institution's chief executive officer.
- Section 13 provides that the Central Bank shall maintain a central register for each licensed institution, including the name, head office and branch office addresses and class or category of license held.
- Section 8 provides that any director, significant shareholder, or manager of a financial institution shall hold a position within a financial institution, only if Central Bank decide they are "fit and proper" for such position. Determining whether that person as "fit and proper" involves the assessment of their personal information, including their character, professional record, and other personal attributes, as described in Sections 97 and 98.
- Section 59-69 states that the Central Bank shall appoint external auditors the authority to access and review books, records, financial statements of financial institutions, to effectively perform their duties. These records are likely to include personal data.
- Section 88 provides the reasons for the removal of a director or officer from their position, which includes.

The activities of providing, evaluating and storing personal data of individual license applicants, shareholders, directors and other officers described above constitute personal data processing. The above activities of providing, evaluating, and storing personal data for shareholders, directors, and other officers amount to personal data processing.

Lawful basis for processing

The Banking Act provides several bases for processing personal data:

- As outlined in the previous section, director's and officers' personal data are processed for the purpose of the processing of their appropriateness for their designation, maintenance or removal from their position, and pursuant to their obligation under the Act.
- Section 178 discusses the requirement for secrecy of information, and allows individuals associated with licensed financial institutions to disclose information of their customers only where a written authorization of the customer or their legal representative is given, when it is required by law or a court order, and where it is part of an intergovernmental agreement among participating governments. This section reflects the lawful basis of consent and processing of personal data under a court order.

Obligations of the entity processing personal data

- Section 178 requires that no individual who, in their role as a director, officer, employee, agent, auditor, receiver, administrator, or liquidator of a licensed financial institution, acquires knowledge of a depositor's or customer's identity, assets, liabilities, transactions, or other details may disclose such information to any person or authority. Disclosure is allowed only under the following conditions: if the customer or their legal representative provides written authorization, if it is required by law or a court order, or if an intergovernmental agreement applies. This provision mirrors recognized lawful bases for processing personal data, including consent and compliance with a court order. This provision safeguards financial confidentiality while allowing lawful disclosures in specific circumstances.

Data subject rights

The Banking Act, under section 178(2), provides that individuals have the right to request summaries of their credit ratings, which echoes the right to access.

Cross-border transfers of personal data

The Banking Act, under Section 94 allows the Central Bank to enter into formal agreements or arrangements with foreign supervisory or resolution authorities, to facilitate coordination, cooperation, and the exchange of information between the Central Bank and the foreign authorities. The provision also emphasizes a key condition: the Central Bank can only share information if it is confident that the foreign authority has a legal obligation to protect the confidentiality of the shared information in accordance with applicable laws or regulations. The sharing of data is likely to include personal data, such as financial records, credit scores, names of customer data.

This provision reflects the principle of adequacy of protection, which is found in multiple data protection frameworks, and ensures that when personal data is transferred from one jurisdiction to another, the receiving jurisdiction must offer a level of protection that is as robust as what is available in the originating jurisdiction.

Additionally, Section 89 states that, in the interest of public policy, and upon request by the Central Bank, licensed institutions must share personal data with the Central Bank to ensure compliance with the Act. This information is likely to include personal data.

Institutions and penalties

While there is no specific institution established for the enforcement of data protection standards, the Central Bank generally oversees the data collection and processing to ensure compliance and risk management. The penalties for non-compliance or failure to submit the required information or provision of false data carries the penalty of $25,000 per Section 96.

Conclusion

The Act lacks most of the basic provisions covering the protection of personal data, such as confidentiality obligations, especially on data security, data minimization, quality, transparency, and provision on cross-border transfers of personal information. However, these Act would not contradict with a generally applicable data protection framework.

4.B.8 National identification (including digital and functional forms)

There is currently no legislation on this area that has been enacted in Antigua and Barbuda.

4.B.9 Passports

Introduction, scope of application and definition of key terms

The Immigration and Passport Act No. 6 of 2014 provides a framework for the control of the entry and departure of individuals to and from Antigua and Barbuda, and covers issues related to passports. Section 2 defines passports as a "valid official document issued by a Government, certifying the identity and citizenship of the holder of the document and entitling the holder of the document to travel under its protection to and from foreign countries".

While the Act does not specify the types of data to be included in passports, certifying the identity of passport holders typically involves collecting names, dates of birth, signatures, unique numbers, photographs, and gender. The processes of gathering, evaluating, confirming, and incorporating this information into passports constitute the processing of personal data.

Under Section 11, a valid passport or other travel document is required for individuals' entry in Antigua and Barbuda. Under Section 17, passports are provided to and assessed by immigration officers upon individuals' arrival to the country. Also, Section 36 states that citizens of Antigua are entitled to be issued an Antiguan passport and that the contents of the passports and designed and approved by the Cabinet.

Collecting, assessing, verifying and adding this information in passports constitutes processing of personal data.

Lawful basis for processing

When individuals provide personal data for passport issuance, this action constitutes personal data processing, under the lawful basis of complying with the Act. It could be also argued that since immigration control is closely linked with national security, the processing of personal data from passports by officers is based on necessity for public interest.

Obligations of the entity processing personal data

The Act does not impose any obligations to entities processing personal data.

Data subject rights

The Act does not include any data subject rights.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act does not establish any institutions or penalties relevant to personal data.

Conclusion

The Act does not include requirements concerning the processing of personal data, nor does it impose obligations on entities handling personal information regarding confidentiality or data integrity. As such, these Acts would not conflict with any broadly applicable data protection legislation.

4.B.10 Civil registration

Introduction, scope of application and definition of key terms

The Civil Registration (Vital Statistics) Act, 2020 (No. 6 of 2020) sets out requirements for registering vital life events, which in the context of this Act include births, deaths, marriages, divorces, adoptions, and name changes—and addresses related matters.

The registration of these life events is performed by the Registrar General, and by other authorized persons, and involves the processing of personal data:

- Sections 11–21 mandate the registration of births, adoptions, and stillbirths. These processes involve collecting personal data, including parents' names, addresses, dates of birth, marital status, and the mother's number of previous births. The exact information required are listed in Schedule II (Forms A1–A2), which the Registrar processes to issue birth and stillbirth certificates.
- Sections 30–31 require that anyone who dies in a hospital, care facility, home, villa, hotel, or any other building be reported to the Registrar by submitting Forms D1–D2. These forms demand extensive personal information and are processed by the Registrar to issue death certificates.
- Sections 39–43 require the registration of marriages and divorces. Completing these registrations entails providing substantial personal data, which is processed to issue official certificates.
- Section 8 stipulates that the Registrar must keep records of all registered births, adoptions, deaths, marriages, nullities, and divorces. Storing and maintaining these registers constitutes the processing of personal data.

The exact types of personal data required for the registration of the aforementioned life events are detailed in Schedules 2 of the Act. The provision, registration and maintenance of personal information about these life events are considered processing of personal data.

Additionally, Antigua and Barbuda's Civil Registry Act of 2019 establishes the national Civil Registry, the entity responsible for the recording of information regarding vital statistics, change of names, deeds and records, and for the recording of information relating to information identity and for other connected purposes. This Act sets out the obligations and responsibilities of the Registrar and the authorized officials who process information relevant to life events and vital statistics.

Lawful basis for processing

The Civil Registration Act provides a lawful basis for processing inasmuch as it obligates (a)individuals to furnish personal data to register births, stillbirths, deaths, and marriages and (b) the Registrar to record and disclose the data in certificates. The processing of personal data during the act of registration of the event is carried out based on the lawful basis of fulfillment of a legal obligation. Subsequent processing activities carried out by the Registrar are performed as part of their official duties under the Act.

Subsequently, the Registrar General and relevant officials process this personal data in accordance with the statutory mandate of the Act and subsequent regulations to maintain accurate and official records of civil status vital events.

Obligations of the entities processing personal data

- Section 3 of the Civil Registration Act provides that books that are not in use shall be reproduced in a digital format and be kept safe for an infinite period. This provision, which prescribes organizational measures to maintain the records safely, echoes the data protection right of security over personal data.
- Section 21of the Civil Registration Act directly refers to the right to privacy of adoption records, providing that only the Registrar or an authorized individual may search the Registrar of Adoptions and that no information from these records shall be provided except by order of the Registrar. These provisions highlight the sensitive nature of the personal information related to adoptions.

- Section 11 of the Civil Registry Act provides that the Registrar, deputy registrar and all members of staff of the Civil Registry shall sign a confidentiality agreement when in the service of the Civil Registry.

Data subject rights

- Under Sections 23-26 of the Civil Registration Act, individuals have the right, following the prescribed procedure to change their name, which reflects the data subject right of data rectification.
- Section 55 of the Civil Registration Act provides that clerical errors may be corrected by the Registrar, or any person duly authorized in this regard by the Registrar. This provision reflects the right to rectification.

Cross-border transfers of personal data

Neither of the two Acts addresses cross-border data transfers.

Institutions and penalties

The Civil Registration Act outlines offenses and penalties related to providing false information or documents in the registration of births and deaths. Specifically:

- if a person deliberately gives incorrect answers to the Registrar (or their deputy/assistant) about any birth or death.
- If a person intentionally swears or issues a false affidavit, certificate, or other document regarding the registration of a birth or death or alters any such document.
- If a person knowingly submits or uses an affidavit, certificate, or other document that is forged or contains false information.
- If a person knowingly distributes forged or false certificates or documents that claim to be issued by the Registrar.
- If a person deliberately makes any false statement with the intent to have it entered into the official register.

The penalties for these offenses include, on summary conviction, a fine of up to $3,000 and/or up to 12 months in prison and on conviction on indictment, a fine of up to $5,000 and/or up to 5 years in prison.

The Civil Registry Act provides that individuals who make willful destruction of the forms of the Registry are liable on summary conviction to a fine of up to five thousand dollars or to imprisonment for a term not exceeding five years. Also, individuals who willfully provide false information or make false statements are liable on summary conviction to a fine not exceeding one thousand dollars or to imprisonment for a term not exceeding six months.

Conclusion

The legal framework governing civil registration requires the provision, recording and disclosure of certain personal data in connection with births, deaths and marriages that would be regarded as “processing” of personal data under a typical data protection law. The Civil Registration Act indirectly (albeit thinly) reflects a few key data protection principles in relation to such processing but omits important ones such as privacy of certain types of registers. The Civil Registry Act places officials who process personal data in the context of civil registration to the duty of confidentiality. The introduction of a generally applicable data protection law would raise the level of protection of personal data across the board in the civil registration process. Nothing in the Acts contradict or would be inconsistent with a general data protection law, and so no amendment would be required to the Acts and no special accommodation would be required in the new general data protection law.

4.B.11 Electronic communications

Introduction, scope of application and definition of key terms

Telecommunications in Antigua are governed by the Telecommunications Act Cap 423, which governs the licensing of telecommunications stations and apparatus, the responsibilities of licensed dealers, the confidentiality of communications, emergency control of telecommunications, and regulatory powers to enforce compliance. The Act does not define "personal data". However, certain processes described in the Act contain elements of personal data processing:

- Section 7 provides that licensed dealers must keep records of any activities of receiving and delivering telecommunication apparatus. These records contain personal information such as individual names, addresses and financial information, which all constitute personal data.
- Section 19 provides that telecommunication officers have the right to enter to inspect telecommunication stations in respect of which a license is issued. Similarly, this process is likely to contain access to or collection of personal data.
- Sections 4 and 5 requires that licences for telecommunication operations and dealerships require a specific license. Such license is likely to require collection and registration of individuals' personal data.

These activities of collection, maintaining, storing and sharing personal data constitute various forms of personal data processing.

Lawful basis for processing

Processing of personal data under Sections 4,5, 7, and 19 is performed under the lawful basis of compliance with the legal obligations deriving from this Act.

Obligations of the entities processing personal data

The Act does not impose obligations to entities processing personal data.

Data subject rights

The Act does not address the rights of the data subjects whose information is being processed. It lacks provisions for rights to access, correction, erasure or objections to data processing.

Cross border transfers of personal data

The Act does not address the cross-border transfer of personal data.

Institutions and penalties

Section 18 of the Act grants the Cabinet the authority to create rules regarding any matter related to telecommunications, with the aim of more effectively achieving the objectives of the Act. It also allows the Cabinet to impose penalties for breaches of these rules, with fines not exceeding five hundred dollars, recoverable through summary conviction. However, the Act does not explicitly impose penalties for violations related to personal data or privacy rights.

Conclusion

The Act sets out the framework for the operations and regulations of telecommunication services but does not contain any provisions related to protection of personal data, including obligations regarding personal data, lawful basis for processing, data subject rights and cross-border transfers. A generally applicable data protection framework would provide safeguards to personal data processing activities covered under the Act.

4.B.12 Electronic transactions

Introduction, scope of application and definition of key terms

The Electronic Transactions Act of 2013 establishes the legal framework for electronic transactions in Antigua and Barbuda, granting legal effect to electronic documents, records, signatures, and other related matters. This Act also addresses the processing of personal data within the context of electronic communications between two parties, referred to as "the originator" and "the addressee." As defined in Section 2:

> "originator, in relation to an electronic communication, means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but does not include a party acting as an intermediary with respect to that electronic communication"; and
>
> "addressee, in relation to an electronic communication, means a person who is intended by the originator to receive the electronic communication, but does not include a person acting as an intermediary with respect to that electronic communication".

Electronic communications between an originator and addressee will often include the following personal data: their names, email addresses, metadata such as the time and location of an email, identifiers included in a signature (phone numbers, physical addresses, and other contact details may be shared directly within the email content), along with any information revealed in the context of their communication.

The definition of "authentication data" encompasses a username, password, and license key, which are considered personal data processed within the context of electronic transactions, particularly in relation to electronic signatures.

According to the definition of "electronic communications", which cover information being "generated, communicated, processed, sent, received, recorded, stored, or displayed by electronic means", personal data undergo "processing" as they are transferred by the originator and subsequently received and stored by the addressee.

However, the Act does not impose any obligations on the originator, or the addressee of electronic communications regarding the protection, maintenance of integrity, or safety of personal data. Additionally, there are no provisions concerning data subject rights, cross-border data transfers, or relevant institutions authorized to oversee electronic communications. As a result, electronic transactions would benefit from a comprehensive data protection framework that imposes obligations, rights, and responsibilities regarding the processing of personal data.

Lawful basis for processing

Personal data involved in electronic transactions, as defined under the Act, are processed under several lawful bases:

- Under Sections 16-21, the processing of personal data involved in the formation and enforcement of an electronic contract is performed under the lawful basis of contractual necessity. In the context of automated contracts, personal data is required to fulfill the terms and obligations outlined in the contract, such as providing services, delivering goods, or managing transactions
- Under Section 6 the legal recognition of electronic communications, and Section 7 the legal recognition of electronic records. Providing personal data through electronic communications and in electronic records constitutes personal data processing based on contractual necessity and is legitimized through the lawful obligations under this Act.

Obligations of the entity processing personal data

- Section 26(2) provides that where a security procedure is applied by the parties involved in the formation of an electronic record, the appropriateness of that security procedure can be

determined by various factors, including the nature of the transaction, the level of technological modernity of the party and more. Given that electronic records are likely to contain personal data, this principle echoes the data protection principle of data security.

- Section 31 establishes the framework governing the use of electronic records and electronic signatures by the government and its agencies. It provides that when a public authority decides to perform any of the its key functions set out in subsection (1) of Section 31, by means of electronic records or in electronic form, the public authority may specify, among other factors "the control processes and procedures that may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; or (e) any other required attributes for electronic records or payments that are currently specified for corresponding paper." This requirement reflects the requirement of records to be processed with confidentiality, security and integrity.

Data subject rights

The Act does not address data subject rights.

Cross-border transfers of personal data

Section 25 the Act addresses cross-border recognition of electronic signatures and certificates. The Act allows parties to mutually agree on the use of a particular type of electronic signatures and certificates which are recognized as sufficient for the purpose of cross-border recognition.

Institutions and penalties

The Act does not establish institutions not it provides for penalties relevant to processing of personal data.

Conclusion

While the Act provides a framework for regulating electronic communications and ensuring the validity of electronic documents and signatures, it addresses inadequately the issue of protection of personal data. The Act would not conflict with a data protection framework aligned with international good practices. It would be supplemented by provisions on confidentiality, data security safeguards and cross-border data transfers. It would also ensure that both originators and addressees are held accountable for the responsible processing of personal data.

4.B.13 E-signatures

Introduction, scope of application and definition of key terms

Electronic signatures are addressed within the Electronic Transactions Act of 2013. Specifically, Sections 22-28 provide the legal framework for the recognition of electronic signatures in the context of electronic transactions. The Act defines the following key terms:

- Under Section 2 of the Act, a signature is defined as a method used to identify a person and to indicate the intention of that person in respect of the information contained in a record;
- Signature creation data is the unique data, including codes or private cryptographic keys or a unique configured physical device which is used by the signatory in creating an electronic signature;
- Secure electronic signature means an electronic signature that is treated as a secure electronic signature by virtue of section 28 or any other provision of this Act.

The use of electronic signatures would typically constitute processing of personal data under a data protection law.

Lawful basis for processing

Where an electronic signature is used to enter into or perform contractual obligations, the performance of the contract would constitute a lawful basis of processing the personal data embedded within these signatures (e.g., name, email address, unique identifiers). Under Section 22, where a signature is mandated by law, an electronic signature satisfies this requirement, provided it effectively identifies the individual and serves to demonstrate their intent regarding the creation of an electronic record. Consequently, the processing of personal data within the signature is justified on the lawful basis of compliance with the legal obligations outlined in this Act.

Under Section 23 of the Act, parties of the transaction may agree to the use of a particular method or form of electronic signature or security procedure.

Obligations of the entity processing personal data

- Section 22 provides that when the law requires a document or record to be signed, or imposes consequences for not having a signature, the requirement for a signature is satisfied for electronic records if two conditions are met: when it effectively identifies the individual and serves to demonstrate their intent regarding the creation of an electronic record. This provision echoes the data protection principle of "integrity", as the validity of an electronic signature is conditional upon the integrity, validity and accuracy of the information to which it relates being maintained.
- Similarly, Section 27 reflects the requirements for an electronic signature to be treated as a secure electronic signature in the context of an electronic transaction. For the signature to be considered secure, it needs to be unique to the person using it, capable of identifying the person who created it, created using a method or means that is under the sole control of the person using it, linked to the electronic record it relates to in such a way that any changes to the record would invalidate the signature. Through these criteria, an electronic signature is uniquely linked to the signer and tamper-proof, protecting the integrity of the associated record.
- Section 31 establishes the framework governing the use of electronic records and electronic signatures by the government and its agencies. It provides that when a public authority performs any of the its key functions (set out in subsection (1) of Section 31), by means of electronic records or in electronic form, the public authority may specify "the control processes and procedures that may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; or (e) any other required attributes for electronic records or payments that are currently specified for corresponding paper." These requirements reflect the requirement of records to be processed with confidentiality, security and integrity.

Data subject rights

The Act does not data subject rights in relation to the right to access, correct or erasure their personal data provided in the context of e-signatures.

Cross-border transfers of personal data

Section 25 addresses the cross-border recognition of electronic signatures as it pertains to the foreign certificates and signatures in relation to their legal effectiveness. Additionally, the Act allows parties to agree on the types of electronic signatures or certificates they prefer to utilize for their transactions.

Institutions and penalties

There Act does not establish any relevant institutions.

Section 38 penalizes the activity of intentionally submitting or sharing false or misleading information, whether in official filings or to individuals using electronic signatures. It provides that it is an offence when

a person "(a) files information required under this Act that contains false or misleading information; or (b) provides a consumer or a user of an electronic signature with false or misleading information."

Conclusion

While the Electronic Transactions Act provides a framework for regulating electronic signatures, electronic communications and ensuring the validity of electronic documents and signatures, it addresses inadequately most aspects pertaining to data protection. The Act would not conflict with a data protection framework aligned with international good practices. It would be supplemented from its provisions especially as it pertains to security safeguards and cross-border data transfers. It would also ensure that both originators and addressees are held accountable for the responsible processing of personal data.

4.C Dominica

4.C.1 Data protection

There is currently no legislation in this area.

4.C.2 Cybersecurity and cybercrimes

There is currently no legislation in this area.

4.C.3 Consumer protection

Introduction, scope of application and definition of key terms

While Dominica does not have a separate consumer protection law, Sections 37-38 of the Electronic Transactions Act of 2023 cover the consumer protection aspects related to electronic communications. See Section 4.C.12 below.

4.C.4 Freedom of information requests

There is currently no legislation in this area.

4.C.5 Health

Introduction, scope of application and definition of key terms

The health sector in Dominica is governed by three Acts: The Medical Act of 1991("Medical Act"), the Hospitals and Health Care facilities Act of 2002 ("Hospitals and Health Care Facilities Act"), and the Hospitals Authority Act of 2021 ("Hospital Authorities Act").

- The Medical Act provides the legal framework for the registration and practice of medical practitioners, dentists, opticians, and druggists in Dominica. Although the Act does not define "personal data" or "patient data," it covers the processing of personal information to the extent that is requires individuals applying for licensure in the aforementioned fields to submit applications containing significant personal data to the relevant medical boards. The boards review their applications and, if they fulfill the required criteria, they register them as licensed practitioners. The types of personal data required for each profession include individuals' names, addresses, and qualifications and are detailed in Schedules A-G of the Act.

  Additionally, Section 10 mandates that the registrar, appointed by the Minister, must maintain an official Medical Register of all qualified practitioners, including medical practitioners, dentists, opticians, and druggists. The Medical Register shall include the names and addresses, descriptions and dates of qualifications as well as the dates of registration for all persons qualified to practice.

The collection, evaluation, storage, and review of personal data included in the applications constitute the processing of personal data.

- The Hospitals and Health Care Facilities Act provides the legal framework governing the licensing of hospitals and healthcare facilities in Dominica. It covers the processing of personal data, insofar as it requires individuals or entities seeking to register a building as a hospital or healthcare facility to apply to the relevant Board. These applications require sharing of various types of information, including the name of the person responsible for the facility's operation and management ("Administrator"), and other types of personal data. Additionally, the Act requires the Board to "prepare and maintain a Register containing names, addresses and such other particulars as may be prescribed of all hospitals or health care facilities which are licensed under this Act".

  In addition, under Section 26, Administrators of hospitals or health facilities are required to collect and maintain patient's personal data including: "(a) the name, age, sex and usual place of abode of each patient, and the date of his admission, or attendance, as the case may be; (b) the diagnosis of each patient; (c) the name of the medical practitioner attending each patient; (d) the date on which each patient leaves the hospital or health care facility and, if transferred to another hospital or health care facility, the name of the other hospital or health care facility, in the event of the death of a patient in the hospital or health care facility, the date of his death; (e) births occurring at the health care facility; (f) communicable diseases requiring notification; (g) such other particulars as may be prescribed by Regulations."

  The collection, assessment, and maintenance of personal data for licensing hospitals and healthcare facilities, along with the management of patient information, constitute the processing of personal data.

- The Hospital Authority Act provides the legal framework providing for the establishment of Dominica's Hospitals Authority ("Authority"), the administration and management of hospitals and other matters related to health facilities. This Act covers the processing of personal data to the extent required to fulfil the function of the Board of the Authority, which is "to employ, discipline and terminate medical staff, officers and employees, subject to this Act" (Section 7(h)).

Lawful basis for processing

- Under the obligations required by the Medical Act, individuals who submit applications for their license as registered medical professionals must provide to the relevant Boards their personal data prescribed in Schedules A-G. The Boards evaluate the data to determine applicants' qualifications and issue certificates of competency. Additionally, appointed registrars are responsible for maintaining the personal data of qualified practitioners in the Medical Registers, as required by the Act.

- Under the Hospitals and Health Care Facilities Act, personal data provided to the Board through applications are processed for the purpose of determining whether buildings shall be registered as hospitals or healthcare facilities. Additionally, patients and practitioners working in hospitals and health facilities are required to submit personal data to the Administrator, as set out in Section 26. This information is then processed by the Administrator for the purpose of maintaining a registrar, under their obligations under this Act.

- Under the Hospital Authority Act, medical staff, officers and employees provide their personal data in compliance with the legal obligation under this Act, and in the context of their employment by the Board. The Board processes their personal data in accordance with the Act. Additionally, officers and members of the Authority are required to manage any personal data

that they receive in accordance with the Act, and under the duty of confidentiality established in Section 49.

Obligations of the entity processing personal data

While the Acts do not explicitly provide obligations for entities processing personal data, they contain certain provisions which reflect certain data protection principles:

- Sections 21 of the Medical Act makes it an offence to fraudulently register or attempt to register oneself as any kind of medical practitioner, or assist another in doing so, with a penalty of up to two years' imprisonment. Similarly, under Section 22, any registrar or individual who knowingly makes, causes, or permits a false or incorrect entry in the medical register (or any copy thereof) is also guilty of an offence, subject to the same two-year imprisonment penalty. These provisions reflect the intention to maintain accurate, and not misleading, and echo the personal data principles of data accuracy and data quality.
- Section 26 (2)-(5) of the Hospitals and Health Care Facilities Act, require that "any updates regarding register of patients must be recorded as soon as practicable", and that patients' deaths shall be communicated with the Chief Medical Officer within 48 hours. It also states that knowingly registering false entries in the register of patients constitutes an offence. The aforementioned provisions underscore the principles of data accuracy and data quality of personal information.

  Additionally, Section 27(4) provides that "no confidential case history notes" shall be open to routine hospital and health facilities inspections and evaluations. Section 32 also requires certain individuals, such as inspectors, their assistants, and Board members, to maintain "secrecy" regarding any matters they learn while performing their duties, unless disclosure is necessary for their role or legally required by a court or law. Breaches of this obligation for secrecy carry penalties, including fines and imprisonment. These provisions provide a direct obligation of secrecy and confidentiality over the processing of personal data.
- Section 49(1) of the Hospitals Authority Act imposes strict confidentiality obligations on members and officers of the Dominica Hospitals Authority, requiring them to maintain secrecy and ensure that patient information is disclosed only when necessary for legal or operational purposes. Section 49(2) further mandates that members and officers take an oath of secrecy and establishes penalties for any breaches. These provisions uphold the principles of confidential processing of personal data, as well as data accuracy and data quality.

Data subject rights

The Acts provide data subject rights, in the following narrow circumstances:

- Section 15 of the Medical Act authorizes the Registrar to correct errors in the medical register, allowing for the amendment of omissions or inaccuracies, including updates to a registered individual's name or address as new information becomes available. Additionally, Section 16 grants registered individuals the right to request the removal of their name from the medical register.
- The Hospital Authority Act, under Section 48, provides individuals with the right to access their health records subject to the payment of a prescribed fee.

Cross-border transfers of personal data

The Acts under assessment do not address cross-border transfers of personal data.

Institutions and penalties

- The Medical Act establishes the Medical Board, which oversees the registration of medical and related professions. The penalties for breaches related to the processing of personal data are outlined in Sections 21 and 22: Section 21 makes it an offence for anyone to fraudulently register or attempt to register themselves, or assist another in doing so, with a penalty of up to two years' imprisonment. Section 22 imposes penalties for fraudulent entries in the medical register, with offenders also facing up to two years' imprisonment.
- Section 4 of the Hospitals and Health Care Facilities Act establishes the Hospitals and Healthcare Facilities Licensing Board ("Board"), as the body responsible for ensuring compliance with the Act. Its powers and functions are set out under Section 5. Under Section 32 of this Act, it states that breaches of secrecy may result in a fine of $20,000 or imprisonment for up to 2 years.
- The Hospitals Authority Act establishes the Dominica Hospitals Authority, as responsible for the overall management and administration of such hospitals and other health facilities. It also provides for civil proceedings under specific circumstances, which include negligence or bad faith.

Conclusion

The aforementioned Acts include limited provisions on personal data protection and grant certain data subject rights. However, they lack essential safeguards, such as requirements for securing the personal data of registered practitioners, officers, and patients, mandated data retention periods, and the right to request data deletion. Notably, the Acts do not contain any provisions that would conflict with or hinder the implementation of a comprehensive data protection framework aligned with international best practices.

4.C.6 Education

Introduction, scope of application and key definitions

The Education Act of 1997 provides the legal framework governing the establishment, regulation, and management of educational institutions in Dominica, including provisions for compulsory education, curriculum standards, teacher qualification, and governance. While it does not contain definitions directly relevant to personal data processing, the Act covers the processing of students' personal data in several contexts:

- Section 22(1) provides that principals shall establish and maintain a record of each student enrolled in the school. The exact types of information included in the records are set out in Section 30 of the Act and include personal data.
- Section 22(4) sets out the persons who are entitled to examine, copy, or obtain a certified copy of student records.
- Section 40 provides the right to school attendance counsellors to "stop any child who appears to be of compulsory school age" and is not at school, concerning their age, name and address, school in which they are registered, reason for absence from school and any other related matter.
- Section 82(1) of the Act provides that students who wish to be considered for special education programs, shall be assessed by the Chief Education Officer. The determination of their eligibility to these programs requires the assessment of personal information which, under most data protection frameworks, are considered "sensitive" or "special" due to their intimate character.

The aforementioned activities constitute forms of personal data processing.

Lawful basis for processing

- Sections 22, 30, 40, 82: As noted in the previous section, personal data is provided by students and their parents as a requirement for their registration to school, and in fulfillment of their obligations under this Act, or as part of a contract between the student or parent and the school. This data is processed by principals, parents, school attendance officers, government officials and the Chief Education Officer for various purposes outlined in the Act. These include establishing and maintaining student records, performing official functions, accessing and obtaining copies of records, monitoring attendance, providing access to special educational services, and carrying out other administrative duties.
- Section 22(5): Parental or individual consent is required for the examination of student records, given that the record is not available "to any other person or institution without the written permission of the parent, or, where the student is eighteen years of age or older, the student." This provision ensures that personal data is accessed and reviewed only with explicit consent of either the parent or legal guardian or the student of legal age.

Obligations of the entity processing personal data

The Act places specific obligations on principals regarding the processing of students' personal data, in line with key data protection principles:

- Section 22(5) echoes the principle of confidentiality, providing that student records must be privileged and may only be accessed by school or departmental officials for official purposes.
- Section 22(7) provides that authorized individuals may request corrections to student records, if inaccuracies or incomplete information are identified, reflecting the principles of data accuracy and data quality.

However, the Act does not include provisions for maintaining the security of personal data or for the obligation of retaining student information and personal data only as long as necessary.

Data subject rights

The Act provides some rights over personal data of students, including:

- Right to access: Section 22(4) refers to access rights whereby parents and students of the age of 18 years or over may access copies of their records.
- Right to rectification of records: Section 22(7) allows parents or students over 18 years to request corrections over the data maintained by the school.

Cross-border transfers of personal data

The act does not address cross-border transfers of personal data.

Institutions and penalties

Section 7 of the Act states that the Chief Education Officer is responsible for the implementation of the obligations and rights of the Act. The Act does not include any fines or penalties associated with breaches of the aforementioned obligations regarding the processing of personal data.

Conclusion

The Act promotes confidential handling of student data and establishes basic data subject rights. However, it does not include provisions covering data retention periods, data security measures, or cross-border data transfers. A generally applicable data protection framework, aligned with international good practices, would supplement this Act's provisions.

4.C.7 Financial services (including digital financial services)

Introduction, and scope of application

Financial services in Dominica are governed by: The Banking Act of Dominica of 2015 ("Banking Act"), which regulates banking business and focuses on the operations of licensed financial institutions and the Offshore Banking Act of Dominica of 1996 ("Offshore Banking Act"), which governs the business of offshore banking.

The Offshore Banking Act covers the processing of personal data through the following provisions:

- Section 5(3) outlines the types of information which the Minister needs to evaluate before granting a license to an offshore bank. This evaluation requires performing a due diligence over all "directors, associates, and affiliates" of the entity. This information contains personal data, including individuals' financial net worth, details about their character and any "other requirements" that the Minister deems appropriate.
- Section 10 (1), (2) states that the Financial Secretary may assist the Minister in supervising financial institutions, which includes the Financial Secretary's right to access books, records, documents, cash and securities of licensees. Accessing such information is likely to involve collecting and assessing personal data.
- Section 12(1) provides that the Magistrate may authorize the Financial Secretary with a search warrant authorizing the Financial Secretary or their associate to enter a premises, vehicle, vessel or aircraft, to conduct searches therein. These searches may involve or reveal personal data of directors, associates, affiliates or other individuals.

The Banking Act covers the process of issuing licenses for various forms of financial institutions. This process involves the assessment of various forms of personal data, including information of their shareholders, directors and officers.

- Section 7(1) provides that entities submitting applications to obtain a license to operate as a financial institution are required to submit to the Central Bank various types of information, including personal data, including: "detailed information regarding the persons who will hold, or ultimately benefit from significant shareholdings, directly or indirectly, the respective values of the shares and the percentage of ownership" and "detailed information regarding the directors and officers, including their qualifications and experience, financial position, business interests and performance of the business concerns under their control or management."
- Similarly, Section 36(1) provides that that entities submitting applications to obtain a license to operate as a holding company are required to submit to the Central Bank various types of information, including personal data, such as" the names, addresses, occupations, business and professional history for the past ten years, certified financial positions, and corporate affiliations of persons who will hold or benefit from shareholdings, directly or indirectly, in the proposed financial holding company, and the respective values of the shares", " the particulars of the directors and officers of the proposed financial holding company, including their qualifications, experience, business and professional history for the past ten years, certified financial position, business interests and performance of the business concerns under their control or management."
- Section 61 grants external auditors the authority to access and review books, records, financial statements, and other sources specified in Section 61(2) to effectively perform their duties. These records are likely to include personal data.
- Section 97(1) focuses on corporate governance by outlining a set of criteria whose joined consideration determines whether individuals who are, or may become directors, significant

shareholders, or officers of a licensed financial institution or holding company are deemed "fit and proper" for this role. This assessment involves the evaluation of substantial amounts of personal data, including academic credentials, professional qualifications, and relevant experience.

- Section 103 provides the reasons for the removal of a director or officer from their position, which constitutes a decision that requires the assessment of personal information.

The activities of providing, evaluating and storing personal data of shareholders, directors and other officers, as described above, constitute forms of personal data processing.

Notably, the definition of the term "person" in the Act covers both natural and legal entities: "an individual, a public body, company, partnership, trust, association or body of persons whether corporate or unincorporated."

Lawful basis for processing

As reflected in the previous section, the Offshore Banking Act provides various lawful bases for the processing of personal data:

- Under Section 5(3), directors, associates, and affiliates share the information required by the Act to facilitate the due diligence required for the issuance of their license to carry offshore banking activities. The Minister then processes the information for the purpose of assessing the application and issuing a license.
- Under Section 10 (1), (2) the Financial Secretary may access books, records, documents, cash and securities of licenses in the context of their obligations under the Act to assist the Minister in carrying out their supervisory responsibilities.
- Under Section 12(1) the Financial Secretary is authorized by the Magistrate to conduct searches on the premises, vehicles, vessels or aircraft of licensees.

The Banking Act provides several bases for processing personal data:

- As outlined above, Sections 7(1), 36(1), and 61(1) require the processing of personal data of directors, shareholders, and officers for the assessment of their suitability for their position.
- Section 178 discusses the requirement for secrecy of information, and allows individuals associated with licensed financial institutions to disclose information of their customers only where a written authorization of the customer or their legal representative is given, when it is required by law or a court order, and where it is part of an intergovernmental agreement among participating governments.

Obligations of the entity processing personal data

The Offshore Banking Act includes certain obligations to which financial institutions and other personnel must adhere to when processing personal data, especially regarding the confidentiality of customer information.

- Under Section 26, the Offshore Banking Act, emphasizes the duty of "preservation of secrecy", prohibiting the Financial Secretary or any assistant or appointee from disclosing information relating to any application "by any person under the provision of this Act or to the affairs of a financial institution or any customer of a financial institution which he has acquired in the performance of his duties under this Act."
- Section 178 of the Banking Act provides the requirement for secrecy of information and prohibits individuals associated with licensed financial institutions from disclosing any information

regarding the identity, assets, liabilities or transactions of their customers, subject to limited exceptions.

Data subject rights

The Banking Act, under section 178(2), provides that individuals can request summaries of their credit ratings, which echoes the data subject right to access.

Cross-border transfers of personal data

The Banking Act, under Section 94 allows the Central Bank to enter into formal agreements or arrangements with foreign supervisory or resolution authorities, to facilitate coordination, cooperation, and the exchange of information between the Central Bank and the foreign authorities. The provision also emphasizes a key condition: the Central Bank can only share information if it is confident that the foreign authority has a legal obligation to protect the confidentiality of the shared information in accordance with applicable laws or regulations. The sharing of data is likely to include personal data, such as financial records, credit scores, names of customer data.

This provision reflects the principle of adequacy of protection, which is found in multiple data protection frameworks, and ensures that when personal data is transferred from one jurisdiction to another, the receiving jurisdiction must offer a level of protection that is as robust as what is available in the originating jurisdiction.

Additionally, Section 89 states that, in the interest of public policy, and upon request by the Central Bank, licensed institutions must share personal data with the Central Bank to ensure compliance with the Act. This information is likely to include personal data.

Institutions and penalties

While there is no specific institution established for the enforcement of data protection standards, the Central Bank generally oversees the data collection and processing to ensure compliance and risk management. The penalties for non-compliance or failure to submit the required information or provision of false data carries the penalty of $25,000 per Section 96.

The Offshore Banking Act under Section 26(1) states that breaches of confidentiality result in a fine of $10,000.00 or imprisonment of up to one year, upon summary conviction.

Conclusion

The Banking Act and the Offshore Banking Act focus on the requirement for confidential treatment of personal data processed by the Central Bank and financial institutions. However, both laws lack obligations on data security, data minimization, quality and transparency. However, these Acts would not contradict with a generally applicable data protection framework.

4.C.8 National identification (including digital and functional forms)

There is currently no legislation in this area.

4.C.9 Passports

The Immigration and Passport Act Cap. 18.01 is an act to impose restrictions on immigration and to govern the issue and production of passports. The Act does not deal with processing of personal data.

4.C.10 Civil registration

Introduction, scope of application and definition of key terms

The Registration of Births and Deaths Act Cap 35.30 governs the registration of births and deaths in Dominica. The process of registration covered by the Act is performed by the Registrar General, registrars,

and deputy registrars appointed by the Minister. It covers the processing of personal data in the following contexts:

- Section 16 requires that the registration of a child's birth, requires the parent or relative to provide substantive amounts of personal data, set out in Form 1 of the Act, that include date and place of birth, the child's name and sex, the name, surname, and address of the father, the mother's name and maiden name, the father's occupation or rank, the informant's signature, description, and residence, the date of registration, the registrar's signature, and any name added after registration.
- Section 27 provides that registering a person's death requires the submission of personal data detailed in Form 2: the date and place of death, the deceased's name, surname, sex, age, rank, profession or occupation, cause of death, as well as the informant's signature, description, and residence, the date of registration, and the registrar's signature.

The Act requires the sharing, recording, and disclosure of specific personal data related to births, deaths, and marriages, which is considered as "processing" under data protection laws.

Lawful basis for processing

Personal data provided by parents, relatives or occupiers of the house where the birth or death took place, are processed by the Registrars and other authorized officials to perform the administrative activity of registering life events such as births, and deaths, burials, required by the Act.

This legal requirement is evident in the Act's language, which mandates that "it shall be the duty" of the parties mentioned above to perform these registrations (Section 16 and 22). Subsequently, the Registrar General, registrars and deputy registrars process this personal data in accordance with the Act and subsequent regulations to maintain accurate and official records of civil status and provide certified copies.

Obligations of an entity to process personal data

The Act vaguely refers to the principle of personal data security in Section 43(3), where it requires that the registrar shall "safely keep each of the register books." Furthermore, the penalties for false statements outlined in Section 50 underscore the principles of data quality and data accuracy.

However, the Act does not impose additional obligations on entities regarding the processing of personal data, such as data minimization, data security protocols and data breach notification requirements.

Data subject rights

The Act grants data subjects with two rights with respect to their personal data:

- Right to access: Under Section 44 the public may search for the indices of certified copies of registers and obtain copies.
- Right to rectification: Under Section 23 parents, guardians or other responsible individuals may alter a child's name within 12 months of their birth registration.
- Also, under Section 38 clerical errors may be corrected by authorized persons, upon payment of a fee and submission of a statutory declaration and the original entry remains unaltered with the corrections being made in the margin.

Cross- border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

Section 50 of the Act states that providing false information regarding births or deaths, such as claiming a live-born child was stillborn or tampering with official records, constitutes an offence.

Section 50 also criminalizes the destruction or injury of birth and death registers. Offenders may face a fine of up to $500 for summary conviction or up to $5,000 and/or 12 months of imprisonment for more serious cases.

Conclusion

The Act establishes the framework for collections and maintenance of personal data in relation to births and deaths but lacks several international data protection standards which deal with confidentiality, data protection and security. By addressing these issues, it would enhance the Act's overall alignment with international good practices. Introducing a comprehensive data protection law that does not exclude the processing activities under this Act would enhance the overall protection of personal data within the civil registration process. Importantly, the Act does not contain provisions that would contradict or be inconsistent with a generally applicable data protection law.

4.C.11 Electronic communications

Introduction, scope of application and definition of key terms

The Telecommunications Act of 2000 governs the electronic communications in Dominica by establishing the National Telecommunications Regulatory Commission ("Commission") and regulating the licensing of telecommunication providers and other related matters. Dominica is a signatory to the Treaty establishing the Eastern Caribbean Telecommunications Authority ("ECTEL:), a regional agreement designed to foster competition in the telecommunications sector and harmonize policies across the region. Therefore, its national telecommunications law is aligned with ECTEL's legislative standards.

This Act addresses personal data processing to a limited extent, in the context of the following activities:

- The Minister, ECTEL, and the Commission collect, process, and store personal data when receiving and process applications for licenses, frequency authorizations, and any subsequent modifications or renewals of these licenses.
- Section 62: Telecommunication providers may hold subscriber personal information, which cannot be disclosed, unless a lawful basis exists.

The activities of disclosing, safeguarding, and maintaining personal data for the purpose of issuing licenses and for delivering telecommunication services constitute personal data processing.

Lawful basis for processing

The Act contains various lawful basis for processing personal data:

- Personal data collected as part of application process for licenses, frequency authorizations, and any subsequent modifications or renewals of these licenses. They are kept in records and on the basis of a legal obligation according to the Act.
- Additionally, under Section 62, personal data provided by subscribers to telecommunications providers for the purpose of receiving services—whether based on consent or contractual obligations—must be processed by the providers in accordance with the Act and their agreements with subscribers. Section 62 and 61 also states that subscriber personal data and messages may only be disclosed only under the subscriber's consent or in compliance with a court order.

Obligations of the entities processing personal data

The Act provides certain obligations to entities that process personal data, which reflect data protection principles.

- Section 14 provides that sharing of information that constitutes an "unjustified invasion of personal privacy" is protected from being disclosed in investigative records compiled for enforcement purposes, which reflects the intention to of safeguarding individual's privacy.

- Section 62 provides for the "secrecy of personal information," mandating that subscriber personal data must remain confidential and may only be disclosed when a lawful basis exists.
- Section 61 protects the confidentiality of the transmitted messages over telecommunications from disclosure, without consent or court order. These safeguards echo the principle of confidentiality of personal data.

Data subject rights

The Act does not address any provisions for data subject rights.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

Section 8 of the Act establishes the Commission and grants it the authority to carry out various functions, including advising the Minister on the development of national telecommunications policy, overseeing technical regulation, and setting technical standards for the telecommunications sector, as outlined in Section 12.

The Act provides penalties for violations related to personal data processing. Under Section 64, an individual who knowingly discloses personal information, in violation of their confidentiality obligations under Section 62, commits an offense and may face a fine of up to fifteen thousand dollars or imprisonment for up to one year.

Conclusion

The Act contains limited requirements for confidential processing of personal data and provides penalties for unlawful disclosures. However, it does not include any requirements for data security and minimization and secure cross border data transfers. The Act does not contain any provisions that would contradict or be inconsistent with a generally applicable data protection law.

4.C.12 Electronic transactions

Introduction, scope of application and definition of key terms

The Electronic Transactions Act of 2013 establishes the legal framework for electronic transactions in Dominica, granting legal effect to electronic documents, records, signatures, and other related matters. This Act also addresses the processing of personal data within the context of electronic communications between two parties, referred to as "the originator" and "the addressee." As defined in Section 2:

- "originator, in relation to an electronic communication, means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but does not include a party acting as an intermediary with respect to that electronic communication"; and
- "addressee, in relation to an electronic communication, means a person who is intended by the originator to receive the electronic communication, but does not include a person acting as an intermediary with respect to that electronic communication".

Electronic communications between an originator and addressee will often include the following personal data: their names, email addresses, metadata such as the time and location of an email, identifiers included in a signature (phone numbers, physical addresses, and other contact details may be shared directly within the email content), along with any information revealed in the context of their communication.

The definition of "authentication data" encompasses a username, password, and license key, which are considered personal data processed within the context of electronic transactions, particularly in relation to electronic signatures.

According to the definition of "electronic communications", personal data undergo "processing" as they are transferred by the originator and subsequently received and stored by the addressee.

However, the Act does not impose any obligations on the originator, or the addressee of electronic communications regarding the protection, maintenance of integrity, or safety of personal data. Additionally, there are no provisions concerning data subject rights, cross-border data transfers, or relevant institutions authorized to oversee electronic communications. As a result, electronic transactions would benefit from a comprehensive data protection framework that imposes obligations, rights, and responsibilities regarding the processing of personal data on both originators and addressees.

Lawful basis for processing

Personal data involved in electronic transactions are processed under several lawful bases:

- Processing personal data performed in the context of electronic transactions is performed in compliance with a legal obligation under an Act, or due to the necessity of performing a public task. Section 7 and 8 provide for the legal recognition of electronic transactions. Specifically, Section 8 allows information that is normally required by law to be given or recorded in writing (or in printed form) to be provided electronically, as long as two key conditions are met: the electronic version must be accessible to the intended recipient, and it must be capable of being retained so that it can be retrieved and used for future references. This rule applies even if the law explicitly requires written records or imposes penalties for failing to provide information in writing. As long as the electronic record can be accessed and stored properly, it can legally replace the traditional written or printed format.
- Under Sections 16-21, the processing of personal data involved in the formation and enforcement of electronic contracts is performed under the lawful basis of contractual necessity. In the context of automated contracts, personal data is required to fulfill the terms and obligations outlined in the contract, such as providing services, delivering goods, or managing transactions.

Obligations of the entity processing personal data

The Act provides minimal obligations to entities processing personal data:

- Under Section 25(2), parties have the flexibility to establish standards for information security by determining the use of specific security procedures. This grants them a degree of control over the security measures implemented. However, it also places the responsibility on the parties themselves to negotiate and agree upon appropriate safeguards.
- Additionally, under Section 24, where a signature creation data or authentication data may be used to create a signature or authenticate any electronic record that has legal effect, each signatory shall (a) exercise reasonable care to avoid unauthorized use of its signature creation data or authentication data, which reflects data integrity and accuracy.
- Section 31 establishes the framework governing the use of electronic records and electronic signatures by the government and its agencies. It provides that when a public authority decides to perform any of the its key functions set out in Section 31(1), by means of electronic records or in electronic form, the public authority may specify, among other factors "the control processes and procedures that may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; or (e) any other required attributes for electronic records or payments that are currently specified for corresponding paper." This requirement reflects the requirement of records to be processed with confidentiality, security and integrity.
- Section 37 mandates that anyone selling goods or services to consumers via electronic communication must provide clear, accurate, and accessible information, including their legal

name, principal geographic address, and an electronic means of contact or telephone number. This provision reflects the principles of data accuracy and data quality.

Data subject rights

Section 21 provides the data subject right of data rectification. It allows individuals to withdraw sections of electronic communications that contain errors, if certain conditions are met. It also requires senders to notify the recipient about the error and prevents them from deriving material benefit from erroneous communication.

Cross-border transfers of personal data

Under section 25(3) the Act addresses cross-border recognition of electronic signatures and certificates. The Act allows parties to mutually agree on the use of a particular type of electronic signatures and certificates which are recognized as sufficient for the purpose of cross-border recognition.

Institutions and penalties

The Act does not establish any institutions.

Section 39 penalizes the act of intentionally submitting or sharing false or misleading information, whether in official filings or to individuals using electronic signatures. It provides that it is an offence when a person "files information required under this Act that contains false or misleading information; or provides a consumer or a user of an electronic signature with false or misleading information."

Conclusion

While the Electronic Transactions Act provides a framework for regulating electronic communications and ensuring the validity of electronic documents and signatures, it addresses inadequately several aspects pertaining to data protection. The Act would not conflict with a data protection framework aligned with international good practices. It would be supplemented from its provisions especially as it pertains to security safeguards and cross-border data transfers. It would also ensure that both originators and addressees are held accountable for the responsible processing of personal data.

4.C.13 E-signatures

Introduction, scope of application and definition of key terms

Electronic signatures are addressed in Sections 22-28 of the Electronic Transactions Act of 2013, that provide the legal framework for the recognition of electronic signatures.

Under Section 2 of the Act, electronic signatures are defined as: "any electronic sound, symbol, process attached to or logically associated with an electronic record; and executed or adopted by a person with the intent to sign the electronic record; and a digital signature, a biometrical signature and any other signature based on an electronic process;"

The use of electronic signatures would typically constitute processing of personal data under a data protection law.

Lawful basis for processing

When electronic signatures are used to enter into or fulfill contractual obligations, the processing of any personal data embedded within them (such as name, email address, or unique identifiers) is performed on the basis of the fulfillment of that contractual obligation.

Obligations of the entity to process personal data

- Section 22 provides that when the law requires a document or record to be signed, or imposes consequences for not having a signature, the requirement for a signature is satisfied for electronic records if two conditions are met. First, the method used must identify the person and show their

intention regarding the information in the electronic record. Second, the method must either be reliable for the purpose of the transaction, considering the context and any relevant agreements, or be proven to fulfill the required functions of identification and intention, either by itself or with additional evidence. In essence, electronic records can fulfill signature requirements as long as the method used is dependable and demonstrates the signer's identity and intent. This provision echoes the data protection principle of integrity of personal data, inasmuch as the validity of an electronic signature is conditional upon the integrity, validity and accuracy of the information to which it relates being maintained.

- Similarly, Section 27 provides that for a signature to be considered secure, the signature needs to be unique to the person using it, capable of identifying the person who created it, created using a method or means that is under the sole control of the person using it, linked to the electronic record it relates to in such a way that any changes to the record would invalidate the signature. Through these criteria, an electronic signature is uniquely linked to the signer and tamper-proof, protecting the integrity of the associated record. This provision echoes the principle of data security and data integrity.
- Section 31 establishes the framework governing the use of electronic records and electronic signatures by the government and its agencies. It provides that when a public authority performs any of its key functions by means of electronic records or in electronic form, that public authority may specify "the control processes and procedures that may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; or any other required attributes for electronic records or payments that are currently specified for corresponding paper." This requirement reflects the requirement of records to be processed with confidentiality, security and integrity.

Data subject rights

The Act does not contain data subject rights related to electronic signatures.

Cross-border transfers of personal data

Section 25(3) addressed the cross-border recognition of electronic signatures, as it pertains to the foreign certificates and signatures in relation to their legal effectiveness. Additionally, the Act allows parties to agree on the types of electronic signatures or certificates they prefer to utilize for their transactions.

Institutions and penalties

There Act does not establish any relevant institutions.

Section 39 penalizes the act of intentionally submitting or sharing false or misleading information, whether in official filings or to individuals using electronic signatures. It provides that it is an offence when a person "files information required under this Act that contains false or misleading information; or provides a consumer or a user of an electronic signature with false or misleading information."

Conclusion

While the Electronic Transactions Act provides a framework for regulating electronic signatures, electronic communications and ensuring the validity of electronic documents and signatures, it addresses inadequately several aspects pertaining to data protection. The Act would not conflict with a data protection framework aligned with international good practices. It would be supplemented from its provisions especially as it pertains to security safeguards and cross-border data transfers. It would also ensure that both originators and addressees are held accountable for the responsible processing of personal data.

4.D Grenada

4.D.1 Data protection

Overview

Grenada's legal framework on protection of personal data is governed by the Data Protection Act of 2023 ("Act"). The purpose of the Act is to create a comprehensive data protection framework for Grenada. It also provides the establishment of a Commission as the body responsible for monitoring and enforcing compliance with the Act. As of now, it has not yet entered into effect. The Act largely mirrors the OECS Model Bill of 2016.

While the Act establishes certain key rights and obligations regarding protection and processing of personal data, it does not include some key elements from the international good practices outlined in Section 2 of this report.

Scope of applicability

The section below is generally consistent with international good practices, applying to both private and public entities. However, the Act's scope is overly restrictive, covering only a limited range of processing activities. To fully align with international good practices, the scope should be expanded.

Applicability limited to "commercial transactions"

Similar to the OECS Model Bill, this Act restricts the definition of personal data to information "related to commercial transactions." (See Section 3.A.1of this report.)

Broad exemption for processing by regulatory authorities

Similar to the OECS Model Bill, Section 22(2)(e) of the Act exempts from several of the data protection principles personal data that are processed for the purpose of discharging regulatory functions. (See Section 3.A.1of this report.)

General elements of data protection law

Some of the definitions contain contradictions, lack clarity, and would require revision to align with international good practices.

Definition of "personal data" is potentially limiting

As with the OECS Model Bill, the Act defines personal data in a manner that may limit the application of the Act. (See Section 3.A.1of this report.)

Definition of "sensitive personal data" excludes important attributes

As with the OECS Model Bill, the Act's definition of sensitive personal data that omits attributes that should be afforded additional safeguards when being processed. (See Section 3.A.1 of this report.)

Use of the terms "data users," "public bodies," "private bodies" and "persons"

As with the OECS Model Bill, the Act uses the terms "data users", "private bodies", "private bodies" and "persons" inconsistently. This drafting approach creates limitations, confusion and shall be revised. (See Section 3.A.1 of this report.)

No definition of "consent"

As with the OECS Model Bill, the Act does not define "consent". (See Section 3.A.1 of this report.)

Relation with other national legal instruments

As with the OECS Model Bill, Section 6 of this Act concerning its effect on other laws may confuse matters (See Section 3.A.1 of this report.)

Principles governing the processing of personal data

The Act reflects data protection principles in Sections 7-14, addressing lawful bases, security, purpose limitation, and data quality. However, the current formulation of these principles could be improved.

Principle of lawful, fair and transparent processing

As with the OECS Model Bill, the Act does not include a principle mandating that personal data be processed in a lawful, fair, and transparent manner, as is required by established international good practices. (See Section 3.A.1of this report.)

Principle of data minimization

As with the OECS Model Bill, the Act does not explicitly include a "minimum necessary" standard for processing of personal data. (See Section 3.A.1of this report.)

Lawful basis for public interest

As with the OECS Model Bill, the Act does not include a lawful basis on necessity for substantial public interest. (See Section 3.A.1of this report.)

Additional protection for processing personal data of children or persons with limited capacity to consent

As with the OECS Model Bill, the Act does not include additional protections for the processing of personal data for children and persons lacking the legal capacity to consent. (See Section 3.A.1of this report.)

Limitations on data retention do not have exceptions

As with the OECS Model Bill, Section 11 sets out the "*retention principle*" but limiting personal data retention by data users too tightly. (See Section 3.A.1of this report.)

Individual rights concerning personal data

Sections 15-19 of the Act provides some key data subject rights and sets out circumstances and timelines under which they can be exercised. While they are largely aligned with international good practices, the Act does not provide the rights of data subjects to withdraw consent, oppose the processing of their personal data with automated means, and delete their personal data. (See Section 3.A.1of this report.)

Data security

The Act has several significant omissions, notably the lack of requirements for data processors and data controllers to provide notifications in the event of a data breach.

Lack of specific data security requirements

Section 10 of the Act outlines the obligation of a data user to process personal data securely. As with the OECS Model Bill, the Act could provide greater specificity to support effective security frameworks for safeguarding personal data. (See Section 3.A.1of this report.)

No personal data breach notification obligations

As with the OECS Model Bill, the Act does not include any personal data breach obligations. Our analysis and recommended approach are provided in the context of the OECS model Bill, in Section 3.A.1of this report.

No requirements on data users when engaging data processors

Similar to the regional data protection framework, the Act does not require data users to take any measures to ensure that data processors can assist them in complying with the Act. Our recommended approach is provided in the context of the OECS model Bill, in Section 3.A.1 of this report.

No data processor liability for data security

Section 10(1) addresses data security requirements for data users. Section 10(2) addresses data security requirements for data processors, but, as with the OECS Model Bill, it does not make data processors directly liable for failure to adopt adequate data security measures. (See Section 3.A.1of this report.)

No requirement for Data Privacy Impact Assessments (DPIAs)

As with the OECS Model Bill, the Act does not mandate that data users conduct Data Protection Impact Assessments (DPIAs). (See Section 3.A.1of this report.)

Cross-border data transfers of personal data

As with the OECS Model Bill, the Act does not include provisions on cross-border data transfers. (See Section 3.A.1of this report.)

Institutions

Our internal research and contacts attempted by our local team members were not able to locate an online presence or physical establishment of the Commission.

Unclear and insufficient funding resources

The assertion that the Commission should receive funding by Parliamentary appropriations is helpful. It may be worth considering whether to permit the Commission to retain fines or receive grants, (e.g., from development agencies) and to act independently from political interference.

Enforcement

Disproportionate and unclear fines and penalties

Overall, the Act provides several mechanisms through which data subjects can file a complaint (Section 29-30) to initiate the Commission's investigation, and, in turn the Commission issue an enforcement notice when it has identified a violation of the Act (Section 34). In addition, the Act applies liability to senior leadership of legal entities, making them directly liable for offences. This is potentially somewhat harsh: it should suffice to address liability to the entity rather than its officers. We would also discourage the use of criminal offences for data protection violations. (See Section **Error! Reference source not found.** of this r eport.)

4.D.2 Cybersecurity and cybercrimes

Introduction, scope of application and definition of key terms

The Electronic Crimes Act No. 23 of 2013, amended by Act No. 10 of 2014, provides the legal framework governing the prevention and punishment of electronic crimes and related matters in Grenada. The Act's primary objectives include preventing unauthorized access, modification, and misuse of computer systems by establishing specific offences. Additionally, it facilitates the collection of electronic evidence crucial for criminal investigations. To achieve these goals, the Act establishes rules and protocols for data handling and processing. It also enforces strict criminal penalties for specified offenses to deter malicious activities and promote responsible use of computer technologies.

The Act defines data and access to in relation to electronic systems, however it does not specifically mention that data includes personal details. Section 2 of the Act defines the term "data" as –

representations of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including electronic program, text, images, sound, video and information within a database or electronic system.

This broad definition does not differentiate between personal and non-personal data and so the Act's prohibitions and obligations apply to what are commonly referred to in data protection laws as "personal data."

Also, despite not explicitly defining the term "processing", Section 2 references numerous activities performed on computer systems that deal with data, including: "transform", "scramble", "access, "damage", "tracking", "modify." These activities, to the extent that they cover personal data, constitute forms of personal data processing.

Lawful Basis for Processing

In the various offences established under Section 5- 18 that include unauthorized using, intercepting, modifying and accessing data and computing systems "without lawful excuse or justification", the requirement for authorization echoes the data protection principle of lawful processing.

Broadly, these provisions seek to ensure that processing is aligned with established legal requirements.

Obligations of the entity processing personal data

Although the Act does not provide affirmative general data processing obligations (only criminal prohibitions), it reflects some notions often included in data protection laws:

- Section 12 covers the protection of children's data by imposing increased fines for offenses involving data pertaining to children, reflecting the higher level of sensitivity often accorded to such data in data protection frameworks.
- Section 27 provides that a person who has obtained data under a lawful basis shall not use or disclose that data for any purpose other than the one for which it was originally collected, unless there is a lawful reason to do so. This provision reflects the data protection principle of purpose limitation of processing.

Data subject rights

The Act does not address data subject rights over their personal data.

Cross-border transfers of personal data

The Act does not include cross-border data transfers.

Institutions and penalties

The Act under Section 33 provides for the Minister to make regulations for the purpose of giving effect to the provisions of the Act and the enforcement is done by the police with investigative powers outlined in the sections of the Act. The penalties are listed as follows:

- Section 5(2): unauthorized access or data manipulation carries a fine of $200,000.00 or imprisonment of up to three years or both.
- Section 7: identity theft carries fines of up to $50,000.00 or imprisonment of up to three years or both.
- Section 8: electronic forgery penalties carry dines up to $100,000.00 or imprisonment up to three years or both.

Conclusion

The Electronic Crimes Act's broadly addresses two forms of processing that would relate to typical data protection law. The first is to prohibit certain forms of data processing, particularly those that were performed without lawful authority or having other criminal aspects. The second is to affirmatively require certain procedures (e.g., judicial order) for police and other authorized persons to obtain data (which would include personal data) in the context of investigations and prosecution. In doing so, the Act establishes a framework for combating cybercrimes and incorporates some minimal provisions that align with data protection principles. However, it does not include many typical data protection provisions, e.g., security

standards and institutional structures, which are essential for effectively safeguarding personal data involved in the prohibited or authorized processing activities.

A generally applicable data protection framework that aligns with international good practices would address these gaps in providing the necessary supplementary measures to ensure robust protection of personal data.

4.D.3 Consumer protection

Introduction, scope of application and definition of key terms

The Consumer Protection Act No. 2 of 2018 focuses on the promotion and protection of the interests of consumers in Grenada. It aims to ensure the protection of life, health and safety of consumers and establishes the Consumer Affairs Office and the Consumer Affairs Tribunal, as the institutions responsible for the implementation and enforcement of the rights and obligations established under the Act.

Although the Act does not define the terms "consumer data" or "consumer information," it includes several cases where personal data is being processed, including:

- Section 55 requires individuals or businesses to display their official name on certain business documents. For individuals, the name must match that on an official ID. Additionally, documents such as trade catalogs, sales records, and business letters must include the business's operating name, location, and, if applicable, the registered name used for business purposes. This information is likely to contain personal data.
- Section 56 requires that suppliers of goods shall include the "name of the procure or producers".
- Section 60(1) requires suppliers of goods or services to provide a record of transactions exceeding $10 for the consumer. The record must include key details including the supplier's name or registered business name, along with their VAT, registration number, and the address of the premises where the good or service was supplied. These records are likely to include personal data.
- Section 69(1) requires suppliers offering repair services to a consumer, to keep records stating the name, address and phone number of the consumer.
- The process for filling complaints with the Consumer Affairs Office (Sections 11-31) and hearings before the Consumer Affairs Tribunal (Sections 11-30) also involve processing of personal data of the parties, including basic identifiers such as name, contact details, and identification numbers, as well as demographic information and details about the complaint itself. During the hearing, additional data, such as witness information, legal representation details, and any relevant documents (e.g., evidence, medical records, or financial information) are also being processed.

The use of personal data in business transactions, including recordkeeping and disclosures, as well as for law enforcement purposes, involve various forms of personal data processing.

In addition, Sections 36-37 of the Electronic Transactions Act of 2023 covers certain consumer protection aspects related to electronic communications.

Lawful basis of processing

Under Sections 55, 56, 60, and 69 personal data disclosed and maintained in the context of business transactions are processed under the lawful basis of compliance with the obligations of the Act. Additionally, the personal data involved in the investigation and enforcement are processed for enforcement or investigative actions.

Obligations of entities processing personal data

The Act sets out limited obligations for entities processing personal data. The requirement for accurate representation of the products and services mentioned throughout the Act echoes the data protection principle of data accuracy. However, the Act does not include any other requirements regarding processing of personal data.

Section 36 of the Electronic Transactions Act requires persons using electronic communications to sell goods or services to provide "accurate, clear and accessible information about themselves", which aligns with the principles of personal data accuracy. The purpose of this requirement is that by having access to this information, consumers can easily identify and contact the seller, enhancing transparency and trust in electronic transactions.

Data subject rights

The Act does not address data subject rights related to consumer protection.

Cross-border transfer of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act establishes two institutions: the Consumer Affairs Office and the Consumer Affairs Tribunal, none of which govern the protection or security of personal data. The penalties and fines associated with non-compliance with the Act do not cover instances related to the handling of personal data.

Conclusion

The Act lacks most aspects of personal data protection. However, it would not contradict a generally applicable data protection law aligned with international good practices.

4.D.4 Freedom of information requests

There is currently no legislation in this area.

4.D.5 Health

Introduction and scope of application and definitions

The legal framework on health in Grenada is governed by two laws: The Grenada Health Practitioners Act Cap 132 A of 2010 ("Health Practitioners Act"), which provides for the registration and regulation of health practitioners, and the Grenada Hospitals Authority Act of 1998 ("Hospitals Authority Act"), which provides for the powers and duties of the Grenada Hospitals Authority.

The Health Practitioners Act covers the processing of personal data in several instances:

- Sections 38, 39, 40, and 89 require the Council to assess various types of information when processing individuals' applications to register as medical professionals, dentists, general practitioners, specialists, or interns. This information is likely to include personal data such as the individual's name, age, academic record, and professional credentials.
- Section 31 requires the Council to provide annual reports to the Minister and subsequently to Parliament. These reports are likely to include personal data.
- Section 43 states that individuals registered with the Council may receive a certificate, which includes personal data.

- Section 96 states that the Council shall maintain records for registered individuals, including people's names, personal and business addresses, and qualifications, all of which constitute personal data.
- Section 117 requires health practitioners to maintain records of their patients for a specific period of time.

Submitting personal information through applications, evaluating those applications, and maintaining related records and databases constitute forms of processing personal data.

The Hospitals Authority Act does not govern the processing of personal data.

Lawful basis of processing

As explained above, personal data are processed in the context of Sections 38, 39, 40, 89, 31, 43, 96 and under the lawful basis of compliance with legal obligations under the Health Practitioners Act.

Obligations of the entity processing personal data

The Health Practitioners Act also includes several obligations relating to personal data:

- Section 116 limits disclosure of information only to what is necessary for the fulfilment of the Council's or Committee's functions. This provision echoes the data protection principle of data minimization and purpose limitation.
- Sections 115 and 116 requires members of the Council to operate under the duty of confidentiality and take "the prescribed oath of secrecy". This provision reflects the intent to protect personal data and echoes the principle of confidentiality.
- Section 111 makes it an offence to make or produce false or misleading statements, which echoes the principle of data accuracy.

Data subject rights

The Health Practitioners Act does not mention specific provisions for data subject rights, other than the patients' right to obtain copies of their medical records and registered practitioners' certificates of registration, which reflect the data subject's right to access.

Cross-border transfers of personal data

The Act does not address cross-border transfers.

Institutions and penalties

The Act states that the Council and committees shall oversee the professional conduct and handling of patient's records. Under Section 111, making false statements, forgery or altering certificates or licenses carries the fine of $20,000.00 or imprisonment up to two years.

Conclusion

The Health Practitioners Act deals with the obligations for managing personal data (those of medical practitioners) in the health sector, focusing on record maintenance. It contains provisions that reflect certain aspects of data protection but lack several key elements. The Act does not contain any provisions that would conflict with or impose barriers in the implementation of a generally applicable data protection framework which would be aligned with the best international practices.

4.D.6 Education

Introduction, scope of application and key definitions

The Education Act Cap 86 of 2002 governs the delivery of education services in Grenada, by both the public and the private sectors. The Act contains provisions with regard to student personal information and records.

The Act refers to the processing of students' personal information in several contexts:

- Section 23(1) provides that principal "must establish and maintain for each student enrolled in the institution a student record". The exact types of information included in the records are set out in Section 31 of the Act and include personal data.
- Section 23(6) sets out the individuals who have the right to examine, copy, or obtain a certified copy of a student's records. Having access to personal data constitutes a form of processing.
- Section 45 provides the right to school attendance counsellors to "enter any premises" and "stop any child who appears to be of compulsory school age" and is not at school, concerning their age, name and address, school in which they are registered, reason for absence from school and any other related matter.
- Sections 47 and 65 require that school principals must submit student reports to the Chief Education Officer. As explained above, these reports include personal data such as student names, attendance records and academic performances.
- Section 115(1) of the Act provides that students who wish to be considered for special education programs shall be assessed by the Chief Education Officer. The determination of their eligibility to these programs requires the assessment of personal information which, under most data protection frameworks, are considered "sensitive" or "special" due to their intimate character.

The aforementioned activities constitute forms of processing personal data of students.

Lawful basis for processing

- Sections 23, 31, 45, 47, 67, 115: As stated in the previous section, personal data is provided by students and their parents in fulfillment of their obligations under this Act. It may also be provided in the context of a contract between the school and the parents or the student. This data is processed by principals, department officials, parents, school attendance officers, and the Chief Education Officer for various purposes outlined in the Act. These include establishing and maintaining records, performing official functions, accessing and obtaining copies of records, monitoring attendance, providing access to special educational services, and carrying out other administrative duties.
- Section 23(6): Parental or individual consent is required for the examination of student records, as records are not available "to any other person or institution without the written permission of the parent, or, where the student is eighteen years of age or older, the student." This provision ensures that personal data is accessed and reviewed only with explicit consent.

Obligations of the entity processing personal data

The Act provides certain obligations for entities processing personal data of students, which echo principles of data protection:

- Section 23(5) provides that student records shall be accessed by specific individuals under certain lawful bases and reflect the principle of confidentiality. Also, Section 23(7) states that the student data is "privileged information". These sections echo the data protection principle of

confidentiality. This principle is also reflected in Section 23(9), which states that disclosure of "student information from a student's record in contravention of subsection (7) commits an offence", with a penalty of one thousand dollars.

- Section 23(9) provides that specific individuals may request corrections to student records if inaccuracies or incomplete information are identified, reflecting the principles of data accuracy and quality.

However, the Act does not include provisions for maintaining the security of personal data or for retaining personal data only as long as necessary, including in student reports.

Data subject rights

- Section 23(6) reflects the data subject right to access, by providing "authorized persons" with the right to access and obtain copies of their records under Section 23(6).
- Sections 23(9-11) reflect the right to rectification, as it provides "authorized persons under section 23(6) with the right to correct inaccuracies in their records.

Cross-border transfers

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Ministry of Education handles appeals for unresolved disputes, and the Chief Education Officer, is responsible for the enforcement of compliance and resolution of disputes.

The penalty stipulated in the Act is for the disclosure of student records which carries a fine of up to $1,000.00.

Conclusion

The Education Act establishes a framework for the processing of student data including their personal information. It includes certain limited safeguards to personal data, including prohibition of unlawful disclosures and provides certain data subject rights. However, it does not include provisions covering data retention periods, data security measures, or cross-border data transfers, which are essential components for comprehensive data protection. A generally applicable data protection framework, aligned with international good practices, would supplement this Act's provisions.

4.D.7 Financial services (including digital financial services)

Introduction, and scope of application

The Banking Act of Grenada (2015) regulates banking operations, the establishment of a unified banking space, and the collection, processing, and disclosure of personal data by licensed financial institutions. Notably, the Act defines the term "person" broadly, encompassing both natural and legal entities, including individuals, public bodies, companies, partnerships, trusts, associations, and other organizations, whether incorporated or not. While it does not explicitly define "customer data" or "personal data," it governs the processing of customer information and imposes specific safeguards and reporting obligations. Additionally, the Act outlines the licensing and operational requirements for various financial institutions, within which personal data related to shareholders, directors, and officers is assessed.

- Section 7(1) provides that applications to obtain a license to operate as a financial institution requires submitting to the Central Bank various types of information, including " detailed information regarding the persons who will hold or ultimately benefit from significant shareholdings, directly or indirectly, the respective values of the shares and the percentage of ownership" and "detailed information regarding the directors and officers, including their

qualifications and experience, financial position, business interests and performance of the business concerns under their control or management."

- Similarly, 36(1) provides that applications to obtain a license to operate as a holding company requires submitting to the Central Bank various types of information, including " the names, addresses, occupations, business and professional history for the past ten years, certified financial positions, and corporate affiliations of persons who will hold or benefit from shareholdings, directly or indirectly, in the proposed financial holding company, and the respective values of the shares", and " the particulars of the directors and officers of the proposed financial holding company, including their qualifications, experience, business and professional history for the past ten years, certified financial position, business interests and performance of the business concerns under their control or management."
- Section 38 also provides that the Bank may grant such license if it is satisfied that the proposed officers and significant shareholders are "fit and proper" for the positions. This assessment includes the evaluation of a variety of criteria, including personal data of these individuals. The criteria of what constitutes the "fit and proper" standard are set out in Section 97(1).
- Section 61, which addresses auditing, grants external auditors the authority to access and review books, records, financial statements, and other sources specified in Section 61(2) to effectively perform their duties. These records are likely to include personal data. Section 74 provides that persons authorized to examine and investigate may have full access to the premises of the financial institution and may require directors, employees and officers to grant information. This process is likely to result in the collection of personal data.
- Section 97(1) emphasizes corporate governance by outlining a set of criteria to determine whether an individual who is, or may become, a director, significant shareholder, or officer of a licensed financial institution or holding company is deemed "fit and proper." This assessment involves the evaluation of substantial personal data, including academic credentials, professional qualifications, and relevant experience. Similarly, Section 98 contains criteria for determining whether a person is "fit and proper" to be a significant shareholder, which also include the processing of personal data.
- Section 103 provides the reasons for the removal of a director or officer from their position, which requires the assessment of various factors, including personal data.
- Section 94 allows the Central Bank to enter into agreements or arrangements with foreign supervisory or resolution authorities to facilitate coordination, cooperation, and the exchange of information. This exchange is likely to include personal data.

The activities of providing, evaluating and storing personal data of shareholders, directors and other officers, as described above, constitute forms of personal data processing.

The financial sector in Grenada is also governed by the Money Laundering Act of 1984, which does not cover the processing of personal data.

Lawful basis for processing

The Banking Act provides the following lawful bases for processing personal data:

- As outlined in the previous section, Sections 7(1), 36(1), and 61(1) of the Act mandate the processing of personal data belonging to directors, shareholders, and officers. This is done to meet the Act's requirements, including evaluating license applications and conducting audits.
- Section 178 discusses the requirement for secrecy of information, and allows individuals associated with licensed financial institutions to disclose information of their customers only

where a written authorization of the customer or their legal representative is given, when it is required by law or a court order, and where it is part of an intergovernmental agreement among participating governments. This section reflects the lawful basis of consent and processing of personal data under a court order.

Obligations of the entity processing personal data

The Banking Act provides certain obligations to financial institutions regarding processing of personal data:

- Section 178 provides the requirement for secrecy of information and prohibits individuals associated with licensed financial institutions from disclosing any information regarding the identity, assets, liabilities or transactions of their customers, subject to exceptions.

Data subject rights

Under section 178(2) individuals may request summaries of their credit ratings, which echoes the right to access.

Cross-border transfers of personal data

There are only two instances where the Act addresses broadly cross-border transfers.

Section 94 allows the Central Bank to enter into formal agreements or arrangements with foreign supervisory or resolution authorities, for the purpose of facilitating coordination, cooperation, and the exchange of information between the Central Bank and the foreign authorities. The provision also emphasizes a key condition: the Central Bank can only share information if it is confident that the foreign authority has a legal obligation to protect the confidentiality of the shared information in accordance with applicable laws or regulations. The sharing of data is likely to include personal data, such as financial records, credit scores, names of customer data.

This provision reflects the principle of adequacy of protection, which is found in multiple data protection frameworks, and ensures that when personal data is transferred from one jurisdiction to another, the receiving jurisdiction must offer a level of protection that is as robust as what is available in the originating jurisdiction.

Additionally, Section 89 states that, in the interest of public policy and upon request by the Central Bank, licensed institutions must share personal data with the Central Bank to ensure compliance with the Act. This activity involves data sharing of information that is likely to include personal data.

Institutions and penalties

While there is no specific institution established for the enforcement of data protection standards, the Central Bank generally oversees the data collection and processing to ensure compliance and risk management. The penalties for non-compliance or failure to submit the required information or provision of false data carries the penalty of $25,000 per Section 96.

Conclusion

The Banking Act focuses on the processing of personal data in the financial sector. While it addresses confidentiality and includes limited data subject rights, it lacks provisions on data security, data minimization, quality and transparency. By amending the Act to encompass these areas, they stand a better chance at complying with international data protection standards and avoiding potential risks for data subjects. However, these Acts would not contradict with a generally applicable data protection framework.

4.D.8 National identification (including digital and functional forms)

There is currently no legislation in this area.

4.D.9 Passports

Introduction, scope of application and definition of key terms

The Immigration Act Cap 145 of Grenada of 1980 (amended by No. 52 of 1991, Act No. 15 of 1993, Act No. 6 of 2001, Act No. 6 of 2011) governs the issuance and renewal of passports in Grenada. While the Act doesn't provide what types of data will be included in the passport, typically passport information contains individuals' names, dates of birth, signatures, unique numbers, photos and gender. The process of collecting, verifying and adding this information in passports constitutes the processing of personal data. The personal data required for the issuance and renewal of passports are handled by the Chief passport officer and the passport officers.

- Section 2 of the Passport Exemptions regulation provides that individuals entering Grenada from certain countries are exempted from the requirement to hold a valid passport. Assessment of individuals' passports constitutes processing of personal data.
- Personal data are also processed in the context of individuals' declarations, related to their immigration status and for the issuance of certificates. The personal data collected in each instance are included in the Immigration exemption regulation, under regulation 2, the International E/D Card Tarjeta Internacional E/D, under regulation 3 and the Certificates of Identity, under regulation 7.

Chapter 226 of the Passports Act also coves the issuance of passports in Grenada is which provides for the renewal and issuance of passports and other related matters. Sections 3, 4, and 5 of this Act authorizes the Minister or officers to process the required information in order to issue or renew passports.

Lawful basis for processing

The activity of providing personal data by submitting their passports for inspection and assessment or by completing immigration forms constitutes a form of personal data processing that is performed under the basis of compliance with the legal obligations of this Act.

The personal data included in their passports are then processed by officers in order to access an individual's application, declaration or request to enter the country, in accordance with the provisions of this Act. It could be also argued that since immigration control is closely linked with national security, the processing of personal data from passports and other relevant forms by officers is based on necessity for public interest.

Obligations of entities processing personal data

The Immigration Act does not require entities that process personal data to comply with any obligations or uphold any standards or requirements.

The Passport Act, while it does not explicitly outline specific requirements and obligations for entities processing personal data, it includes provisions in Section 10 that make it an offence to "alter or tamper with a passport" or to "engage in personation or false representation by holding oneself out as the holder or rightful possessor of a passport when one is not." These provisions underscore the principle of integrity and data quality.

Data subject rights

None of the Acts provide data subjects with any rights over their personal data.

Cross- border transfers of personal data

None of the Acts include any provisions regarding the transfer of personal data.

Institutions and penalties

The Immigration Act does not establish any penalties regarding processing of personal data under this Act, nor does it establish any institutions or authorities.

As mentioned above, the Passports Act, on Section 10 includes a provision making it an offence to "alter or tamper with a passport", to make a "personation or false representation holds himself or herself out as being the holder or the rightful possessor of a passport when he or she is not".

Conclusion

Both the Immigration Act and the Passports Act, which set out provisions related to passports in Grenada, do not include safeguards concerning the processing of personal data, and do not place obligations on entities handling personal information, such are requirements for confidential processing of personal information or practices on data security. As such, these Acts would not conflict with any broadly applicable data protection legislation.

4.D.10 Civil registration

Introduction and scope of application and definition of key terms

The Registration of Births and Deaths Act Cap 280 governs the registration of births and deaths in Grenada. The registration of these life events is performed by the Registrar General, registrars, and deputy registrars, as well as other authorized persons by the Minister. The Act covers the processing of personal data in several instances:

- Section 17 requires that registering a child's birth requires providing the information outlined in Form 1, including: the date and place of birth, the child's name and sex, the name, surname, and address of the father, the mother's name and maiden name, the father's occupation or rank, the informant's signature, description, and residence, the date of registration, the registrar's signature, and any name added after registration.
- Section 29 provides that, for the registration of a person's death, the following information, as detailed in Form 2, must be provided: the date and place of death, the deceased's name, surname, sex, age, rank, profession or occupation, cause of death, as well as the informant's signature, description, and residence, the date of registration, and the registrar's signature.

The Act requires the provision, recording, and disclosure of specific personal data related to births, deaths, and marriages, which qualify as "processing" under data protection laws.

Lawful basis for processing

Personal data provided by parents, relatives or occupiers of the house where the birth or death took place are processed by the Registrars and other authorized officials, in order to perform the administrative activity of registering life events, in compliance with the obligations prescribed in the Act.

This legal requirement is evident in the Act's language, which mandates that "it shall be the duty" of the parties mentioned above to perform these registrations (Section 17 and 29). Subsequently, the Registrar General, registrars and deputy registrars process this personal data in accordance with the statutory mandate of the Act and subsequent regulations to maintain accurate and official records of civil status and provide certified copies.

Obligations of the entity processing personal data

The Act echoes the principle of personal data security in Section 46(3), which requires that the registrar "safely keep each of the register books." Furthermore, the penalties imposed for false statements outlined in Section 53 underscore the principles of data quality and data accuracy.

However, the Act does not impose additional obligations on entities regarding the processing of personal data, such as a duty for confidentiality and integrity.

Data subject rights

The Act provides the following rights with respect to individuals' personal data:

- Right to access: Under Section 47(4) the public may search the register's copies and also obtain copies.
- Right to rectification: Under Section 25, parents, guardians or other responsible individuals may alter a child's name within 12 months of their birth registration. Also, under Section 40 clerical errors may be corrected by authorized persons, upon payment of a fee and submission of a statutory declaration and the original entry remains unaltered with the corrections being made in the margin.

Cross-border transfers of personal data

The Act does address cross-border transfers of personal data.

Institutions and penalties

Section 53 of the Act provides that intentionally providing false information to a registrar regarding births or deaths, such as claiming a live-born child was stillborn or tampering with official records constitutes an offence.

Conclusion

The Act establishes the framework for collections and maintenance of personal data in relation to births and deaths, but it lacks several international data protection standards which deal with confidentiality, data protection and security. By addressing these issues, it would enhance the Act's overall alignment with international good practices. Introducing a comprehensive data protection law that does not exclude the processing activities under this Act would enhance the overall protection of personal data within the civil registration process. Importantly, the Act does not contain any provisions that would contradict or be inconsistent with generally applicable data protection law.

4.D.11 Electronic communications

Introduction, scope of application and definition of key terms

In Grenada, electronic communications are regulated by Act No. 31 of 2000, which also establishes the National Telecommunications Authority. Grenada is a signatory to the Treaty establishing the Eastern Caribbean Telecommunications Authority ("ECTEL"), a regional agreement designed to foster competition in the telecommunications sector and harmonize policies across the region.

The processing and protection of personal data are addressed to a limited extent in the Act, specifically in the following instances:

- Personal data are being shared with the Minister, ECTEL, and the Commission and assessed as part of the application process for licenses, frequency authorizations, and any subsequent modifications or renewals of these licenses.
- Under Section 61, telecommunication providers may hold subscriber personal information, which cannot be disclosed, unless a lawful basis exists.

The activities of disclosing, safeguarding, and maintaining personal data for the purpose of issuing licenses and for delivering telecommunication services constitute personal data processing.

Lawful basis for processing

- Personal data collected and stored as part of application processes are processed pursuant to the lawful basis of a legal obligation under this Act.
- Under Section 61, personal data provided by subscribers to telecommunications providers for the purpose of receiving their services are be processed by the providers in accordance with the Act and their agreements with subscribers. Section 61 and 60 also state that subscriber personal data

and messages may be disclosed only under the subscriber's consent or in compliance with a court order.

Obligation of the entity processing personal data

- Section 14 provides that information which constitutes an "unjustified invasion of personal privacy" is protected from being disclosed in investigative records compiled for enforcement purposes, which reflects the intention to of safeguarding individual's privacy.
- Section 62 provides for the "secrecy of personal information," mandating that subscriber personal data must remain confidential and may only be disclosed when a lawful basis exists.
- Section 61 protects the confidentiality of the transmitted messages over telecommunications from disclosure, without consent or court order. These safeguards echo the principle of confidentiality of personal data.

Data subject rights

The Act does not address data subject rights.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

Section 7 of the Act establishes the Commission. Section 12 outlines the functions of the authority which include carrying out various functions, including advising the Minister on the development of national telecommunications policy, overseeing technical regulation, and setting technical standards for telecommunications.

The Act also provides penalties for violations related to personal data processing. Under Section 63, any individual who knowingly discloses personal information in violation of the obligation for confidentiality of personal information provided under Section 60, commits an offense and, upon conviction, may face a fine of up to fifteen thousand dollars or imprisonment for up to one year.

Conclusion

The Act contains limited requirements for confidential processing of personal data and provides penalties for unlawful disclosures. However, it does not include any requirements for data security and minimization and secure cross border data transfers. The Act does not contain any provisions that would contradict or be inconsistent with a generally applicable data protection law.

4.D.12 Electronic transactions

Introduction, scope of application and definition of key terms

The Electronic Transactions Act of 2013 establishes the legal framework for electronic transactions in Grenada, granting legal effect to electronic documents, records, signatures, and other related matters. This Act also addresses the processing of personal data within the context of electronic communications between two parties, referred to as "the originator" and "the addressee." As defined in Section 2:

- "originator, in relation to an electronic communication, means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but does not include a party acting as an intermediary with respect to that electronic communication"; and
- "addressee, in relation to an electronic communication, means a person who is intended by the originator to receive the electronic communication, but does not include a person acting as an intermediary with respect to that electronic communication".

Electronic communications between an originator and addressee will often include the following personal data: their names, email addresses, metadata such as the time and location of an email, identifiers included in a signature (phone numbers, physical addresses, and other contact details may be shared directly within the email content), along with any information revealed in the context of their communication.

The definition of "authentication data" includes usernames, passwords, and license keys, which are considered personal data processed within the context of electronic transactions, particularly in relation to electronic signatures.

According to the definition of "electronic communications", which cover information being "generated, communicated, processed, sent, received, recorded, stored, or displayed by electronic means", personal data undergo "processing" as they are transferred by the originator and subsequently received and stored by the addressee.

However, the Act does not impose any obligations on the originator, or the addressee of electronic communications regarding the protection, maintenance of integrity, or safety of personal data. Additionally, there are no provisions concerning data subject rights, cross-border data transfers, or relevant institutions authorized to oversee electronic communications. As a result, electronic transactions would benefit from a comprehensive data protection framework that imposes obligations, rights, and responsibilities regarding the processing of personal data.

Lawful basis for processing

Personal data involved in electronic transactions, as defined under the Act, are processed under several lawful bases:

- The personal data provided and received can be processed based on compliance with a legal obligation under an Act, or due to the necessity of performing a public task. Section 7 and 8 provide for the legal recognition of electronic transactions. Specifically, Section 8 allows information that is normally required by law to be given or recorded in writing (or in printed form) to be provided electronically, as long as the electronic version must is accessible to the intended recipient, and capable of being retained so that it can be retrieved and used for future references. This rule applies even if the law explicitly requires written records or imposes penalties for failing to provide information in writing.
- Under Sections 16-21, the processing of personal data involved in the formation and enforcement of an electronic contract is performed under the lawful basis of contractual necessity. In the context of automated contracts, personal data is required to fulfill the terms and obligations outlined in the contract, such as providing services, delivering goods, or managing transactions.

Obligations of the entity processing personal data

The Act imposes certain minimal obligations for entities processing personal data:

- Under section 25(2), parties involved in a transaction may set standards for information security procedures and measures. This practice highlights the importance of security measures, while placing the responsibility on the parties themselves to negotiate appropriate security measures.
- Additionally, under Section 24, where a signature creation data or authentication data may be used to create a signature or authenticate any electronic record that has legal effect, each signatory is required to exercise reasonable care to avoid unauthorized use of its signature creation data or authentication data, which reflects data integrity and accuracy.
- Section 31 establishes the framework governing the use of electronic records and electronic signatures by the government and its agencies. It provides that when a public authority decides to perform any of the its key functions set out in Section 31(1), by means of electronic records or in electronic form, the public authority may specify, among other factors "the control processes and

procedures that may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; or any other required attributes for electronic records or payments that are currently specified for corresponding paper." This requirement reflects the requirement of records to be processed with confidentiality, security and integrity.

- Section 36 mandates that anyone selling goods or services to consumers via electronic communication must provide clear, accurate, and accessible information, including their legal name, principal geographic address, and an electronic means of contact or telephone number. This provision reflects the principles of data accuracy and data quality.

Data subject rights

Section 21 provides the right to data rectification. It allows individuals to withdraw sections of electronic communications which contain errors if certain conditions are met. It also requires senders to notify the recipient of the error and prevents them from deriving material benefit from erroneous communication. The Act does not mention any further obligations in relation to confidentiality, data security or compliance with the same.

Cross-border transfers of personal data

Under section 25(3) the Act addresses cross-border recognition of electronic signatures and certificates. The Act allows parties to mutually agree on the use of a particular type of electronic signatures and certificates which are recognized as sufficient for the purpose of cross-border recognition.

Institutions and penalties

The Act does not establish any relevant authorities or institutions.

Section 38 penalizes the act of intentionally submitting or sharing false or misleading information, whether in official filings or to individuals using electronic signatures. It provides that it is an offence when a person "(a) files information required under this Act that contains false or misleading information; or (b) provides a consumer or a user of an electronic signature with false or misleading information."

Conclusion

While the Electronic Transactions Act provides a framework for regulating electronic communications and ensuring the validity of electronic documents and signatures, it addresses inadequately several aspects pertaining to data protection. The Act would not conflict with a data protection framework aligned with international good practices. It would be supplemented from its provisions especially as it pertains to security safeguards and cross-border data transfers. It would also ensure that both originators and addressees are held accountable for the responsible processing of personal data.

4.D.13 E-signatures

Introduction, scope of application and definition of key terms

Electronic signatures are addressed in Sections 22-28 of the Electronic Transactions Act of 2013. These Sections provide the legal framework for the recognition of electronic signatures in the context of electronic transactions.

Under Section 2 of the Act, electronic signatures are defined as: "a) any electronic sound, symbol, process attached to or logically associated with an electronic record; and executed or adopted by a person with the intent to sign the electronic record; and (b) a digital signature, a biometrical signature and any other signature based on an electronic process;"

The use of electronic signatures would typically constitute processing of personal data under a data protection law.

Lawful basis for processing

When electronic signatures are used to enter into or fulfill contractual obligations, the processing of any personal data embedded within them (such as name, email address, or unique identifiers) is performed on the basis of the fulfillment of that contractual obligation.

Obligations of the entity to process personal data

- Section 22 provides that when the law requires a document or record to be signed or imposes consequences for not having a signature. The requirement for a signature is satisfied for electronic records if the method used identifies the person and shows their intention regarding the information in the electronic record. This provision echoes the data protection principle of integrity of personal data inasmuch as the validity of an electronic signature is conditional upon the integrity, validity and accuracy of the information to which it relates being maintained.
- The same principle is also reflected in Section 27, which outlines the requirements for an electronic signature to be treated as a secure electronic signature in the context of an electronic transaction. For the signature to be considered secure, it needs to be unique to the person using it, capable of identifying the person who created it, created using a method or means that is under the sole control of the person using it, linked to the electronic record it relates to in such a way that any changes to the record would invalidate the signature. Through these criteria, an electronic signature is uniquely linked to the signer and tamper-proof, protecting the integrity of the associated record.
- As mentioned in the section above, Section 31 of the Act establishes the framework governing the use of electronic records and electronic signatures by the government and its agencies. It provides that when a public authority decides to perform any of the its key functions by means of electronic records or in electronic form, the public authority may specify, among other factors "the control processes and procedures that may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; or (e) any other required attributes for electronic records or payments that are currently specified for corresponding paper." This requirement reflects the requirement of records to be processed with confidentiality, security and integrity.

Data subject rights

The Act does address data subject's rights.

Cross-border transfers of personal data

Section 25(3) addressed the cross-border recognition of electronic signatures, as it pertains to the foreign certificates and signatures in relation to their legal effectiveness. Additionally, the Act allows parties to agree on the types of electronic signatures or certificates they prefer to utilize for their transactions.

Enforcement

Section 38 penalizes the act of intentionally submitting or sharing false or misleading information, whether in official filings or to individuals using electronic signatures. It provides that it is an offence when a person "files information required under this Act that contains false or misleading information; or provides a consumer or a user of an electronic signature with false or misleading information."

Conclusion

While the Electronic Transactions Act provides a framework for regulating electronic communications and ensuring the validity of electronic documents and signatures, it addresses inadequately several aspects pertaining to data protection. The Act would not conflict with a data protection framework aligned with

international good practices. It would be supplemented from its provisions especially as it pertains to security safeguards and cross-border data transfers. It would also ensure that both originators and addresses are held accountable for the responsible processing of personal data.

4.E Montserrat

4.E.1 Data protection

Montserrat does not have a framework governing the protection of personal data.

4.E.2 Cybersecurity and cybercrimes

Introduction, scope of application and definition of key terms

Montserrat does not have a general framework governing cybersecurity or cybercrimes. However, the Penal Code (Amendment) Act 2022 introduces several cybercrime provisions, such as unauthorized access, computer-related forgery and computer-related fraud. The same Act also defines critical infrastructure and sets out offences related thereto.

The Act defines "data" and provides guidance on the interpretation of "access" in relation to electronic systems; however, it does not specifically address personal data. Section 289A of the Act defines "data" on the basis of what data includes, which encompasses –

> *(a) material in whatever form stored electronically;*
>
> *(b) the whole or part of a computer program; or*
>
> *(c) any representation of information or of concepts in a form suitable for use in a computer, including a program suitable to cause a computer to perform a function.*

This broad definition does not differentiate between personal and non-personal data. Therefore, the Act's prohibitions and obligations apply to what are commonly referred to in data protection laws as "personal data."

Also, despite not explicitly defining the term "processing", the Act references numerous activities performed on computer systems that deal with data, including accessing, modifying, transmitting, storing, and removing data.

Lawful basis for processing personal data

The offences of "unauthorized access to computer system, program or data" and "unauthorized acts with intent to impair operation of computer, etc." (Sections 289C and 289D) highlight the requirement for authorization to access or otherwise process data. This reflects the data protection principle of lawful processing, aiming to ensure that data handling activities are lawful.

Broadly, these provisions seek to ensure that processing is aligned with established legal requirements.

Obligations of the entity processing the personal data

Although the Act does not provide affirmative general data processing obligations (only criminal prohibitions), it reflects some notions often included in data protection laws:

- Section 289N establishes the principle that services providers do not have an obligation to monitor content, unless their actions are based on a court order or other legal requirements.
- Section 289K recognizes the legal capacity of corporate bodies to commit offences under the Act. Accordingly, responsibility for such offences extends to the directors and officers if the corporate entity is involved in any of the offences established by the Act.
- Section 211D(6) excludes certain materials from the scope of the search and seizure for the offence of stalking, which includes "human tissue or tissue fluid", which may constitute

biometric data under most data protection frameworks. Exclusion of biometric data from search and seizure adds additional protection to certain types of data, which is a common principle in many data protection frameworks.

Data subject rights

The Act does not address data subject rights over personal data.

Cross-border transfers of personal data

The Act does not include cross-border processing of any data.

Institutions and penalties

The Act does not establish or designate any regulatory authority or institution responsible for overseeing compliance other than typical investigation and enforcement by police subject to judicial oversight. For example, Section 211D requires that a police officer apply for a warrant issued by the Magistrate to enter and search the premises when investigating the offence of stalking.

The penalties stipulated in the Act include the following:

- Section 289C: Unauthorized access to computer system, program or data carries a fine of up to $500,000.00 or imprisonment of up to seven years or both.
- Section 289D: Unauthorized acts with intent to impair operation of computer, etc. carry a fine of up to $500,000.00 or imprisonment of up to seven years or both.
- Section 289E: Offences affecting critical infrastructure, which are the same offences as set out in sections 289C and 289D with an impact on critical infrastructure, carry a fine of up to $1,000,000.00 or imprisonment of up to fifteen years or both.

Conclusion

The Act does not directly address personal data but establishes offences that criminalize certain behaviors in relation to data, which could include personal data. It broadly addresses two forms of processing that would typically fall under data protection laws. The first is to prohibit certain forms of data processing, particularly those that are performed without lawful authority or having other criminal aspects. The second is to affirmatively require certain procedures (e.g., a warrant) for police and other authorized persons to obtain data (which would include personal data) in the context of investigations and prosecution. In doing so, the Act establishes a framework for combating cybercrimes and incorporates some minimal provisions that align with data protection principles. However, it does not include many typical data protection provisions, e.g., security standards and institutional structures, which are essential for effectively safeguarding personal data involved in the prohibited or authorized processing activities.

A generally applicable data protection framework that aligns with international good practices would address these gaps in providing the necessary supplementary measures to ensure robust protection of personal data.

4.E.3 Consumer protection

There is currently no consumer protection legislation in Montserrat.

4.E.4 Freedom of information requests

There is currently no freedom of information request framework in Montserrat.

4.E.5 Health

Introduction, scope of application and definition of key terms

The legal framework on health in Montserrat is governed by two laws: the Public Health Act Cap 14.01 ("Public Health Act"), which provides for the promotion and preservation of the health of the inhabitants of Montserrat, and the Medical Act Cap 14.02 ("Medical Act"), which regulates the registration and practice of medical practitioners in Montserrat.

The Public Health Act does not govern the processing of personal data

The Medical Act covers the processing of personal data in several instances:

- Sections 4 through 13 govern various types of processing of data in relation to the Medical Register, which includes the names, last names, and addresses of medical practitioners, dentists, opticians, chemists and druggists. These sections require the Registrar to update the Medical Register by adding, correcting, or removing the personal data of medical professionals.
- Section 14 requires the Registrar to publish a copy of the Medical Register in the Gazette annually, which includes personal data of medical professionals.

Lawful basis of processing

The Medical Act provides a lawful basis for processing inasmuch as it obligates and/or authorizes (a) medical professionals to furnish personal data (along with other necessary information) to register with the Medical Register and (b) the Registrar register them and process their personal data according to this Act.

The processing of personal data by the Registrar during the act of medical professionals' registration is carried out largely based on the lawful basis of fulfillment of legal obligations. Subsequent processing activities carried out by the Registrar are performed largely as part of their official duties under the Act.

Obligations of the entity processing personal data

The obligations imposed by the Medical Act on the Registrar and practitioners in the processing of records embody the principle of data accuracy, which is reflected in several provisions throughout the Act:

- Section 8 authorizes the Registrar to correct any errors or omissions in the Medical Register, which echoes the principle of data accuracy.
- Section 15 establishes the offence of registration by false representation, while Section 16 imposes a penalty on the Registrar for making a false entry, which both echo the principle of data accuracy.

Data subject rights

The Medical Act does not explicitly provide for data subjects' rights to access, rectify, or erase their personal data.

Cross-border transfers of personal data

The Medical Act does not address cross-border transfers of personal data.

Institutions and penalties

The Registrar is responsible for handling the personal data of medical practitioners, dentists, opticians, chemists and druggists, who are registered in the Medical Register.

The relevant penalties in the Medical Act are listed as follows:

- Section 15 provides that obtaining registration in the Medical Register by false representations is subject to a penalty of two years' imprisonment.

- Section 16 provides that the Registrar or any other person who fraudulently makes, causes or permits to be made any incorrect entry in the Medical Register shall be subject to a penalty of two years' imprisonment.

Conclusion

The Medical Act deals with the obligations for managing personal data (those of medical practitioners) in the health sector, focusing on record maintenance. It has provisions that support some aspects of data protection, but various gaps. The Medical Act does not contain any provisions that would conflict with or impose barriers in the implementation of a generally applicable data protection framework, which would be aligned with the best international practices.

4.E.6 Education

Introduction, scope of application and definition of key terms

The Education Act Cap 16.01 governs the administration of educational institutions. It dictates the roles and responsibilities of students, parents, teachers and principals. Additionally, it highlights the personal information required to be admitted into an educational institution and guarantees the right to education.

The Act regulates the management and handling of students' as well as parents' personal information, including:

- Section 21 requires every principal to establish and maintain a student record for each student enrolled in a school, which includes personal data of the student and the student's parents. Additionally, the principal must maintain accurate student records and provide reports to parents or guardians periodically.
- Section 30 sets out the content of the Student's Register, which includes the name, address, telephone number and date of birth of each student, as well as the name and residence of the student's parents.

Lawful basis for processing personal information

The Act establishes several lawful bases for the processing of personal data:

- Performing Administrative Functions (Sections 21 and 30): As described in the previous section, the Act provides for processing of personal data about students and their parents by principals for managing student records, monitoring attendance, and performing other administrative functions.
- Consent for Examination of Records (Section 21(6)): Parental or individual consent is required for the examination of student records. This provision ensures that personal data is accessed and reviewed only with explicit approval.

Obligations of the entity processing personal data

The Act imposes obligations on schools and principals concerning the processing of personal data, reflecting key principles of data protection:

- Accurate Data Maintenance (Sections 21 and 30): Principals are responsible for maintaining accurate student records and registers under sections 21 and 30, which echoes the principle of data accuracy. Additionally, the Director of Education must review any rectification requests on student records and provide directions on disputes related to any inaccuracies.
- Privileged Use and Limited Third-Party Access (Section 21(4)): Student records cannot be disclosed to any other person without the written consent of the parents or the student, if the student is 18 years or older. The Act imposes limitations on third-party access without consent, which promotes confidentiality and integrity of personal data.

- Data Minimization (Section 21(6)): Records may only be used by the relevant school and departmental officials as necessary for performing their duties, which echoes the principle of data minimization.

The Act does not contain a requirement for maintaining security of personal data in the student records.

Data subjects rights

The Act provides several rights to the students as well as the parents regarding their personal data such as:

- Access to records: Section 21(4) provides for the data subject right to access, which establishes that the parents of a student or the student who is 18 years or older may access that student's record and obtain copies thereof. This provision promotes transparency and allows individuals to stay informed about the information held about them.
- Rectification of records: Section 21(8) sets out a right to rectification, as it provides authorized persons under the Act to request the correction of inaccuracies in the records. If a request for rectification is denied or results in an unfavorable outcome, the Act provides an appeals process, allowing for further review mechanism.

Cross- border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Ministry of Education is the primary institution that enforces the Act. The Act imposes penalties for the unauthorized disclosure of student records. Under Section 21(11), such offenses attract a fine of up to $1,000, which may not be high enough to deter non-compliance.

Conclusion

The Act promotes transparency in the management of students' personal data by establishing rights for students and clearly defining institutional responsibilities related to data processing. However, it does not include provisions covering data retention periods, data security measures, or cross-border data transfers, which are essential components of a comprehensive data protection framework. A generally applicable data protection framework, aligned with international good practices, would supplement this Act's provisions.

4.E.7 Financial services (including digital financial services)

The Financial Services Commission Act Cap 11.02 governs the responsibilities of the Financial Servies Commission with regard to financial records and statements. It also establishes the Commission's authority to request information and require the production of documents from financial institutions or individuals classified as financial institutions. However, the Act does not explicitly clarify whether the requested information includes personal data.

Certain requested documents may contain personal data, such as the names and addresses of individuals classified as financial institutions. Nevertheless, the Act does not specifically regulate the collection and processing of personal data.

Sections 47 and 48 outline rules on confidentiality and disclosure of information obtained under the Act. To the extent that such information includes personal data, these provisions align with international best practices on data confidentiality.

A comprehensive data protection framework, aligned with global standards, would not contradict the Act's provisions. On the contrary, it would complement and support any personal data processing that may occur under the Act.

4.E.8 National identification (including digital and functional forms)

There is no formal legislation that has been enacted in this area in Montserrat.

4.E.9 Passports

There is no formal legislation that specifically addresses passports in Montserrat.

4.E.10 Civil registration

Introduction, scope of application and definition of key terms

The Registration of Births and Deaths Act Cap 6.13 governs the process for registration of births and deaths in Montserrat. It outlines the duties of the Registrar and other authorities for recording and maintaining information and the penalties for non-compliance or provision of false information.

The Act provides the framework for recording, maintaining and managing civil status records in Montserrat. These records are formal and legally recognized documents. The process of registration and rectification of civil status records covered by the Act is performed by the Registrars and includes the processing of personal data.

For instance, Schedule A includes a template for the register book of births, which illustrates that the personal data are recorded for the registration of a child's birth includes the child's name, sex, place and date of birth, the parents' names, the father's name, rank or occupation and domicile, signature of the person completing the registration (father, mother or other informant).

The Act requires the provision, recording, and disclosure of specific personal data related to births and deaths, which qualifies as "processing" under typical data protection laws.

Lawful basis for processing personal information

Personal data provided by individuals or their parents are processed by the Registrars under the authority of the Act in order to register life events such as births and deaths. This legal requirement is evident in the Act's language, which mandates that the Registrar shall "*inform himself carefully of every birth […] and register particulars relating to such birth*" (Section 7) and shall "*inform himself as carefully as possible of every death […] and register particulars relating to such death*" (Section 18). Subsequently, the Registrar and relevant officials process this personal data in accordance with the statutory mandate of the Act and subsequent regulations to maintain accurate and official records of births and deaths.

Obligations of the entity processing the personal data

The Act does not establish clear obligations for confidentiality, integrity, secrecy, or security. Additionally, it lacks procedures for notification and response in the event of data breaches.

Data subject rights

The Act provides the right to access and the right to rectification. Individuals may request certified copies of entries upon payment of a fee (Section 26) and request correction of errors in the register (Section 21).

Cross- border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and Penalties

The Act designates the Registrar and the General Registry Office as the primary institutions responsible for implementing its provisions. The penalties include failure to provide information, which is subject to fines of up to $400, false statement or documentation subject to fines of up to $100 or imprisonment for up to six months on summary conviction, and imprisonment up to five years on indictment. Additionally, tampering with registers is subject to imprisonment for up to two years.

Conclusion

The Act provides several provisions governing the collection, administration, and management of records of births and deaths, and contains processes that promote their accuracy. However, it offers limited safeguards and protections for personal data. The absence of data subject rights, obligations for data security and safeguards against breaches poses significant risks to individuals' personal information. Addressing these gaps by implementing additional clauses would ensure the Act's compliance with international data protection standards.

Introducing a comprehensive data protection law that does not exclude the processing activities under this Act would enhance the overall protection of personal data within the civil registration process. Importantly, the Act does not contain any provisions that would contradict or be inconsistent with generally applicable data protection law.

4.E.11 Electronic communications

Introduction, scope of application and definition of key terms

The Telecommunications Act Cap 18.07 governs the regulation of telecommunication services within Montserrat, with subsidiary legislation outlining the administrative, technical, and procedural rules for its operation.

The Act addresses the processing of personal data by authorizing the relevant authority, the telecommunications officer or any other person appointed by the Governor to grant licenses, to collect and process personal information, such as names, business addresses, email addresses, and phone numbers, primarily in relation to the licensing process for telecommunications network and service operators. Additionally, the Act states that operators themselves receive and process subscriber personal information as part of their service delivery.

Lawful basis of processing

The telecommunications officer or any other person appointed by the Governor to grant licenses is required to keep a register, recording the particulars of every license issued. These records may include personal data relating to the representatives of the applicants.

Additionally, applicants provide their representatives' personal information as part of the application process to obtain, modify, or renew the various types of licenses listed in the Act. Subsequently, the telecommunications officer or any other person appointed by the Governor to grant licenses would process the personal information pursuant to the provisions of this Act.

Operators also process subscribers' personal data as part of their contractual obligations to deliver telecommunications services.

Obligations of the entity processing personal data

The Act does not impose any affirmative obligations on entities processing personal data. It does not outline responsibilities for data protection during processing, nor does it address data security measures, data minimization, or the confidentiality of communications.

Data subject rights

The Act does not provide data subject rights over their personal data.

Cross- border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act establishes penalties for non-compliance with various provisions of the Act:

- Section 4 prohibits any person from establishing a telecommunication station or operating telecommunication apparatus without a license.
- Section 7 mandates penalties for failure to keep records, which is subject to a penalty not exceeding $48.
- Section 12 prohibits intercepting and disclosing the contents of communications.
- Section 20 is a catch all provision which states that where no penalties are expressly provided, the guilty person shall be liable on summary conviction to a penalty not exceeding $250 or to imprisonment for a term not exceeding 6 months or both.

Conclusion

The Act primarily provides the framework for telecommunication infrastructure and services, but it does not address the collection, processing or protection of personal data. It does not provide adequate measures to ensure its security and protection. To address these shortcomings, the Act would benefit from the implementation of additional safeguarding and security protocols. Furthermore, it should be complemented by a comprehensive data protection framework to enhance the security and integrity of the personal data involved.

4.E.12 Electronic transactions

Introduction, scope of application and definition of key terms

The Electronic Transactions Act Cap 11.32 governs electronic transactions, communication of electronic records, electronic signatures, documents and other transactions which involve the processing of personal data. Its goal is to ensure that electronic transactions carry the same legal standing as traditional paper transactions. In this Act, the term "transaction" is not used in its literal, commercial sense. Rather, it is defined broadly as *"a transaction whether or not for consideration and whether or not of a commercial nature.*"

This Act regulates personal data in the context of exchange of "electronic records" between two persons, designated as "the originator" and "the addressee".

As defined in Section 2:

> *"electronic record," means a record processed and maintained by electronic means;*
>
> *"originator," in relation to an electronic record, means a person who –*
>
> *(a) sends an electronic record;*
>
> *(b) instructs another to send an electronic record on his behalf; or*
>
> *(c) has an electronic record sent by his electronic agent, but does not include –*
>
> > *(i) a person who sends an electronic record on the instructions of another; or*
> >
> > *(ii) a person acting as an intermediary with respect to that electronic record; and*
>
> *"addressee," in relation to an electronic record, means a person who is intended by the originator to receive the electronic record, but does not include a person acting as an intermediary with respect to that electronic record.*

Exchange of electronic records between an originator and addressee may include the following personal data: their names, email addresses, metadata such as the time and location of an email, identifiers included in a signature (phone numbers, physical addresses, and other contact details may be shared directly within the email content), along with any information revealed in the context of their communication.

According to the definition of "electronic records", which cover information "*processed and maintained by electronic means*", personal data undergo "*processing*" as they are transferred by the originator and subsequently received and stored by the addressee.

The Act authorizes the Governor, acting on the advice of the Cabinet, to make regulations prescribing standards for the processing of personal data. However, the Act does not directly impose obligations on the originator, addressee or intermediaries regarding the protection, maintenance of integrity, or safety of personal data. Although not provided as an obligation, Section 33 allows information security service providers to include a pseudonym in the relevant certificate instead of the signature device holder's name, at the request of the signature device holder, which may provide an added layer of data security for personal data.

Additionally, there are no provisions concerning data subject rights, cross-border data transfers, or relevant institutions authorized to oversee the exchange of electronic records. As a result, electronic transactions would benefit from a comprehensive data protection framework that imposes obligations, rights, and responsibilities regarding the processing of personal data on both originators and addressees.

Lawful basis for processing personal information

The Act does not explicitly mention any lawful bases for processing personal data, but Section 32 provides for the Governor to issue regulations prescribing the standards for the processing of personal data. In addition, Section 22 provides for the Minister to establish and maintain a register of approved information security service providers, which would likely include personal data of such providers recorded in the register. The Governor is authorized to prescribe the particulars that will be recorded in such registers.

Obligations of the entity processing personal data

Obligations pertaining to electronic signatures are explained below under 4.E.13.

Section 24 of the Act echoes the principle of confidentiality of personal data; it establishes that information provided to information security service providers must be kept confidential and not be disclosed unless one of the conditions listed under Section 24(2) is present.

Section 30 mirrors the internationally recognized principle that intermediaries, such as internet service providers, cloud platforms, or e-commerce service providers, are not liable for processing personal data transmitted through their systems if they act as passive conduits, provided that they are liable to comply with any contractual obligations and any order of a court or a competent authority.

Data subject rights

The Act does not explicitly address data subject rights such as right to access, rectify or erase their personal data.

Cross- border transfers of personal data

The Act does not restrict cross-border data transfers. Under Section 20, the Act provides for the recognition of foreign electronic signatures, but does not control whether, how or where personal data may or may not be transferred abroad.

Institutions and penalties

The Act makes no provision in relation to established institutions to oversee compliance nor does it mention penalties associated with non-compliance or misuse of exchange of electronic records and personal data. The Act does not establish or authorize an entity responsible for overseeing and implementing its provisions related to electronic records.

Conclusion

While the Electronic Transactions Act provides a framework for regulating the exchange of electronic records and ensuring the validity of electronic documents and signatures, it addresses inadequately several aspects pertaining to data protection. The Act would not conflict with a data protection framework aligned

with international good practices. It would be supplemented from its provisions especially as it pertains to security safeguards and cross-border data transfers. It would also ensure that both originators and addressees are held accountable for the responsible processing of personal data.

4.E.13 E-signatures

Introduction and scope of application and key terms

E-signatures are governed by Part 5 of the Electronic Transactions Act Cap 11.32.

Under Section 2 of the Act, "*electronic signature*" is defined as:

> *an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record.*

The Act also defines a "*signature device*" as:

> *unique data or a uniquely configured physical device, which is used by the signatory for the purposes of creating an electronic signature.*

The Act sets out certain requirements and obligations for "information security service providers." Although these service providers are not explicitly defined, "*information security service*" is defined as:

> *a service […] which is provided to an originator, intermediary or recipient of an electronic record, and which is designed to –*
>
> *(a) secure that that record can be accessed, or can be put into an intelligible form, only by certain persons; or*
>
> *(b) secure that –*
>
> *(i) the authenticity;*
>
> *(ii) the time of processing; or*
>
> *(iii) the integrity,*
>
> *of such record is capable of being ascertained.*

The use of electronic signatures would typically constitute processing of personal data under a data protection law.

Lawful basis for processing

The Act does not explicitly set out lawful bases for processing of personal data that may be linked to the creation, collection, storage, verification, and transmission of electronic signatures. However, electronic signatures may be used to enter into a contract or to perform contractual obligations. Therefore, the performance of a contract would be a lawful basis for processing the personal data embedded within these signatures (e.g., name, email address, unique identifiers).

Obligations of the entity processing personal data

The Act echoes the data protection principle of "integrity" of personal data inasmuch as the validity of an electronic signature is conditional upon the integrity of the information to which it relates being maintained, i.e., that the information has not been altered.

Section 29 outlines the responsibilities of signature device holders and requires them to prevent unauthorized use of their signature device. Their obligations also include notifying the relevant parties if they suspect their signature has been compromised and ensuring that the information associated with their signature is accurate.

Additionally, the Act defines "information security service" to include services that ensure the integrity of a record can be ascertained.

Data subject rights

The Act does not data subject rights in relation to the right to access, correct or erasure their personal data provided in the context of e-signatures.

Cross-border transfers of personal data

The Act does not restrict cross-border data transfers. Under Section 20, the Act provides for the recognition of foreign electronic signatures, but does not control whether, how or where personal data may or may not be transferred abroad.

Institutions and penalties

The Act does not mention any established institution or body responsible for enforcement nor does it mention penalties associated with non-compliance.

Conclusion

The Electronic Transactions Act, as it pertains to governing electronic transactions, lacks several key requirements covering processing of personal data. This framework would not conflict but would benefit from a generally applicable data protection framework developed in alignment with global best practices.

4.F Saint Kitts and Nevis

4.F.1 Data protection

Overview

Saint Kitts and Nevis' legal framework on protection of personal data is governed by the Data Protection Act of 2018 ("Act"). The Act applies across the economy and addresses protection of personal data by private and public entities, including the Houses of Parliament. The Act largely mirrors the OECS Model Data Protection Law of 2016.

While the Act establishes certain key rights and obligations regarding protection and processing of personal data, it does not include some key elements from international good practices outlined in Section 2 of this report. Based on our research and information from our local team, this Act has not yet been proclaimed.

Scope of applicability

The section below is generally consistent with international good practices, applying to both private and public entities and defining personal data to include automated processing. However, as discussed further, the Act's scope is overly restrictive, covering only a limited range of processing activities. To fully align with international standards, the scope should be expanded.

Applicability limited to "commercial transactions"

Similar to the OECS Model Bill, this Act restricts the definition of personal data to information "related to commercial transactions." A detailed analysis and recommended approach regarding this limitation are provided in the context of the OECS model Bill, as discussed in Section 3.A.1of this report.

Broad exemption for processing by regulatory authorities

Similar to the OECS Model Bill, Section 21(2)(e) of the Act exempts from several of the data protection principles personal data that is processed for the purpose of discharging regulatory functions. See Section 3.A.1of this report.)

General elements of a data protection law

Some of the definitions contain contradictions, lack clarity and require revision to align with international good practices.

Definition of "personal data" is potentially limiting

As with the OECS Model Bill, the Act's definition of personal data may limit the application of the Act (See Section 3.A.1 of this report.)

Definition of "sensitive personal data" excludes important attributes

As with the OECS Model Bill, the Act's definition of sensitive personal omits certain attributes which should be afforded additional safeguards when being processed. (See Section 3.A.1 of this report.)

Use of the terms "data users," "public bodies," "private bodies" and "persons"

As with the OECS Model Bill, the Act uses the terms "data users", "private bodies", "private bodies" and "persons" inconsistently. This drafting approach creates limitations, confusion and shall be revised. (See Section 3.A.1of this report.)

No definition of "consent"

As with the OECS Model Bill, the Act does not define "consent". (See Section 3.A.1 of this report.)

No clear concept of a "data processor"

As with the OECS Model Bill, the Act does not define "data processor". (See Section 3.A.1of this report.)

Relation with other national legal instruments

As with the OECS Model Bill, Section 5 of the Act concerning its effect on other laws may confuse matters (See Section 3.A.1of this report).

Principles governing the processing of personal data

The Act reflects data protection principles in Sections 7-13, addressing lawful bases, transparency, security, purpose limitation, and data quality. However, the current formulation of these principles could be improved.

Principle of lawful, fair and transparent processing

As with the OECS Model Bill, the Act does not include a principle mandating that personal data be processed in a lawful, fair, and transparent manner, as is required by established global best practices. (See Section 3.A.1of this report.)

Principle of data minimization

As with the OECS Model Bill, the Act does not explicitly include a "minimum necessary" standard for processing of personal data. (See Section 3.A.1of this report.)

Lawful basis for public interest

As with the OECS Model Bill, the Act does not include a lawful basis on necessity for substantial public interest. (See Section 3.A.1of this report.)

Additional protection for processing personal data of children or persons with limited capacity to consent

As with the OECS Model Bill, the Act does not include additional protection for the processing of personal data for children and persons lacking the legal capacity to consent. (See Section 3.A.1of this report.)

Limitations on data retention do not have exceptions

As with the OECS Model Bill, the Act sets out the "*retention principle*" but limiting personal data retention by data users too tightly. (See Section 3.A.1of this report.)

Individual rights concerning personal data

Sections 14-19 of the Act outline the key data subject rights and set out the circumstances and timelines under which they should be exercised. While they are largely aligned with international good practices, the Act does not provide the rights of data subjects to withdraw consent, oppose the processing of their personal data with automated means, and delete their personal data. (See Section 3.A.1of this report.)

Data security

The Act has several significant omissions, notably the lack of requirements for data processors and data controllers to provide notifications in the event of a data breach.

Lack of specific data security requirements

Section 10 of the Act outlines the obligation of a data user to process personal data securely. As with the OECS Model Bill, the Act could provide greater specificity to support effective security frameworks for safeguarding personal data. (See Section 3.A.1of this report.)

No personal data breach notification obligations

As with the OECS Model Bill, the Act does not include any personal data breach obligations. (See Section 3.A.1of this report.)

No requirements on data users when engaging data processors

As with the OECS Model Bill, the Act does not require data users to take any measures to ensure that data processors can assist them in complying with the Act. (See Section 3.A.1 of this report.)

No data processor liability for data security

Section 10(1) addresses data security requirements for data users. Section 10(2) addresses data security requirements for data processors, but, as with the OECS Model Bill, it does not make data processors directly liable for failure to adopt adequate data security measures. (See Section 3.A.1 of this report.)

No requirement for Data Privacy Impact Assessments (DPIAs)

As with the OECS Model Bill, the Act does not mandate that data users conduct Data Protection Impact Assessments (DPIAs). (See Section 3.A.1of this report.)

Cross-border transfers of personal data

As with the OECS Model Bill, the Act does not include provisions on cross-border data transfers. (See Section 3.A.1 of this report.)

Institutions

Our internal research and contacts attempted by our local team members were not able to locate an online presence or physical establishment of the Information Commissioner. Lack of provisions on the funding of the Information Commissioner.

Lack of provisions on the funding of the Information Commissioner

As with the OECS Model Bill, neither the Act nor the Freedom of Information Act that establishes the Information Commissioner provides for the funding of the Commissioner. (See Section 3.A.1 of this report.)

Enforcement

Disproportionate and unclear fines and penalties

Overall, the Act provides several mechanisms through which data subjects can file a complaint to initiate the Commission's investigation, and, in turn, the Commission issue an enforcement notice when it has

identified a violation of the Act (Sections 25-26). The decisions of the Commission are subject to appeal, which provides an additional accountability layer. In addition, the Act applies liability to senior leadership of legal entities, making them directly liable for offences. This is potentially somewhat harsh: it should suffice to address liability to the entity rather than its officers. We would also discourage the use of criminal offences for data protection violations. (See Section **Error! Reference source not found.** of this report.)

4.F.2 Cybersecurity and cybercrimes

Introduction, scope of application and definition of key terms

The Electronic Crimes Act 4.41 aims to combat cybercrime through computer systems and promote data integrity. The Act's primary objectives include preventing unauthorized access, modification, and misuse of computer systems. The Act prohibits knowingly causing a computer system to secure access to a program or data without lawful authority to do so and various other forms of unlawful access, interception and modification of computer systems and data (Sections 4 – 17). Additionally, it facilitates the collection of electronic evidence crucial for criminal investigations. To achieve these goals, the Act establishes rules and protocols for data handling and processing. It also enforces strict criminal penalties for specified offenses to deter malicious activities and promote responsible use of computer technologies.

Section 2 of the Act defines the term "computer data" as –

> *any representations of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.*

This broad definition does not differentiate between personal and non-personal data. Therefore, the Act's prohibitions and obligations apply to what are commonly referred to in data protection laws as "personal data."

Lawful basis for processing personal data

In the Act's various offences of using, intercepting, modifying and accessing data and computing systems its reference to "without lawful authority" echo the data protection principle of lawful processing, aiming to ensure that data handling activities are lawful.

Obligations of the entity processing the personal data

Although the Act does not provide affirmative general data processing obligations (only criminal prohibitions), it reflects some notions often included in data protection laws:

- Data Integrity: Sections 5 and 6 criminalize interfering with data and computer systems, which align with the data integrity principle.
- Confidentiality: Section 7 makes it an offence to intercept transmissions, including non-public communications or electromagnetic emissions carrying computer data. This supports the confidentiality of personal data by criminalizing unauthorized surveillance and interception.
- Lawful Basis for Processing: The provisions on procedural powers (Sections 18-22) provide strict guidelines for law enforcement to access, seize, or intercept electronic data only through judicial authorization, such as warrants or magistrate orders. This echoes the principle of lawful processing, which ensures that access to personal data is limited to legal grounds.

However, the Act does not include obligations to implement technical and operational security measures necessary to safeguard personal data involved in its processing activities. Not does it include provisions for data breach notifications in the event of a data breach or incident

Data subject rights

The Act does not address data subject rights over personal data.

Cross-border transfers of personal data

The Act does not address cross-border processing of any data.

Institutions and penalties

The Act does not establish or designate any regulatory authority or institution responsible for overseeing compliance other than typical investigation and enforcement by police subject to judicial oversight.

The penalties stipulated in the Act include fines and imprisonment with application depending on the nature of the offence and whether it is the first or subsequent offence.

Conclusion

The Electronic Crimes Act 4.41 broadly addresses two forms of processing that would relate to typical data protection law. The first is to prohibit certain forms of data processing, particularly where performed without lawful authority or having other criminal aspects. The second is to affirmatively require certain procedures (e.g., judicial order) for police and other authorized persons to obtain data (which would include personal data) in the context of investigations and prosecution. In doing so, the Act establishes a framework for combating cybercrimes and incorporates some provisions that align with data protection principles. However, it does not include many typical data protection provisions, e.g., security standards and institutional structures, which are essential for effectively safeguarding personal data involved in the prohibited or authorized processing activities.

A generally applicable data protection framework that aligns with global best practices would address these gaps in providing the necessary supplementary measures to ensure robust protection of personal data.

4.F.3 Consumer protection

Introduction, scope of application and definition of key terms

The Consumer Protection Act 2023 provides for the promotion and protection of consumer interest, in relation to the supply of goods and the provision of services; to ensure protection of life, health and safety of consumers. It establishes a Consumer Affairs Department to oversee and enforce the provisions of the Act.

Lawful basis for processing

The Act provides for the collection and processing of consumer complaints, which involves the processing of personal data. Section 21(2) mandates that consumer complaints be submitted using the form in Schedule 2. The form requests personally identifiable information such as the complainant's name, address, contact details, details of the complaint, and supplier's information, which could also include personal data.

Section 21(3) states that complaints can be made orally but must be reduced to writing and confirmed with a signature or identifying mark. This means that personal data is recorded and stored. In addition, Section 23(1) specifies that upon receipt of a complaint, the Director must provide a certified copy of the complaint to the complainant and submit a copy of the complaint to the Consumer Protection Board. This implies that personal data is shared within governmental or regulatory bodies handling consumer protection.

Section 24 allows the Consumer Affairs Department to conduct investigations into complaints. Section 26 grants the Director or an authorized officer the power to obtain further information or documents from consumers and suppliers and require individuals to appear and provide oral or written evidence. These provisions expand the scope of personal data processing as additional information may be collected during these steps.

Obligations of entities to process personal data

The Act includes provisions related to the confidentiality of business information, particularly in Sections 172 and 173. Section 172 prohibits any person from publishing or disclosing documents, communications, or information obtained under the Act without written consent from the Chairperson, unless necessary for

official duties. It also grants privilege to any statements or documents provided in an investigation or proceeding before the Board, treating them as if they were privileged in a court of law. On the other hand, Section 173 mandates that the Consumer Protection Board and any individual administering the Act must treat all documents, information, and matters disclosed in the course of administration as secret and confidential.

These provisions restrict unauthorized disclosure of information obtained under the Act and provide safeguards for the personal data processed under the Act.

Data subject rights

Section 78 establishes the right to information in plain and understandable language. Accordingly, consumers have the right to receive clear, intelligible, and comprehensible information in contracts, disclosures, or agreements. This aligns with the data protection principle of transparency, ensuring that individuals understand how their data is used.

While the Act does not explicitly recognize traditional data subject rights (such as the right to access, rectification, erasure, or objection to data processing), it establishes consumer rights that overlap with privacy and data protection principles.

Cross- border transfers of personal data

The Act does not contain a specific framework for cross-border transfers of personal data. However, the provisions on distance selling suggest an implied regulatory framework for international consumer transactions that may involve cross-border personal data processing. A generally applicable data protection law would complement and support these provisions by establishing rules and safeguards for cross-border processing of personal data.

Institutions and penalties

The Act establishes the Consumer Protection Board, the Consumer Affairs Department, and the Appeals Tribunal. The Board is responsible for overseeing consumer protection matters, resolving complaints, and ensuring compliance with the Act. The Department is responsible for receiving and investigating consumer complaints. It plays a crucial role in collecting evidence and reporting findings to the Consumer Protection Board. Finally, the Appeals Tribunal is an independent body that hears appeals against decisions made by the Consumer Protection Board.

Unauthorized disclosure of documents, communications, or information obtained under the Act is subject to a fine of up to $5,000 or imprisonment of up to six months, or both.

Conclusion

The law on consumer protection lacks most aspects of personal data protection. It would not contradict a generally applicable data protection law aligned with global best practices, and it would be appropriately supplemented by the provisions of such a law.

4.F.4 Freedom of information requests

Introduction, scope of application and definition of key terms

The Freedom of Information Act 2018 governs information requests made to public bodies. A request for information is "*a request in writing to any official of a public body that is in sufficient detail to enable an experienced official to identify, with reasonable effort, whether or not the body holds a record with that information.*"

Section 8 provides that a record includes:

> *any recorded information, regardless of its form, source, date of creation, or official status, whether or not it was created by the body that holds it and whether or not it is classified.*

The definition of records does not distinguish between personal or non-personal data. Therefore, the information obtained from public bodies may include personal data.

The Act defines "personal information" as

> *information which relates to a natural living person who can be identified from that information.*

This definition covers a smaller subset of data compared to the generally accepted definition of "personal data" in data protection frameworks, because it relates to only data that relates to living persons. The exclusion of personal data relating to deceased persons is not aligned with international best practice.

Lawful basis for processing

The Act provides a lawful basis for processing inasmuch as it allows individuals to make information requests about the records containing their personal data that are kept by public bodies.

The processing of personal data by public bodies during the record keeping process is carried out based on the lawful basis of fulfillment of legal obligations as set out in the relevant legislation. Subsequent processing activities carried out by the public bodies in response to information requests are performed as part of their official duties under the Act.

Obligations of entities to process personal data

The Act sets out several obligations for public bodies that align with key data protection principles:

- Transparency: Under Section 18, public bodies must publish and disseminate information about their record-keeping systems, the types of information they hold, the categories of data they publish and the procedures for making an information request at least annually. This obligation reflects the principle of transparency as it ensures that data subjects are informed about how their records are maintained.
- Data Accuracy: Section 20 mandates that public bodies implement adequate procedures for correcting personal information, which reinforces the principle of data accuracy.
- Confidentiality: Section 28 establishes a confidentiality obligation for public bodies, which ensures that information is not unlawfully disclosed and is consistent with data protection best practices.
- Enhanced Protections for Sensitive Data: Section 29 requires public bodies to implement additional safeguards for health data, which echoes the principle of providing enhanced protections for sensitive categories of data.
- Lawful Basis for Processing: Section 30 permits a public body to refuse to confirm or disclose the existence of a record if required by law or a court order, which reflects the principle of lawful data processing and the need for legal justification when restricting access to information.
- Data Retention Periods: Section 34 sets out a data retention period of 30 years. While most data protection frameworks advocate for proportionate retention periods, they also emphasize the irreversible deletion of data once it is no longer needed for its original purpose.

Data subject rights

The Act provides the following data subject rights:

- Right to be Informed: The Act provides data subjects with the right to be informed as set out in Section 5. Accordingly, individuals have the right to be informed whether or not a public body holds a record containing their personal data.

- Right to Access: Section 13 provides data subjects with the right to request a copy of the record. However, the public body may refuse to provide the information in the form requested by the applicant if it interferes with the effective operation of the public body or would damage the record.
- Right to Rectification: The Act also provides the implied right to rectification by requiring public bodies to establish procedures for correction of personal data (Section 20).

The Act does not provide other data subject rights such as the right to erasure, the right to restrict processing or object to processing.

Cross- border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act does not mention an institution established to oversee these provisions, but it appoints an Information Commissioner who receives regular reports and shall ensure compliance with the Act. The penalties associated with the Act include criminal sanctions inclusive of fines up to $5,000 or imprisonment of up to two years for obstructing access, interfering with records or unlawfully destroying information.

Conclusion

The Act seeks to promote transparency and grant individuals the right to access information held by public bodies. While it introduces some safeguards, it falls short of international best practices in data protection. Given that the Act governs the disclosure of data, including potentially personal data, it would significantly benefit from the adoption of a comprehensive data protection framework aligned with global standards.

Additionally, the Act's definition of "personal information" may conflict with such a framework due to its exclusion from deceased persons. Amending this definition alongside the introduction of new data protection legislation would be a prudent approach to ensure legal consistency.

Finally, the 30-year data retention period could be revised to incorporate a proportionality standard, ensuring that data is retained only for as long as necessary for its original purpose.

4.F.5 Health

Introduction, scope of application and definition of key terms

The Public Health Act Cap 9.21 of 2020 regulates several aspects of public health, including the duties, powers and functions of the Minister and various entities involved in public health. The main focus is on issues such as the prevention, treatment and limitation of diseases, conducting investigations and ensuring the proper functioning of the public health institutions.

The Act provides only limited references to personal data processing activities:

- Sections 5 and 7 empower the Minister to establish boards and committees, as well as appoint key public health professionals, including the Chief Medical Officer for the State, Medical Officers of Health, Community Health Nurses, Environmental Health Officers, and other public health officers. The appointment of these individuals and the formation of these committees inherently involve the processing of personal data.
- Section 9 authorizes the Minister to establish a Health Emergency Operating Centre, which entails the collection and medical analysis of data. This implies the processing of personal information, including health records, particularly during national health emergencies.
- Under Regulation 8 (Schedule 2), medical professionals are mandated to complete the "Notifiable Disease Form," which requires them to record personal information about their patients. This includes the patient's name, gender, contact details, profession, medical records, and diagnosis.

The Act does not place any obligations of confidentiality on the processing of personal data under covered by the Act.

Lawful basis for processing personal data

The Act provides a lawful basis for the collection, management, assessment, and storage of personal data related to the appointment of medical officers and other relevant officials, as well as the establishment and operation of the Health Emergency Operating Centre. Personal data may be lawfully processed by the Health Emergency Centre on the grounds of public emergency and vital interest in relation to public health. Given that the Centre operates during national health emergencies or disasters, such processing is essential to safeguarding public well-being and ensuring an effective emergency response.

Similarly, patients provide their personal information when completing required forms as part of their contractual agreement with their medical provider and to fulfill the legal obligations set forth by this Act. The data collected through these forms are processed in accordance with the Act, ensuring that patients receive appropriate medical care.

Obligations of the entities processing personal data

The Act does not impose clear obligations on entities processing personal data, nor does it provide guidance on ensuring that the data collected are kept secure or are used only for the intended purpose.

Data subject rights

The Act does not provide for rights of individuals with respect to their personal data, such as the right to access, rectification or erasure.

Cross border transfer of personal data

The Act does not address cross-border transfer of personal data.

Institutions and penalties

The Act includes a provision for penalties which focuses on non-compliance with various public health duties, such as refusing to answer inquiries from health officers or obstructing their duties under section 16. However, these penalties are focused on public health offenses rather than breaches of data protection or privacy related violations.

The Act does not establish institutions and authorities mandated to oversee processes related to personal data. However, it establishes committees and boards responsible for supporting the Minister in fulfilling his or her responsibilities under the Act. Additionally, the Act grants the Minister the authority to activate the Health Emergency Operating Centre which, in the event of a national emergency, may process personal data as part of its response efforts.

Conclusion

The Act lacks specific personal data safeguards, such as requirements for entities to comply with data security and management standards, recognition of individuals' rights over their personal data, and clear penalties for data protection violations. However, this absence would not create conflict with a generally applicable data protection law that would align with international good practices. Such a law would bridge this gap by establishing the necessary protection and regulatory framework.

4.F.6 Education

Introduction, scope of application and definition of key terms

The Education Act No.9 of 2005 provides for a regulatory system for the delivery of education services in Saint Christopher and Nevis. The provisions in the Act mainly focus on the collections, maintenance and disclosure of students' personal data and records.

The Act regulates the management and handling of students' personal information, including:

- Section 22 requires principals to maintain records on students in accordance with the Chief Education Officer's guidelines and to periodically provide the parents with a report on the student's academic performance and conduct.
- Section 27 requires a birth or baptism certificate to be admitted to a primary school.
- Section 30 sets out the content of the Student's Register, which includes the name and date of birth of each student. Additionally, the Chief Education Officer may prescribe other information to be included in the Student's Register, which may include other types of personal data.
- Section 44 mandates principals to report students' lack of attendance to the relevant authorities, such as the Chief Education Officer. Such reporting includes the names, ages and residences of students who do not attend school as required.
- Section 138 lists under the duties of teachers that every teacher must "*maintain whatever registers, records, or other forms as may be required by the principal, Chief Education Officer, or this Act and make those registers, records, or other forms available for inspection by the Chief Education Officer or by any person authorized by the Chief Education Officer.*" These registers and records are likely to include personal data on students and would be available for inspection by authorized persons, which allows for further processing of this data.

Lawful basis for processing

The main lawful basis for the processing of personal data under the Act is performing administrative functions (Sections 27, 30, and 138). As described in the previous section, the Act provides for processing of personal data about students by principals for managing student records, monitoring attendance, and performing other administrative functions.

Additionally, Section 22(6) requires parental or individual consent for the examination of student records. This provision ensures that personal data is accessed and reviewed only with explicit approval.

Obligation of the entity to process personal data

The Act imposes obligations on schools and principals concerning the processing of personal data, reflecting key principles of data protection:

- Accurate Data Maintenance (Sections 22 and 30): Principals are responsible for maintaining accurate student records and registers under sections 22 and 30, which echoes the principle of data accuracy. Additionally, the Chief Education Officer must review any rectification requests on student records and provide direction on disputes related to any inaccuracies.
- Privileged Use and Limited Third-Party Access (Section 22(5)): Student records cannot be disclosed to any other person without the written consent of the parents or the student, if the student is 18 years or older. The Act imposes limitations on third-party access without consent, which promotes confidentiality and integrity of personal data.
- Data Minimization (Section 22(6)): Records may only be used by the relevant school and departmental officials as necessary for performing their duties, which echoes the principle of data minimization.

The Act does not contain a requirement for maintaining security of personal data in the student records.

Data subject rights

The Act provides several rights to the students as well as the parents regarding their personal data such as:

- Access to Records: Section 22(5) provides the data subjects the right to access, which establishes that the parents of a student or the student who is 18 years or older may access that student's

record and obtain copies thereof. This provision promotes transparency and allows individuals to stay informed about the information held about them.

- Rectification of Records: Section 22(8) sets out a right to rectification, as it provides authorized persons under the Act to request the correction of inaccuracies in the records. If a request for rectification is denied or results in an unfavorable outcome, the Act provides an appeals process, allowing for further review mechanism.

Cross- border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act appoints the Chief Education Officer to oversee record-keeping and compliance with its reporting requirements. It also establishes the Education Appeal Tribunal to hear appeals against decisions made by the Chief Education Officer. The penalty for unauthorized disclosure of student records is a fine of up to $1,000, which may not be high enough to deter non-compliance.

Conclusion

The Act promotes transparency in the management of students' personal data by establishing rights for students and clearly defining institutional responsibilities related to data processing. However, it does not include provisions covering data retention periods, data security measures, or cross-border data transfers, which are essential components of a comprehensive data protection framework. A generally applicable data protection framework, aligned with international good practices, would supplement this Act's provisions.

4.F.7 Financial services (including digital financial services)

Introduction, scope of application and definition of key terms

The Banking Act Cap 21.01 governs the regulation of banking business, the establishment of a unified banking space and related matters within Saint Kitts and Nevis. It covers the processing of personal data inasmuch as it applies to depositor and customer information, their financial transactions and related information. It also covers the handling of personal information of financial institutions shareholders and officers occupying positions in financial institutions.

Although the Act does not establish a full data protection framework, it does provide for a duty of confidentiality and "secrecy of information".

Additionally, the Financial Services Regulatory Commission Act Cap 21.10 establishes the Financial Services Regulatory Commission. This regulates providers of financial services, except for financial services covered by the Banking Act, provides for related or incidental matters. It addresses the processing of personal data to a limited extent and imposes a duty of confidentiality on officials of the Financial Services Regulatory Commission.

Lawful basis for processing

Section 178(1) of the Banking Act sets out the conditions under which personal data related to depositors or customers may be processed lawfully. They specify that individuals who have access to such data in their professional capacity must not disclose them unless one of the following legitimate bases is met:

- Consent: Disclosure may occur if the depositor, customer, or their authorized representatives provide written approval.
- Legal Obligation: Information may be shared when required by the Act itself or by a lawful order of a court with proper jurisdiction.

- Regulatory and International Agreements: Disclosure is permissible under relevant laws of Saint Kitts and Nevis or agreements among Participating Governments (i.e., members of the ECCU), ensuring compliance with broader legal frameworks.
- Legitimate Business Interests: Certain exceptions allow for limited data sharing in response to legitimate business requests, such as providing a general credit rating, or when conducting due diligence in the context of potential acquisitions, so long as appropriate safeguards are in place.

Section 178(2) also allows limited disclosures for business needs, as described in the next section.

Obligations of the entity processing personal data

Licensed financial institutions have obligations under the Banking Act to maintain the confidentiality of data. Section 178 prohibits unauthorized disclosure of customer information, which includes identity information and transactions. Disclosures are permitted if the customer gives written consent or where needed for legitimate business purposes such as credit ratings.

The Banking Act does not provide an obligation for establishing and maintaining a certain level of security measures to safeguard financial information, including financial data. Nor does it address personal data breaches. Given the substantial amounts of financial information and sensitive personal data managed by financial institutions, it would be appropriate for such data to be subject to such data protection obligations.

Under Section 15 of the Financial Services Regulatory Commission Act, the Commissioner, officers, and employees of the Commission are required to take an oath of secrecy. They are also prohibited from disclosing any information relating to the affairs of a customer, member, client, or policyholder of a regulated entity, as well as any confidential matters concerning the Commission itself, obtained in the course of their duties.

Data subject rights

The Acts make no provisions for rights of data subjects in the Act.

Cross border transfers of personal data

Section 94 of the Banking Act authorizes the Central Bank to establish agreements with foreign supervisory authorities and resolution agencies to collaborate and share information. This cooperation is essential for overseeing and managing financial institutions, including banks and financial holding companies, particularly in scenarios where these institutions fail or are at risk of failure. Such agreements may only be entered into if the Central Bank is assured that the foreign authority will maintain the confidentiality of all shared information. Although generally not focused on personal data, this provision underscores the Act's recognition of the necessity for international cooperation within the banking sector. It highlights the importance of reciprocal safeguards to ensure the confidentiality and integrity of data exchanged between jurisdictions.

Institutions and penalties

The Eastern Caribbean Central Bank formulates and implements monetary policy and regulates and supervises financial institutions in order to maintain the integrity of the financial system. The Central Bank manages the issuance and circulation of the national currency, oversees foreign exchange reserves, and ensures efficiency and security of payment and settlement systems.

Under the Banking Act, the Central Bank has the power to impose several penalties for violations related to financial matters. Section 96 provides that any licensed financial institution that knowingly supplies false or misleading statements, returns, information, or data in any material is subject to a penalty of $25,000. This is aligned with typical data protection obligations to maintain the accuracy of personal data.

Conclusion

The Banking Act Cap 21.01 and the Financial Services Regulatory Commission Act establish a foundational framework for maintaining confidentiality in banking operations. However, they do not

address several critical areas necessary for the comprehensive protection of personal data within financial services. The Acts lack provisions for data security measures, the rights of data subjects, and the regulation of cross-border personal data transfers. The Acts would not conflict with, but would rather be supplemented by, a generally applicable data protection framework aligned with global best practices.

4.F.8 National identification (including digital and functional forms)

There is currently no legislation on this area that has been enacted in Saint Kitts and Nevis.

4.F.9 Passports

The Passport and Travel documents Act Cap 6.04 sets out the institutional powers in relation to the issuing and renewal of passports and travel documents. It does not include provisions on the processing of personal data.

4.F.10 Civil registration

There is currently no legislation on this area that has been enacted in Saint Kitts and Nevis.

4.F.11 Electronic communications

Introduction, scope of application and definition of key terms

The electronic communications sector is governed by the Electronic Communications Act 2021 (the "Electronic Communications Act"), which repealed and replaced the Telecommunications Act, Cap. 16.05.

The Electronic Communications Act regulates the electronic communications services and governs licensing, data protection and consumer rights. Its primary purpose is to implement the objectives of the Treaty establishing the Eastern Caribbean Telecommunications Authority.

The Act addresses processing and protection of personal data to a limited extent, specifically in the following instances:

- Personal data are being shared with the Minister, ECTEL, and the Commission and assessed as part of the application process for licenses, frequency authorizations, and any subsequent modifications or renewals of these licenses.
- Under Section 109, licensees may hold personal information relating to retail customers, which cannot be disclosed, unless a lawful basis exists.

The activities of disclosing, safeguarding, and maintaining personal data for the purpose of issuing licenses and for delivering telecommunication services constitute personal data processing.

Lawful basis for processing

The Act contains various lawful basis for processing personal data:

- Personal data collected and stored as part of application processes are processed pursuant to the lawful basis of a legal obligation under this Act.
- Section 109 states that subscriber personal data and messages may be disclosed only with the customer's consent or in compliance with a court order. This provision is aligned with the data protection principle of lawful processing.

Obligations of the entity to process personal data

- Section 23 provides that a commissioner, Chief Executive Officer, employee or member of an advisory committee, secretary, inspector or other employee shall take an oath of secrecy, mandating that personal data must remain confidential and may only be disclosed when a lawful basis exists.

- Section 147 provides that information which constitutes an "unjustified invasion of personal privacy" is protected from being disclosed in investigative records compiled for enforcement purposes, which reflects the intention of safeguarding individual's privacy.
- Section 88 mandates licenses to protect data in the prescribed manner.

Data subject rights

The Act does not address data subject rights.

Cross- border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act appoints the National Telecommunications Regulatory Commission (the Commission) to regulate telecommunications, issue licenses and ensure compliance with the Act. The role of the Commission is to monitor the telecommunication providers to ensure compliance with the Act.

Unauthorized disclosure of personal data is subject to a fine of up to $50,000 or imprisonment for up to 4 years, or both under Section 109.

Conclusion

The Act contains limited requirements for confidential processing of personal data and provides penalties for unlawful disclosures. However, it does not include any requirements for data security and minimization and secure cross border data transfers. The Act does not contain any provisions that would contradict or be inconsistent with a generally applicable data protection law.

4.F.12 Electronic transactions

Introduction, scope of application and definition of key terms

The Electronic Transactions Act Cap 18.44 governs electronic transactions, communication of electronic records, electronic signatures, documents and other transactions which involve the processing of personal data. Additionally, it also includes a chapter on e-government services.

The goal of the Act is to ensure that electronic transactions carry the same legal standing as traditional paper transactions. In this Act, the term "electronic transaction" is not used in its literal, commercial sense. Rather, it is defined broadly as *"the single communication or outcome of multiple communications involved in the sale or purchase of goods and services."* The term "transaction" includes:

(a) a transaction of a non-commercial nature;

(b) a single communication; or

(c) the outcome of multiple related communications.

This Act regulates personal data in the context of exchange of "electronic records" between two persons, designated as "the originator" and "the addressee".

As defined in Section 2:

"electronic record, "means a record processed and maintained by electronic means;

"originator," in relation to an electronic record, means a person who –

(d) sends an electronic record;

(e) instructs another to send an electronic record on his behalf; or

(f) has an electronic record sent by his electronic agent, but does not include –

(i) a person who sends an electronic record on the instructions of another; or

(ii) a person acting as an intermediary with respect to that electronic record; and

"addressee," in relation to an electronic record, means a person who is intended by the originator to receive the electronic record, but does not include a person acting as an intermediary with respect to that electronic record.

Although the Act does not use term "data" in the context of electronic records but rather in the context of electronic signatures, it defines data as:

any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable to cause an information system to perform a function.

Exchange of electronic records between an originator and addressee may include the following personal data: their names, email addresses, metadata such as the time and location of an email, identifiers included in a signature (phone numbers, physical addresses, and other contact details may be shared directly within the email content), along with any information revealed in the context of their communication.

According to the definition of "electronic records", which cover information "*processed and maintained by electronic means*", personal data undergo "*processing*" as they are transferred by the originator and subsequently received and stored by the addressee.

However, the Act does not impose any obligations on the originator, addressee or the intermediary of the electronic communications regarding the protection, maintenance of integrity, or safety of personal data. Additionally, there are no provisions concerning data subject rights, cross-border data transfers, or relevant institutions authorized to oversee electronic communications. As a result, electronic transactions would benefit from a comprehensive data protection framework that imposes obligations, rights, and responsibilities regarding the processing of personal data on both originators and addressees.

Lawful basis for processing personal information

The Act does not explicitly mention any lawful bases for processing personal data. Section 25 provides for the Minister to establish and maintain a register of approved certification providers, which would likely include personal data of such providers recorded in the register. The Minister is authorized to prescribe the particulars that will be recorded in such registers.

Section 34 sets out a notification and takedown mechanism for unlawful content, requiring complainants to submit detailed information including their identity and contact details. The legal basis for the processing of the complaints' personal data by intermediaries would be this Act.

Obligations of the entity processing personal data

Obligations pertaining to electronic signatures are explained below under 4.F.13.

Sections 32 and 35 mirror the internationally recognized principle that intermediaries, such as internet service providers, cloud platforms, or e-commerce service providers, are not liable for processing personal data transmitted through their systems if they act as passive conduits, provided that they are liable to comply with any contractual obligations and any order of a court or a competent authority.

Section 33 establishes safe harbor protections for intermediaries and service providers against liability for hosting or linking to infringing content. Section 34 establishes a takedown obligation for unlawful content for intermediaries. The "notice-and-takedown" requirements align with global best practices ensuring that intermediaries are only liable if they fail to act once notified. However, the Act does not include a counter-notification process, which would allow alleged infringers to challenge wrongful takedowns and reduce the risk of censorship.

Data subject rights

The Act does not explicitly address data subject rights such as right to access, rectify or erase their personal data.

Cross- border transfers of personal data

The Act does not restrict cross-border data transfers. Under Section 29, the Act authorizes the Minister to recognize electronic signatures or certifications established in another jurisdiction, but does not control whether, how or where personal data may or may not be transferred abroad.

Institutions and penalties

The Act authorizes the Minister to appoint the E-Commerce Advisory Board under Section 37. The board advises on matters related to electronic transactions, including advising on the administration of the Act, policy formulation, and regulatory oversight.

The Act does not include penalties associated with non-compliance or misuse of the exchange of electronic records and personal data.

Conclusion

While the Electronic Transactions Act provides a framework for regulating the exchange of electronic records and ensuring the validity of electronic documents and signatures, it addresses inadequately several aspects pertaining to data protection. The Act would not conflict with a data protection framework aligned with international good practices. It would be supplemented from its provisions especially as it pertains to security safeguards and cross-border data transfers. It would also ensure that originators, addressees and intermediaries are held accountable for the responsible processing of personal data.

4.F.13 E-signatures

Introduction, scope of application and definition of key terms

Electronic signatures are governed by Part 5 of the Electronic Transactions Act Cap 18.44.

Under Section 2 of the Act, "*electronic signature*" is defined as:

> *data in electronic form which is attached to, incorporated in or logically associated with other electronic data and which serves as a method of authentication.*

The Act also provides that "*signature*":

> *includes any symbol executed or adopted, or any methodology or procedure employed or adopted by a person with the intention of authenticating a record, including electronic or digital methods.*

The Act also sets out a verification mechanism for electronic signatures through a "certificate," which is defined as:

> *an electronic attestation issued by an approved certification service provider that—*
>
> *(a)links signature-verification data to a person and confirms the identity of that person; or*
>
> *(b)links time-verification data to an electronic record or to an electronic communication and confirms the associated date and time of that electronic record or electronic communication.*

Finally, Section 2 defines a "certification service provider as:

> *a person who issues electronic certificates or provides other services related to electronic signatures, which have been accredited by the accreditation authority.*

Lawful basis for processing

The Act does not explicitly set out lawful bases for processing of personal data that may be linked to the creation, collection, storage, verification, and transmission of electronic signatures. However, electronic signatures may be used to enter into a contract or to perform contractual obligations. Therefore, performance of a contract would be a lawful basis for processing the personal data embedded within these signatures (e.g., name, email address, unique identifiers).

Obligations of the entity to process personal data

The Act echoes the data protection principle of "integrity" of personal data inasmuch as the validity of an electronic signature is conditional upon the integrity of the information to which it relates being maintained, i.e., that the information has not been altered.

Section 30 outlines the responsibilities of signatories and requires them to prevent unauthorized use of their signature device. Their obligations also include notifying the relevant parties if they suspect their signature has been compromised and ensuring that the information associated with their signature is accurate.

Additionally, the Act defines "certification procedure" to include procedures designed to ensure that the integrity of an electronic record can be ascertained.

Cross-border transfers of personal data

The Act does not restrict cross-border data transfers. Under Section 29, the Act provides for the recognition of foreign electronic signatures, but does not control whether, how or where personal data may or may not be transferred abroad.

Data subject rights

The Act does not data subject rights in relation to the right to access, correct or erasure their personal data provided in the context of e-signatures.

Institutions and penalties

The Act does not establish any institutions that enforce the electronic signatures framework.

The penalties for non-compliance include imprisonment for up to 3 years or $20,000 for publishing an unlawful or invalid digital signature and imprisonment for up to 5 years or fines of $30,000 for creating or publishing a certificate for fraudulent purposes.

Conclusion

The Electronic Transactions Act, as it pertains to governing electronic transactions, lacks several key requirements covering processing of personal data. This framework would not conflict but would benefit from a generally applicable data protection framework developed in alignment with global best practices.

4.G Saint Lucia

4.G.1 Data protection

Overview

Saint Lucia's Data Protection Act of 2011, as amended in 2015 ("Act"), applies across the economy and addresses protection of personal data by private and public entities.

The Act is being implemented in phases. Under the Data Protection Act Commencement Order, several key provisions came into effect on January 31, 2023, including Part I, Sections 32–43 of Part III, Part VI, and paragraphs (a) to (g) of Schedule 2. These sections establish that the Act applies to data processing activities in Saint Lucia, both by businesses based in the country and those outside it that process data within Saint Lucia.

The Order enforces fundamental data protection principles such as purpose limitation, accountability, adequacy of safeguards, fairness, and transparency in data processing. It also imposes obligations on data controllers, including requirements for the collection, processing, security of personal data and mandatory registration with the National Data Protection Commissioner. Additionally, the Order specifies exemptions for certain processing activities, including those related to national security, crime, taxation, domestic purposes, journalism, health, social work, research, statistics, historical research, and matters covered by legal professional privilege. The timeline for the remaining provisions of the Act to come into effect is currently unknown.

While certain aspects of the Act align with the OECS Model Bill, it also introduces novel elements that better align it with global best practices compared to other jurisdictions under assessment. However, the Act still contains some omissions and areas that require further clarification.

Scope of applicability

Potential uncertainty over the scope

Under Section 3, the Act applies to data controllers where:

> *(a) the data controller is established in Saint Lucia and the data is processed in the context of the business of that establishment; or (b) the data controller is not established in Saint Lucia but uses equipment in Saint Lucia for processing data otherwise than for the purpose of transit through Saint Lucia" (…)*

The scope of the Act under subparagraph (a) is limited to data controllers "in the context of the business" of the data controller's establishment. To the extent that this could be interpreted to refer only to a firm, it might exclude individuals and non-governmental organizations, charities and unregulated entities. International good practice would not exclude these. The provision could refer instead to "activities."

General elements of a data protection law

Definition of the term "personal data"

The Act defines personal data as "information about a data subject that is recorded in any form" and provides various examples of such information. However, this definition is somewhat restrictive, as it omits personal data that, while not directly identifying an individual, could make them identifiable when combined with other information. We recommend revising the definition of "personal data" to include any information relating to an identified or identifiable natural person in alignment with international good practices. (See Section 2.A.1.)

Definition of "sensitive personal data" excludes important attributes

As with the OECS Model Bill, the Act excludes certain attributes from its definition of sensitive data. (See Section 3.A.1of this report.)

Unclear definition of "data controller"

The Act defines a data controller solely with reference to a "*person*". To the extent that his could leave any uncertainty about the scope of this, it could be revised to explicitly include both natural and legal persons, as well as public authorities, agencies, or other bodies that, either alone or jointly, determine the purposes and means of personal data processing.

No clear concept of a "data processor"

As with the OECS Model Bill, the Act does not define "data processor". (See Section 3.A.1of this report.)

No definition of "consent"

As with the OECS Model Bill, the Act does not define "consent". (See Section 3.A.1of this report.)

Principles governing the processing of personal data

Additional protections for processing personal data of children or persons with limited capacity to consent

As with the OCES Model Bill, the Act does not include additional protections for the processing of personal data for children and persons lacking the legal capacity to consent. (See Section 3.A.1of this report.)

Principle of data minimization

As with the OECS Model Bill, the Act does not explicitly include a "minimum necessary" standard for processing of personal data. (See Section 3.A.1of this report.)

Individual rights of data subjects concerning personal data

Sections 52-57 of the Act establish key data subject rights and set out circumstances and timelines under which they can be exercised. While they are largely aligned with international good practices, except for the right of data subjects to withdraw automated processing.

Right to remove consent for automated processing

We recommend introducing the right of data subjects to withdraw their consent for processing activities through automated means.

Data security

The Act has certain omissions with respect to data security, notably the lack of requirements for data processors and data controllers to provide notifications in the event of a data breach.

Lack of specific data security requirements

Section 45 of the Act outlines the obligation of a data controller to process personal data securely. As with the OECS Model Bill, the Act could go further in providing specificity to support effective security frameworks for safeguarding personal data. (See Section 3.A.1of this report.)

No personal data breach notification obligations

As with the OECS Model Bill, the Act does not include any personal data breach obligations. (See Section 3.A.1of this report.)

No requirements on data users when engaging data processors

As with the OECS Model Bill, the Act does not require data users to take any measures to ensure that data processors will assist them in complying with the Act. (See Section 3.A.1of this report.)

Data Privacy Impact Assessment (DPIA) apply narrowly

Section 12A of the Act sets out the requirement for performing a DPIA:

> *the Commissioner may require a department of government to prepare a privacy impact assessment if the initiatives covered by the privacy impact assessment are of a wide scope or use personal data of a nature that may require the protection of the personal data of an individual*.
>
> The DPIA is required to be submitted to the Commission for approval.

The requirement to conduct a DPIAs appears not to apply to non-governmental data controllers such as private companies and associations, whose processing could have a significant impact on data subjects. We recommend it cover all controllers (and processors too, if they bear obligations under the Act).

The conditions that require carrying out a DPIAs are vague, described as involving a "wide scope" or the use of personal data "of a nature that may require the protection of the personal data of an individual." This is tautologous, in that protection is merited for data of a nature requiring protection. This results in more uncertainty than is necessary. We recommend DPIAs be required for processing activities that significantly impact individuals' rights and freedoms, such as large-scale handling of sensitive data, automated decision-making, and systematic monitoring.

Additionally, mandating that the Commission approves all DPIAs could lead to unnecessary delays in processing activities and hinder efficient data management. It should suffice that the Commission reviews them and may intervene if concerned.

Cross-border transfers of personal data

No clear concept of adequacy or process for issuing adequacy decisions

Section 45 of the Act provides certain limited circumstances under which personal data can be transferred outside the country. These include when:

> *(a) the country or territory to which the personal data is being transferred has comparable safeguards to those in Saint Lucia for the protection of the rights and freedom of the data subject in relation to the processing of personal data; and*
>
> *(b) the Commissioner has authorized the data controller to transfer the personal data to the country or territory outside Saint Lucia.*

Additionally, the Act does not outline a formal process for the Commission to issue a decision, if it so wishes, that any given country does have comparable safeguards. These decisions can be helpful as they provide an official assessment confirming that a receiving country or region has a legal and regulatory framework offering data protection standards that are essentially equivalent to those of Saint Lucia. Such decisions can, if issued, help facilitate cross-border data transfers without the need for additional safeguards. We recommend authorizing the Commission to take such decisions, but not requiring such decisions before a controller relies on the comparability of a jurisdictions laws to Saint Lucia's Act.

Lack of tools and mechanisms supporting cross-border transfers of personal data

The Act does not establish mechanisms that would enable data controllers to transfer personal data across borders without relying solely on the Commission's adequacy decisions. Including alternative safeguards such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), certifications, and codes of conduct would facilitate cross-border data transfers when the laws of the receiving country do not offer protection comparable to Saint Lucia.

Institutions

Our internal research and contacts attempted by our local team members were not able to locate an online presence or physical establishment of the Information Commissioner.

Funding of the Commission

The assertion that the Commissioner should act independently in Section 10 is helpful, as is reference to funding the Commission by Parliamentary appropriations. It may be worth considering whether to permit the Commission to retain fines or receive grants, e.g., from development agencies.

Power to of the Commission obtain information

Under Section 41, the Commission may request and obtain access to an individual's personal data, upon request:

> *The Commissioner may, by notice in writing served on any person, request that person to furnish to him or her in writing in the time specified —*
>
> *(a) access to personal data;*
>
> *(b) information about and documentation of the processing of personal data;*
>
> *(c) information related to the security of processing of personal data; and*
>
> *(d) any other information in relation to matters specified in the notice as is necessary or expedient for the performance by the Commissioner of his or her functions and exercise of his or her powers and duties under this Act.*

It would be preferable to ensure that not only paragraph (d) but the whole section only authorizes the Commission to obtain such data as necessary or expedient in the performance of the Commissioner's

functions and exercise of powers and duties under the Act. This would reduce the risk of overstretching the exercise of the powers under (a), (b) and (c).

Overly broad registration requirements

Under Section 46, data controllers are required to register with the Commission and failure to do so results in a financial penalty.

> *(1) A person shall not act as a data controller, unless that person is registered as a data controller in accordance with section 47. (Substituted by Act 2 of 2015) (2) A person who, without reasonable excuse, acts as a data controller without being registered under this Act, commits an offence and is liable on summary conviction to a fine not exceeding $10,000. (Substituted by Act 2 of 2015)"*

The requirement for entities acting as data controllers to register with the Commission is highly disproportionate, is unworkable, and risks causing more harm than benefit. Given that almost every person that collects any personal data within the scope of the Act is a data controller, this would require a vast registration exercise for which there is no need. Administering and enforcing this obligation would waste resources amidst widespread non-compliance. Only a small number of particularly significant data controllers should be required to register. (See Section 2.G.5)

Enforcement

Overall, the Act provides several mechanisms through which data subjects can file a complaint to initiate the Commission's investigation, and, in turn, the Commission issue an enforcement notice when it has identified a violation of the Act. The decisions of the Commission are subject to appeal, which provides an additional accountability layer. In addition, the Act draws liability to senior leadership of legal entities, making them directly liable for offences. However, the penalties are unclear and disproportionate.

Disproportionate and unclear fines and penalties

As with the OECS Model Bill, Sections 16, 24, 27, and 44 of the Act impose criminal penalties for certain violations. We tend to recommend against criminalizing data protection law breaches. (See Sections 2.H.1 and 3.A.1of this report.)

4.G.2 Cybersecurity and cybercrimes

Introduction, scope of application and definition of key terms

The Computer Misuse Act (Cap 8.14) aims to combat cybercrime through computer systems and promote data integrity. The Act's primary objectives include preventing unauthorized access, modification, and misuse of computer systems. The Act prohibits knowingly causing a computer system to secure access to a program or data without lawful authority to do so and various other forms of unlawful access, interception and modification of computer systems and data (Sections 5 – 15). Additionally, it facilitates the collection of electronic evidence crucial for criminal investigations. To achieve these goals, the Act establishes rules and protocols for data handling and processing. It also enforces strict criminal penalties for specified offenses to deter malicious activities and promote responsible use of computer technologies.

Section 2 of the Act defines the term "data" as –

> *(a) information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose; and (b) representations of facts, information and concepts held in any removable storage medium;*

This broad definition does not differentiate between personal and non-personal data and so the Act's prohibitions and obligations apply to what are commonly referred to in data protection laws as "personal data."

Despite not explicitly defining the term "processing", Section 2 of the Act references numerous activities performed on computer systems that deal with data, including: "access, damage, function, intercept, modify."

Lawful basis for processing

The Act's various offenses related to the use, interception, modification, and access of data and computing systems emphasize the requirement of acting "without lawful authority," mirroring the data protection principle of lawful processing.

Broadly, these provisions aim to align data processing with established legal standards, reinforcing accountability and lawful conduct.

Obligations of the entity processing personal data

Although the Act does not provide affirmative general data processing obligations (only criminal prohibitions), it reflects some notions often included in data protection laws:

- Section 14: Protection of children's data: Section 14 imposes increased fines for offenses involving data pertaining to children, reflecting the higher level of sensitivity often accorded to such data in data protection frameworks.
- Section 21: Purpose limitation and data minimization: Sections 16 – 20 authorize the police and other authorized persons to obtain data for purposes of investigation and prosecution. Section 21 restricts the use of such data for specific purposes unless exceptions, such as court orders or matters of public interest, apply. This restriction aligns with the data protection principles of purpose limitation and data minimization, ensuring that data are utilized appropriately and only when necessary.
- Sections 3 and 19(h): Data integrity and quality: Sections 3 and 19(h) emphasize the importance of "data integrity" as a primary objective of the Act, reflecting the principle of data quality.

However, the Act does not include obligations to implement technical and operational security measures necessary to safeguard personal data involved in its processing activities, nor does it include provisions for data breach notifications in the event of a data breach or incident.

Data subject rights

The Act does not provide data subject rights, except as it would relate to non-compliance by police with required procedures and authorizations for obtaining data in the context of investigation or prosecution.

Cross-border transfers of personal data

The Act does not address cross-border processing of any data.

Institutions and penalties

The Act does not establish or designate any regulatory authority or institution responsible for overseeing compliance other than typical investigation and enforcement by police subject to judicial oversight.

The penalties stipulated in the Act include fines and imprisonment with application depending on the nature of the offence and whether or not it is the first or subsequent offence.

Conclusion

This Act broadly addresses two forms of personal data processing that would relate to typical data protection law. The first is to prohibit certain forms of data processing, particularly those that were performed without lawful authority or having other criminal aspects. The second is to affirmatively require certain procedures (e.g., judicial order) for police and other authorized persons to obtain data (which would include personal data) in the context of investigations and prosecution. In doing so, the Act establishes a framework for combating cybercrimes and incorporates some provisions that align with data protection principles. However, it does not include many typical data protection provisions, e.g., security standards and institutional structures, which are essential for effectively safeguarding personal data involved in the prohibited or authorized processing activities.

A generally applicable data protection framework that aligns with international good practices would address these gaps in providing the necessary supplementary measures to ensure robust protection of personal data.

4.G.3 Consumer protection

Introduction, scope of application and definition of key terms

The Consumer Protection Act (Cap 13.24) of the Laws of Saint Lucia is designed to promote and safeguard consumer rights concerning the supply of goods and the provision of services. The Act provides for the protection of consumers' life, health, and safety and establishes the Consumer Protection Board and the Consumer Protection Appeals Tribunal to oversee and enforce its provisions.

The Act requires agreements between suppliers and consumers to be fair, transparent, and free from misleading terms and conditions. However, it does not address the processing of personal data. Introducing a data protection framework aligned with international good practices would effectively complement this Act by providing additional safeguards for consumers' personal information.

Lawful basis of processing

Under Section 45(1)(a) of the Electronic Transactions Act, suppliers are required to disclose their full name and legal status to consumers. This obligation would amount to a lawful basis for processing such personal information in the context of typical data protection law.

Obligations of the entity processing personal data

Again, under section 45(1)(l) of the Electronic Transactions Act, suppliers are required to make available to consumers "the security procedure and privacy policy of the supplier in respect of the payment, payment information and personal information." This requirement is aligned with the data protection principles of accountability and transparency.

Data subject rights

Under Section 45(2) of the Electronic Transactions Act, suppliers are required to provide certain key individual rights to customers including: *"(a) to review the entire electronic transaction; (b) to correct any mistakes; and (c) to withdraw from the transaction before finally placing any order*". The ability to correct data would align with data protection principles but there is no data subject right beyond this.

Cross-border transfer of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

As set out in the subsection above titled "*introduction, scope of application and definition of key terms*", the entities established to not impact the processing of personal data in the context of consumer protection.

Conclusion

The law on consumer protection lacks most aspects of personal data protection. It would not contradict a generally applicable data protection law aligned with international good practices, and it would be appropriately supplemented by all of the provisions of such a law.

4.G.4 Freedom of information requests

There is currently no legislation in this area. A Freedom of Information Bill has been prepared but not yet enacted.

4.G.5 Health

Introduction and scope of application and definitions

The Health Practitioners Act of 2006, which was amended in 2018, provides for the registration and regulation of health practitioners in Saint Lucia. The Act also addresses the handling of patient and practitioner records, imposing obligations related to the retention, maintenance and sharing of medical records. It thus relates to processing of personal data that are often treated as particularly sensitive in data protection laws.

Sections 46(2), 100(7), 101(1) provide for Council authorities to register practitioners, issue certifications and remove practitioners. These processes entail processing of information, including personal data, including a practitioner's name, home and office address, as well as other information which, if combined, could identify an individual. Consequently, in most cases where the Act refers to "records," they inherently encompass personal data.

Lawful basis of processing

The Act provides a lawful basis for processing inasmuch as it obligates and/or authorizes (a) medical practitioners to furnish personal data (along with other necessary information) to register with their relevant Council (b) the Councils register them and process their personal data according to this Act, and (c) patients to provide personal data to medical practitioners in the context of receiving medical care.

The processing of personal data by Councils and medical practitioners during the act of medical professionals' registration and record creation of patients is carried out largely based on the lawful basis of fulfillment of legal obligations. Subsequent processing activities carried out by the Councils are performed largely as part of their official duties under the Act.

Obligations of the entity processing personal data

The obligations imposed by the Act on Councils and practitioners in the processing of records embody several fundamental principles of personal data processing:

- Section 122: Patient Records: Section 122 obligates health practitioners to maintain accurate patient records, including personal data such as names, medical histories, and treatment details, for a minimum of seven (7) years following the last entry. This retention period aligns with the principle of storage limitation in data processing, ensuring that personal data is not retained indefinitely without justification.
- Sections 19 and 120: Confidentiality Obligations: Under Sections 19 and 120, members of the Council – who are tasked with processing applications from medical and dental practitioners – must respect confidentiality. They are prohibited from disclosing any information related to matters before the Council except as required for the proper performance of their duties. This obligation generally reflects the principle of privacy in personal data processing.
- Section 100(9): Public Access to Registers: Section 100 provides for the Council to keep a register of practitioners. Section 100(7)(a) requires this to include the practitioner's personal and business addresses. Section 100(9) stipulates that the register of practitioners maintained by the Council must be open to public inspection at all reasonable times. This measure promotes the principle of transparency by enabling the public to verify practitioners' credentials. Section 100(11) aligns with data protection principle of privacy by providing that the practitioner's private address shall not appear in the register for public inspection.

Data subject rights

The Act does not explicitly provide for data subjects' rights to access, rectify, or erase their personal data. Section 100(9) grants the public (not only practitioners) the right to access data about practitioners upon

payment of a nominal fee. Additionally, Section 100(10) obligates the Council to periodically update and amend records to ensure their accuracy and currency.

Cross-border transfers of personal data

Section 9 of the Act authorizes the Medical and Dental Council to share information with international registration authorities. However, it does not set out safeguards or conditions governing such transfers.

Globally, medical professional registries collaborate extensively to uphold professional standards, facilitate the mobility of practitioners, and enhance public safety. Organizations such as the World Federation for Medical Education (WFME) and the International Association of Medical Regulatory Authorities (IAMRA) establish standardized protocols and data-sharing agreements that govern the secure and ethical exchange of personal data between registries. These collaborations typically adhere to stringent data protection principles, including data minimization, purpose limitation, and the implementation of robust safeguards like encryption and access controls.

While these practices should bolster the protection of personal data being shared abroad by the Council, the Act does not establish any obligation to ensure that appropriate protections are indeed established and respected. A generally applicable data protection framework would aim to ensure that personal data is handled securely and in compliance with international standards during cross-border exchanges.

Institutions and penalties

The Act establishes the institutions of Medical and Dental Council and the Allied Health Council, which, as explained above, have the obligation of maintaining the confidentiality of information contained in the records.

The Act also establishes several offences. These include offences for making false or misleading statements in the regulatory processes and forging and changing information in certificates of registration, practicing certificates and practitioner licenses (Section 115). These generally promote the quality, accuracy and integrity of data contained within certificates and licenses, thereby providing some additional safeguards for personal data processed under the Act.

Conclusion

The Health Practitioners Act deals with the obligations for managing personal data (largely those of medical practitioners) in the health sector, focusing on record maintenance and limited data sharing for professional purposes. It has provisions that support some aspects of data protection, but various gaps. The Act does not contain any provisions that would conflict with or impose barriers in the implementation of a generally applicable data protection framework which would be aligned with international good practices.

4.G.6 Education

Introduction, scope of application and key definitions

The Education Act Cap 18.01 of the Laws of Saint Lucia governs the administration of education in public, private and assisted schools and focuses on student welfare, parental rights and school operations. The Act allows for the processing of personal data that is specifically required in the creation of student registers and personal records of the students (data subjects) and sets out rules on student data management.

The Act regulates the management and handling of students' personal information, including:

- Sections 22 and 31: Maintenance of Student Records: School principals are required to maintain comprehensive student records. These include students' names, their parents' addresses, and other information which, when combined, could identify the student. Additionally, Section 20(3) requires parents to report any medical conditions that affect their children in order to accurately document relevant health information.

- Section 41: Authority of School Attendance Counsellors: School attendance counsellors are authorized to question students and collect information such as names, ages, addresses, and other identifying details. This information is used to assess whether a child of compulsory school age is not attending school, thereby facilitating timely interventions.
- Section 45: Reporting Non-Attendance: School principals are obligated to report on the names of individuals who have not attended school as required in order to monitor attendance.
- Section 19(2): Students who have attained the age of 18 years are entitled to exercise all the rights and powers, to assume all the obligations, and to receive all the benefits under this Act with respect to them that their parents are otherwise entitled to exercise, assume, or receive on their behalf. To the extent that the processing of student data involves handling the personal data of children under the age of 18, Section 19(2) of the Act reflects the notion often included in data protection law that such data are provided by their parents and legal guardians. This approach aims to implement additional safeguards and protect this vulnerable group of individuals, aligning with international best practices.

Lawful basis for processing

The Act establishes several lawful bases for the processing of personal data.

- Sections 20, 22, 25, 31, and 38: As described in the previous section, the Act provides for processing of personal data about students and their parents by principals and student counselors for managing student records, monitoring attendance, and performing other administrative functions.
- Section 45: Consent for Examination of Records: Parental or individual consent is required for the examination of student records. This provision ensures that personal data is accessed and reviewed only with explicit approval.

Obligations of the entity processing personal data

The Act imposes obligations on schools and principals concerning the processing of personal data, reflecting key principles of data protection:

- Accurate Data Maintenance (Section 22(1)): Principals are required to keep and maintain accurate student records.
- Confidentiality and Restricted Access (Sections 22(6) and 22(11)): Principals must prevent the disclosure of student records to unauthorized individuals. Breaches of this obligation incur penalties.
- Exemption from Liability and Reporting Obligations (Section 22(7) and Section 45): Individuals who provide data in good faith and with due care are exempt from liability, encouraging responsible data handling. Additionally, principals are obligated to submit regular reports to regulatory authorities under Section 45.
- Privileged Use and Limited Third-Party Access (Section 22(6)): Information contained in student records, including personal data, is restricted for use by school and departmental officials only. The Act imposes limitations on third-party access without consent, which promotes confidentiality and integrity of personal data.

The Act does not contain a requirement for maintaining security of personal data, including in student reports.

Data subject rights

The Act provides several rights to the students as well as the parents regarding their personal data such as:

- Access to records: Parents of minors and students aged 18 years or older are entitled to examine and request certified copies of their student records, as stipulated in Section 22(5). This provision promotes transparency and allows individuals to stay informed about the information held about them.
- Rectification of records: Authorized individuals may request corrections to any inaccurate or incomplete records under Sections 22(8)-(10). If a request for rectification is denied or results in an unfavorable outcome, the Act provides an appeals process, allowing for further review mechanism.

Cross-border transfers of personal data

The Act does not address cross-border transfers of information, including personal data.

Institutions and penalties

The Act refers to the following institutions:

- Education Appeal Tribunal: This Tribunal primarily handles appeals related to disputes, including those concerning data rectification and privacy issues. This may strengthen accountability for responsible and lawful processing of personal data.
- Board of Management: This Board is responsible for submitting annual reports and managing school affairs in compliance with data-related obligations. These processes should support educational institutions' adherence to data protection principles reflected in the Act.

In addition, the Act imposes penalties for the unauthorized disclosure of student data. Under Section 22(11), such offenses attract a fine of up to $1,000, underscoring the Act's alignment with personal data protection principles.

Conclusion

The Act promotes transparency in the management of students' personal data by establishing rights for students and clearly defining institutional responsibilities related to data processing. However, it does not include provisions covering data retention periods, data security measures, or cross-border data transfers, which are essential components for comprehensive data protection. A generally applicable data protection framework, aligned with international good practices, would supplement this Act's provisions.

4.G.7 Financial services (including digital financial services)

Introduction, and scope of application

The Banking Act Cap 12.01 governs the regulation of banking business, the establishment of a unified banking space and related matters within Saint Lucia. It covers the processing of personal data inasmuch as it applies to depositor and customer information, their financial transactions and related information. It also covers the handling of personal information of financial institutions shareholders and officers occupying positions in financial institutions.

Although the Act does not establish a full data protection framework, it does provide for a duty of confidentiality and "secrecy of information".

Lawful basis for processing

Section 178(1) of the Act sets out the conditions under which personal data related to depositors or customers may be processed lawfully. They specify that individuals who have access to such data in their professional capacity must not disclose them unless one of the following legitimate bases is met:

- Consent: Disclosure may occur if the depositor, customer, or their authorized representatives provide written approval.
- Legal Obligation: Information may be shared when required by the Act itself or by a lawful order of a court with proper jurisdiction.
- Regulatory and International Agreements: Disclosure is permissible under relevant laws of Saint Lucia or agreements among Participating Governments (i.e., members of the ECCU), ensuring compliance with broader legal frameworks.
- Legitimate Business Interests: Certain exceptions allow for limited data sharing in response to legitimate business requests, such as providing a general credit rating, or when conducting due diligence in the context of potential acquisitions, so long as appropriate safeguards are in place.

Section 178(2) also allows limited disclosures for business needs, as described in the next section.

Obligations of the entity processing personal data

Licensed financial institutions have obligations under the Act to maintain the confidentiality of data. Section 178 prohibits unauthorized disclosure of customer information, which includes identity information and transactions. Disclosures are permitted if the customer gives written consent or where needed for legitimate business purposes such as credit ratings.

The Act does not provide an obligation for establishing and maintaining a certain level of security measures to safeguard financial information, including financial data. Nor does it address personal data breaches. Given the substantial amounts of financial information and sensitive personal data managed by financial institutions, it would be appropriate for such data to be subject to such data protection obligations.

Data subject rights

There Act makes no provisions for rights of data subjects in the Act.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Section 94 authorizes the Central Bank to establish agreements with foreign supervisory authorities and resolution agencies to collaborate and share information. This cooperation is essential for overseeing and managing financial institutions, including banks and financial holding companies, particularly in scenarios where these institutions fail or are at risk of failure. Such agreements may only be entered into if the Central Bank is assured that the foreign authority will maintain the confidentiality of all shared information. Although generally not focused on personal data, this provision underscores the Act's recognition of the necessity for international cooperation within the banking sector. It highlights the importance of reciprocal safeguards to ensure the confidentiality and integrity of data exchanged between jurisdictions.

Institutions and penalties

The Eastern Caribbean Central Bank formulates and implements monetary policy and regulates and supervises financial institutions in order to maintain the integrity of the financial system. The Central Bank manages the issuance and circulation of the national currency, oversees foreign exchange reserves, and ensures efficiency and security of payment and settlement systems.

Under the Act, the Central Bank has the power to impose several penalties for violations related to financial matters. Section 96 provides that any licensed financial institution that knowingly supplies false or

misleading statements, returns, information, or data in any material is subject to a penalty of $25,000. This is aligned with typical data protection obligations to maintain the accuracy of personal data.

Conclusion

The Banking Act Cap 12.01 establishes a foundational framework for maintaining confidentiality in banking operations. However, it does not address several critical areas necessary for the comprehensive protection of personal data within financial services. The Act lacks provisions for data security measures, the rights of data subjects, and the regulation of cross-border personal data transfers. The Act would not conflict with, but would rather be supplemented by, a generally applicable data protection framework aligned with international good practices.

4.G.8 National identification (including digital and functional forms)

Introduction, scope of application and key definitions

The Elections Act Cap 1.02 governs the registration of electors and the conduct of elections in Saint Lucia. Part 2 of the Act, specifically Sections 9-12, includes provisions for the issuance of National Identification Cards. ID cards serve as official proof of an individual's identity not only for electoral purposes but also for broader identification across various sectors of the economy.

As shown in Form 6 in the Schedule to Sections 94-95 of the Act, the issuance of ID cards requires the provision of substantial amounts of personal data. This includes a person's name, address, sex, date of birth, nationality, social security number, height, and potentially other identifying characteristics.

Lawful basis for processing

The Chief Elections Officer is responsible for issuing ID cards. Individuals provide such personal data for the purpose of registering as electors and obtaining ID cards under Form 7 in the Schedule to Sections 94-95 of the Act, providing a lawful basis for the processing of their data to enable the effective administration and integrity of the electoral process and voting by only eligible citizens.

The processing of the personal data for the issuance of ID cards is performed in compliance with this Act.

Obligations of the entity processing personal data

The Act imposes certain obligations regarding personal data, especially in the context of processing data for the issuance of ID cards:

- Under Section 94-95 of the Elections Regulations, enumerators are required to keep registration and identification record cards in a safe place and restrict access to unauthorized persons.
- Under the same regulation, registration and identification cards need to be stored in containers provided by the Chief Registration officer and kept at police stations when overnight storage is necessary. The provisions relate to the physical storage of records and do not include typical data processing obligations.
- Section 94 of the Elections Identification Cards Regulations requires that "*an identification card shall carry specific security measures established within the system and on the card to prevent unauthorized use or production of the card.*"

Except for the security measures mandated by Regulation Section 94, the Act does not require the implementation of any security protocols. Furthermore, the Act does not establish any obligations to notify individuals in the event of a data breach affecting the database that stores personal information related to ID cards.

Data subject rights

There are no provisions in the Act relating to the rights of the data subject whose personal data are being processed for electoral registration and the issuance of ID cards.

Cross-border transfers of personal data

The Act does not mention cross-border transfers.

Institution and Penalties

The Act makes no mention of an institution appointed to oversee data protection, nor are there any penalties listed for breach of confidentiality.

Conclusion

The Elections Act includes some provisions for the physical protection of personal data related to the electoral process but lacks an overall framework for data protection of personal data. It does not include explicit requirements for confidentiality and integrity of personal data processed in the context of ID cards. The Act also lacks provisions on data subject rights, institutional structures and requirements for confidentiality, security and integrity of personal data. This Act would not conflict with any provisions of a new generally applicable data protection framework aligned with the international good practices, and such a framework would provide protections absent in the Act.

4.G.9 Passports

Introduction and scope of application

The Passport Act Cap. 10.03 establishes the guidelines for issuing passports and managing related activities in Saint Lucia. According to the Passport (Application Form) Regulations, applicants must provide various personal details, including their full name, marital status, country and date of birth, physical characteristics, email address, phone number, and a recent photograph. Additionally, married women are required to include information about their spouse or former spouse. This collected data encompasses sensitive personal information, which is essential for the accurate processing and verification of passport applications.

Lawful basis for processing

The Act's provision for collection and other processing of citizens' personal data for the purpose of issuing passports provides a lawful basis for such processing.

Obligation of the entity processing personal data

The Act does not explicitly impose on the Ministry any obligations of confidentiality, secrecy, and security when processing personal data. However, Section 5 establishes an offence that echoes the principle of accuracy by penalizing any actions that undermine the proper management and quality of information contained within passports:

> (*1) A person shall not— (a) make any false statement for the purpose of obtaining a passport; (b) make any statement on an application for a passport which he or she knows to be false; (c) intentionally deface, damage or destroy any passport; (d) forge any passport; (e) unlawfully produce any passport; (f) sell forged passports; or (g) conspire with another person to do any of the acts listed in paragraphs (a) - (f)*

Other than this, the Act is silent on the topic of security over the personal data involved in the process of issuance of passports.

Data subject rights

The Act does not provide rights to data subjects relating to their personal data.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Penalties and institutions

The Act designates the Ministry of Home Affairs as the responsible authority for issuing passports. However, it does not establish any institutions or departments within the Ministry tasked with overseeing the protection and security of personal data involved in the issuance of passports.

The Act promotes the integrity of data by establishing offence outlined above, under the section on "*Obligation of the entity processing personal data*".

Conclusion

Although the Act involves the processing of substantial volumes of personal data, including sensitive information, it does not provide adequate measures to ensure its security and protection. To address these shortcomings, the Act would benefit from the implementation of additional safeguarding and security protocols. Furthermore, it should be complemented by a comprehensive data protection framework to enhance the security and integrity of the personal data involved.

4.G.10 Civil registration

Introduction, scope of application and definition of key terms

The Civil Status Act Cap 4.02 governs the maintenance and management of civil status records which consists of data related to births, deaths, marriages and adoptions. The Act provides the framework for recording, maintaining and managing civil status records in Saint Lucia. These records are formal and legally recognized documents. The process of registration and rectification of civil status records covered by the Act is performed by the Registrars, assistant registrars, and civil status assistants and includes the processing of personal data.

For instance, Section 6A requires that for the registration of a child's birth, the following personal data are required:

> *(a) the Register — (i) the district, (ii) the year, (iii) the page number, (iv) the number of the register;*
>
> *(b) the person, his or her — (i) birth registration number, (ii) date and place of birth, (iii) the name, (iv) the sex, (v) where applicable, whether the person was stillborn;*
>
> *(c) the parents of the person — (i) the name, surname and dwelling place of the father, (ii) the occupation of the father, (iii) the name, surname and dwelling place of the mother, (iv) the occupation of the mother, (v) the age;*
>
> *(d) the full name of the informant, his or her signature, occupation and dwelling place;*
>
> *(e) registration — (i) the date when the person was registered, (ii) the signature of the Registrar, (iii) the signature of the District Registrar, (iv) the name, if added after registration of birth and date when added; and (f) remarks*.

The Act requires the provision, recording, and disclosure of specific personal data related to births, deaths, and marriages, which qualifies as "processing" under typical data protection laws.

Lawful basis for processing

Personal data provided by individuals or their parents are processed by the Registrars and other parties under the authority of the Act in order to register life events such as births, adoptions, marriages, deaths, burials, and baptisms with the Registrar of Civil Status. This legal requirement is evident in the Act's language, which mandates that the birth of a child "*shall be registered*" (Section 8), requires civil status officers and ministers "*to register marriages celebrated by them as a record of civil status in accordance with the Civil Code*" (Section 18), and imposes "*a duty*" to provide information about a person's death to

the Registrar (Section 19). Subsequently, the Registrar and relevant officials process this personal data in accordance with the statutory mandate of the Act and subsequent regulations to maintain accurate and official records of civil status.

Obligations of an entity to process personal data

The Act does not establish clear obligations for confidentiality, integrity, secrecy, or security. Additionally, it lacks procedures for notification and response in the event of data breaches.

Data subject rights

Under Section 25, the Act provides data subjects with the right to rectify their personal data:

> (1) *The Registrar may, at his or her instance or at the instance of an interested party, rectify incorrect or incomplete records of civil status.*
>
> *(2) The Registrar may delegate his or her functions pursuant to this section to one or more Assistant Registrars or Adjudicators appointed by the Judicial and Legal Service Commission*.

Other errors such as date of birth, sex and other details may also be rectified under section 25(A). Data subjects may also apply to have their names inserted on birth certificated if it is missing or incomplete, but this is subject to verification with baptism or other pertinent records under section 25(b).

Cross- border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and Penalties

The Registrar of Civil Status is the primary authority responsible for maintaining and rectifying civil status records.

Conclusion

The Act provides several provisions governing the collection, administration, and management of civil status records, and contains processes that promote their accuracy. However, it offers limited safeguards and protections for personal data. The absence of data subject rights, obligations for data security, safeguards against breaches, and adequate penalties poses significant risks to individuals' personal information. Addressing these gaps by implementing additional clauses would ensure the Act's compliance with international data protection standards.

Introducing a comprehensive data protection law that does not exclude the processing activities under this Act would enhance the overall protection of personal data within the civil registration process. Importantly, the Act does not contain any provisions that would contradict or be inconsistent with a generally applicable data protection law.

4.G.11 Electronic communications

Introduction, scope of application and definition of key terms

The Telecommunications Act, Cap 8.11 governs the telecommunications sector in Saint Lucia, with subsidiary legislation outlining the administrative, technical, and procedural rules for its operation. Additionally, Saint Lucia is a signatory to the Treaty establishing the Eastern Caribbean Telecommunications Authority, a regional agreement designed to foster competition in the telecommunications sector and harmonize policies across the region.

The Act addresses the processing of personal data by authorizing the relevant authority, the Telecommunications Commission, to collect and process personal information—such as names, business addresses, email addresses, and phone numbers—primarily in relation to the licensing process for telecommunications network and service operators. Additionally, the Act states that operators themselves receive and process subscriber personal information as part of their service delivery.

Lawful basis for processing

Applicants provide their representatives' personal information as part of the application process to obtain, modify, or renew a license to operate telecommunications networks or services, as required by Schedule 3 of the Act. Subsequently, the Commission processes the personal information pursuant to the provisions of this Act.

Operators, in turn, process subscribers' personal data as part of their contractual obligations to deliver telecommunications services. Additionally, subscriber consent is required for certain processing activities, such as listing their personal information in a phone directory (Section 19). Furthermore, as outlined in Sections 18 and 61, subscriber data may be disclosed under a court order, allowing processing based on the lawful basis of compliance with a legal obligation.

Obligations of the entity to process personal data

The Act, along with the Telecommunications (Confidentiality in Network and Services) Regulations (Section 73) and the Telecommunications (Private Network Licensing) Regulations (Section 7), outlines key obligations for the protection of personal data.

Section 8 of the Act imposes a general confidentiality requirement on operators, prohibiting them from knowingly disclosing or allowing access to any confidential, proprietary, or competitive information received from another public network operator in relation to interconnection, unless expressly authorized by the operator in writing, or by the Act or these Regulations.

Additionally, Section 61 allows for the disclosure of certain information under specific conditions, as outlined in the Act.

Under Section 8 of the Private Network Licensing Regulations, licensees are obligated to take all reasonable measures to ensure the security of information. This includes safeguarding information acquired during the conveyance of communications and ensuring the privacy and confidentiality of communications related to the private telecommunications network.

Part 4 of the Confidentiality in network and services regulations requiring aiming to safeguard subscribers' information:

- Telecommunications providers must implement policies to tightly control access to subscriber personal and network information by employees or officers.
- Employees with access to subscriber data must sign a non-disclosure agreement, which remains in effect even if the employee changes duties or leaves the company.
- Confidentiality of Subscriber Information: Subscriber personal and network information is confidential and cannot be disclosed without the subscriber's consent or a court order.
- A telecommunications provider must obtain subscriber consent before listing their personal information in a directory.
- A provider may disclose subscriber network information only to prevent fraud, abuse, or unlawful use, or to provide the subscribed services.

Data subject rights

The Act does not provide rights of data subjects over their data.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The National Telecommunications Regulatory Commission is the primary authority responsible for the development of the telecommunication and broadcasting services and radio communications of Saint Lucia.

Among its other duties, it is responsible for receiving and reviewing applications for licenses (which include personal data), investigate and resolve disputes relating to interconnections or sharing of infrastructure between telecommunications providers and initiate legal proceedings against a licensee or authorized frequency holder for the purposes of compliance.

Regarding penalties related to personal data Section 61of the Act provides that any individual who knowingly discloses personal data in violation of the Act commits an offence. Upon conviction, the individual is liable to a fine of up to $15,000 or imprisonment for a term not exceeding two years.

Conclusion

Although the Act requires personal data to be treated with confidentiality, it does not provide adequate measures to ensure its security and protection. To address these shortcomings, the Act would benefit from the implementation of additional safeguarding and security protocols. Furthermore, it should be complemented by a comprehensive data protection framework to enhance the security and integrity of the personal data involved.

4.G.12 Electronic transactions

Introduction, scope of application and definition of key terms

The Electronic Transactions Act Cap 8.17 governs electronic transactions, electronic communications, electronic signatures, documents and other transactions which involve the processing of personal data. In this Act, the term "transaction" is not used in its literal, commercial sense, which includes payments and economic transactions. Rather, it is defined as "*(a) a transaction of a non-commercial nature; (b) a single communication; and (c) the outcome of multiple related communications*".

This Act regulates personal data in the context of electronic communications between two persons, designated as "the originator" and "the addressee". As defined in Section 2:

- "*originator*" in relation to an electronic communication, means a person by whom, or on whose behalf, the communication purports to have been sent or generated prior to storage, but does not include a person acting as an intermediary with respect to that communication; and
- "*addressee*" in relation to an electronic communication, means a person who is intended by the originator to receive the electronic communication, but does not include a person acting as an intermediary with respect to that electronic communication.

Electronic communications between an originator and addressee will often include the following personal data: their names, email addresses, metadata such as the time and location of an email, identifiers included in a signature (phone numbers, physical addresses, and other contact details may be shared directly within the email content), along with any information revealed in the context of their communication.

According to the definition of "electronic communications", which cover information being "*generated, communicated, processed, sent, received, recorded, stored, or displayed by electronic means*", personal data undergo "*processing*" as they are transferred by the originator and subsequently received and stored by the addressee.

However, the Act does not impose any obligations on the originator, addressee or the carrier of electronic communications regarding the protection, maintenance of integrity, or safety of personal data. Additionally, there are no provisions concerning data subject rights, cross-border data transfers, or relevant institutions authorized to oversee electronic communications. As a result, electronic transactions would benefit from a comprehensive data protection framework that imposes obligations, rights, and responsibilities regarding the processing of personal data on both originators and addressees.

Lawful basis for processing

Personal data involved in electronic transactions, as defined under the Act, are processed under several lawful bases:

- Under Sections 21, 22, and 29, consent is generally required for the use of electronic communications and signatures. Section 11 addresses the attribution of electronic communications, stipulating that such communications must be sent under authority unless otherwise agreed. Section 30 establishes the legal requirement to provide access to information that exists in paper or any other non-electronic form.
- Under Section 14 of the Act, consent needs to be in place for information to be both provided and accepted in an electronic form: "*(1) This Part does not require a person to use, provide, or accept information in an electronic form without that person's consent. (2) For the purposes of this Part and subject to subsection (3)— (a) a person may consent to use, provide, or accept information in an electronic form subject to conditions regarding the form of the information or the means by which the information is produced, sent, received, processed, stored, or displayed; (b) consent may be inferred from a person's conduct. (3) The consent of a public body to accept information in electronic form may not be inferred from the conduct of the public body but must be expressed by communication accessible to the public or to those most likely to communicate with the public body for the particular purpose to which the information relates. (4) This Part does not authorize a public body to require any person to give, provide or accept information in electronic form without consent.*
- Subsequently, the personal data provided and received pursuant to the lawful basis of consent, can be processed based on compliance with a legal obligation under an Act, or due to the necessity of performing a public task, especially in cases where such data is provided to a public body.
- Under Sections 38-39, the processing of personal data involved in the formation and enforcement of an electronic contract is performed under the lawful basis of contractual necessity. In the context of automated contracts, personal data is required to fulfill the terms and obligations outlined in the contract, such as providing services, delivering goods, or managing transactions.

Data subject rights

The Act provides limited rights of data subjects over their data.

Section 42 provides for the right to correct errors in automated transactions and provides that that "*a transaction has no legal effect if material errors are made by the individual, if the automated system does not provide the opportunity to correct the error or if the individual promptly notifies the other person."*

Obligation of an entity to process personal data

The Act provides several obligations that reflect data protection principles.

Section 15 the Act provides a brief echo of principles of personal data protection in the requirement for maintaining "*integrity*" in relation to electronic signatures:

[T]he integrity of information is maintained only if the information has remained complete and unaltered, other than the addition of any endorsement, or any immaterial change, that arises in the normal course of communication, storage, or display.

Under Section 45, Part 5 on consumer protection requires suppliers to provide information to consumers regarding their security procedures and privacy policy, regarding the payment, payment information and personal information. This is a significant data protection disclosure requirement. It is general enough that it will not contradict provisions in a typical data protection law requiring disclosure to data subjects of the purpose of collection of personal data and how it will be handled.

Cross-Border Transfers

The Act does not restrict cross-border data transfers. Under Section 34, the Act provides for the recognition of foreign electronic signatures, but does not control whether, how or where personal data may or may not be transferred abroad.

Institution and Penalties

The Act makes no provision in relation to established institutions to oversee compliance nor does it mention penalties associated with non-compliance or misuse of electronic communication and personal data. The Act does not establish or authorize an entity responsible for overseeing and implementing its provisions related to electronic communications.

Conclusion

While the Electronic Transactions Act provides a framework for regulating electronic communications and ensuring the validity of electronic documents and signatures, it addresses inadequately several aspects pertaining to data protection. The Act would not conflict with a data protection framework aligned with international good practices. It would be supplemented from its provisions especially as it pertains to security safeguards and cross-border data transfers. It would also ensure that both originators and addresses are held accountable for the responsible processing of personal data.

4.G.13 E-signatures

Introduction and scope of application and key terms

E-signatures are governed by Part 3 of Chapter 8.17 of the Electronic Transactions Act.

Under Section 2 of the Act, "*electronic signature*" is defined as:

> *(a) information that is— (i) contained in, attached to or logically associated with, an electronic document, and (ii) used by a signatory to indicate his or her adoption of the content of that document; (b) does not include any signature produced by a facsimile machine or by an electronic scanning device.*

Also, the Act defines *"encrypted signature***"** as a "*means an electronic signature that is encrypted by means of a private key or other encrypted signature creation device*".

An individual using electronic signatures is a "*signatory*" and is defined as:

> *a person who by means of an encrypted signature creation device has, whether acting himself or herself or through another person, or an automated communications device, acting on his or her behalf, affixed his or her encrypted signature to an electronic document.*

The use of electronic signatures would typically constitute processing of personal data under a data protection law.

Lawful basis for processing

As explained in the analysis on electronic transactions, Section 14 of the Act provides that parties need to consent for information (here, an electronic signature) provided and accepted in an electronic form to be valid. Typically, consent to use the electronic signature would be a lawful basis for processing such personal data. Additionally, where used to enter into or perform contractual obligations, this would also be a lawful basis of processing the personal data embedded within these signatures (e.g., name, email address, unique identifiers).

Data subject rights

The Act does not mention data subject's rights in relation to right to access, correction or erasure their personal data provided in the context of e-signatures.

Obligation of entity to process personal data

The Act echoes the data protection principle of "integrity" of personal data inasmuch as the validity of an electronic signature is conditional upon the integrity of the information to which it relates being maintained, i.e., that the information has not been altered (Section 15 and Sections 21-23). However, this does not amount to an affirmative obligation to maintain the integrity of the information.

In addition, Section 35 of the Act provides that public bodies receiving information in electronic form specify "*control processes and procedures to ensure integrity, security and confidentiality of the information*".

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutional and Penalties

The Act does not mention any established institution or body responsible for enforcement nor does it mention penalties associated with non-compliance.

Conclusion

The Electronic Transactions Act, as it pertains to governing electronic transactions, lacks several key requirements covering processing of personal data. This framework would not conflict but would benefit from a generally applicable data protection framework developed in alignment with international good practices.

4.H Saint Vincent and the Grenadines

4.H.1 Data protection

Overview

Saint Vincent and the Grenadine's legal framework on the protection of personal data is governed by Act No. 18 of 2003 ("Act"), officially cited as the Privacy Act of 2003. The Act states that it aims to "*promote and protect the privacy of individuals, and for connected matters*." As of now, the Act has not entered into force, which will occur upon publication of an order of the Minister in the *Gazette*.

The Act dates from 22 years ago, pre-GDPR and pre-OECS Model Bill. Naturally, then, it does not reflect international good practice that has developed extensively since that time. (It is, though, impressive that the country adopted a privacy law back in 2003.) We describe the gaps between the Act and current international good practice in this section. They are so extensive that we do not consider it useful to suggest amendments to the Act but rather that it be repealed and replaced by a new Act.

Scope of applicability

As explained below, the Act only applies to public sector entities and does not cover automated processing of personal data. Its scope would require a revision to align with international good practices.

Application of the Act limited to public authorities

The Act only creates obligations for "public authorities," which are defined in Section 4 to include:

> *(a) Parliament or any committee of Parliament; (b) the Cabinet as constituted under the Constitution; (c) a Ministry, a department or division of a Ministry; (d) a local authority; (e) a public statutory corporation or body; (f) a body corporate or an incorporated body established for a public purpose, which is owned or controlled by the State; (g) an embassy, consulate or mission of the State or any office of the State situated outside of Saint Vincent and the Grenadines whose functions include the provision of diplomatic or consular services for or on behalf of Saint Vincent*

and the Grenadines; (h) any other body designated by the Minister by regulation made under this Act, to be a public authority for the purposes of this Act."

This leaves unaddressed processing of personal data by private sector entities, non-governmental organizations, associations, individuals and any others, all of which play a major role in personal data processing activities.

Aligning the Act with international good practice would require introducing a number of provisions on scope. These would ensure it is not restricted to the public sector and would include territorial connections. They would also include exemptions for national security, journalistic, artistic and other related purposes. (See Section 2.B.)

General elements of a data protection law

Outdated conceptual and definitional framework

The Act does not use concepts and terminology that are widely used today. We set out some examples below.

- ***Processing:*** The Act does not use consistent terminology when referring to processing activities involving personal data. In several sections, the Act describes these activities as "collection, use, disclosure, and retention." Additionally, it frequently references the "storage" of personal data. This inconsistency results in certain principles and responsibilities being assigned to specific data processing activities while excluding others. Moreover, several crucial activities related to personal data are entirely omitted, including data sharing, data transfer, recording, organization, adaptation or alteration, retrieval, consultation, use, dissemination or making available, alignment or combination, blocking, erasure, and destruction.
- ***Controllers and processors:*** The Act does not delineate the notions of controller or processor, which are particularly useful in allocating responsibilities commensurate with their roles in determining the purpose and manner of processing (controller) or simply acting as an outsourcing provider of a processing service to a controller (processor).
- ***Sensitive personal data:*** The Act does not provide for heightened protections of data that may be particularly sensitive and affect data subjects more than other personal data.

Principles governing the processing of personal data

The Act does not provide clear bases for processing personal data, nor does it contain a set of principles that create obligations for processing of personal data.

Lack of lawful bases processing of personal data

Although the Act references the term "*lawfulness*," it does not establish a framework of lawful bases for processing personal data. Instead, it merely mandates that personal data be collected for lawful purposes and prohibits processing through unlawful means, as specified in Section 7, "collection of information for a lawful purpose," and the prohibition of collecting personal information by "unlawful means."

Section 11 introduces a concept similar to lawful processing of personal data. However, the bases for processing are limited exclusively to disclosures by public authorities, thereby excluding other types of processing activities and those conducted by private sector entities. Specifically, Section 11 states:

(1) Subject to section 12, where a public authority holds personal information, it shall not disclose the information to a person, body or agency (other than the individual concerned), unless—

(a) the individual concerned has expressly or impliedly consented to the disclosure;

(b) the disclosure of the information is required or authorised by or under law;

(c) the disclosure of the information is one of the purposes in connection with which the information was collected, or is directly connected to that purpose;

(d) the individual concerned is reasonably likely to have been aware or made aware under section 8(2)(c) that information of that kind is usually passed on to that person, body or agency;

(e) the information is to be disclosed— (i) in a form in which the individual concerned is not identified, or (ii) for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(f) the authority believes on reasonable grounds that disclosure of the information is necessary— (i) to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person, or to public health or safety, (ii) for the prevention, detection, investigation, prosecution or punishment of any offence or breach of law, (iii) the enforcement of a law imposing a pecuniary or custodial penalty or both, (iv) the protection of public revenue, (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal, or (vi) in the interests of national security."

Additionally, the Act omits a clear reference to the term "consent," which is typically a fundamental basis ensuring that individuals maintain control over how their personal data are processed. The reliance on consent is controversial internationally, making it important to define what constitutes valid consent within the Act. The Act would also appropriately address consent by children and others lacking legal capacity.

See generally Sections 2.C.1 and 2.C.2 of this report.

Lack of principles of data protection

Sections 7-14 of the Act refer to certain concepts that reflect some notions of data protection principles. These include references to the concept that personal data accuracy (Section 9), purpose limitation (Section 8) and data security (Section 13). However, each of these principles only relates to specific activities. For example, the obligation of security is associated with the action of "storage", and the requirement for "accuracy" is only required "before use". Furthermore, several crucial principles, such as fairness and transparent processing, and accountability and data minimization are not included. Alignment with international good practice would involve setting out a full set of principles. (See Section 2.C of this report.)

Individual rights concerning personal data

Section 15 provides a right of an individual to request the correction of their personal data:

"*Where a document of a public authority to which access has been given under any enactment, contains personal information of a person and that person claims that the information—*

(a) is incomplete, incorrect or misleading; or

(b) not relevant to the purpose for which the document is held,

the public authority may, subject to subsection (2), on the application of that person, amend the information upon being satisfied of the claim."

The Act does not include other data subject rights which would be aligned with international good practices, such as the right to access and obtain copies of personal data, the right to object to data processing in specific circumstances, the right to request erasure of data, subject to conditions and exceptions, and the right to withdraw consent under certain conditions. (See Section 2.D of this report.)

Data security

Lack of adequate requirements for data security

The Act does not specify various aspects of data security obligations that have become widely used in data protection legislation. Section 13 provides:

"Where a public authority holds personal information, it shall ensure that—

(a) the information is protected, by such security safeguards as is reasonable in the circumstances to take, against loss, unauthorised access, use, modification or disclosure, and against other misuse; and

(b) where it is necessary for the information to be given to a person, body or agency in connection with the provisions of a service to the authority, everything reasonably within the power of the authority is done to prevent unauthorised use or disclosure of the information"

Alignment with international practice would refer to technical and organizational measures and provide examples of what processes could be used. (See Section 2.E.1 of this report.)

Lack of personal data breach notification obligations

The Act does not include any personal data breach obligations. (See Section 2.E.2 of this report.)

Cross-border transfers of personal data

Addressing cross-border transfers of personal data

The Act does not address cross-border transfers of personal data, which are an important part of international good practice today. (See Section 2.F of this report.)

Institutions

Sections 16-38 of the Act provide rules on the establishment and powers of the Information Commissioner ("Commissioner"). As mentioned above, the Commissioner has the power to receive complaints and conduct investigations when there is an alleged violation of the Act. Also, the Commissioner lacks the necessary institutional independence to enforce the Act impartially. As the Act has not yet been proclaimed, a Commissioner has not been appointed.

Enforcement

Although the Act outlines a process of seeking remedies in the event of an alleged violation, it does not grant the Commissioner the authority to impose penalties for breaches of its provisions, perhaps because it only applies to processing by public authorities. Alignment with international good practice would include the power to issue penalties for noncompliance. (See Section **Error! Reference source not found.** of this r eport.)

4.H.2 Cybersecurity and cybercrimes

Introduction, scope of application and key terms

The Cybercrime Act of 2016 establishes offences related to cybercrimes and other related matters. The Act prohibits knowingly causing a computer system to secure access to a program or data without lawful authority to do so and various other forms of unlawful access, interception and modification of computer systems and data (Sections 3 – 21). Additionally, it facilitates the collection of electronic evidence crucial for criminal investigations (22-39). To achieve these goals, the Act establishes rules and protocols for data handling and processing. It also enforces strict criminal penalties for specified offenses to deter malicious activities and promote responsible use of computer technologies.

Section 2 of the Act defines the term "computer data" as "facts, concepts, information including text, sound, image or video, or machine-readable code or instructions, that is in a form suitable for processing in a computer system and is capable of being sent, received or stored and includes a program that can cause a computer system to perform a function. "

This broad definition does not differentiate between personal and non-personal data and therefore, the Act's prohibitions and obligations apply to what are commonly referred to in data protection laws as "personal data."

Despite not explicitly defining the term "processing", Section 2 of the Act references numerous activities performed on computer systems that deal with data, including: "access, damage, function, intercept, modify." To the extent that these activities involve personal data, they constitute various forms of personal data processing.

Lawful basis for processing

The Act establishes various instances of lawful basis for processing personal data: This includes compliance with written laws or judicial orders under Section 21, as well as access granted on the basis of an affidavit under Section 35. Furthermore, Section 27 permits the disclosure of data obtained during investigations, provided it aligns with any written law or is carried out in compliance with a judge's order. Disclosure is justified when the data is required for purposes such as preventing, detecting, or investigating offences, apprehending or prosecuting offenders, preventing injury or harm to a person's health, preventing significant loss or damage to property, or when it serves the public interest. Additionally, the Act's various offences (Sections 3-21) related to unauthorized use, interception, modification, and access to data or computing systems reinforce the principle of lawful processing. The reference to actions taken "without lawful excuse or justification" and the requirement for authorization echo fundamental data protection principles, ensuring that data handling activities remain legitimate and legally compliant under specific circumstances.

Obligations of the entity processing personal data

Although the Act does not provide affirmative general data processing obligations (only criminal prohibitions), it reflects some notions often included in data protection laws:

- Section 14 imposes increased fines for offenses involving data pertaining to children, reflecting the higher level of sensitivity often accorded to such data in data protection frameworks.
- Section 27 requires that disclosure of data obtained in the context of investigatory efforts shall be processed pursuant to specific purposes. These purposes provide limits to the way that personal data shall be processed and echo the principles of purpose limitation.
- Section 28 states that if a judge's order authorizes a police officer to seize and preserve a computer for a specified period under conditions of confidentiality, any breach of this confidentiality requirement will result in penalties. This provision echoes the principle of confidentiality.

Data subject rights

The Act does not address data subject rights.

Cross border transfers

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act imposes the following penalties: illegal interference with data carries on summary conviction fines of up to $100,000 and or imprisonment for up to 2 years or both, illegal acquisition of data on summary conviction carries a fine of up to $100,000 and or imprisonment for up to 2 years, identity related crimes carries a fine of up to $250,000 and or imprisonment for up to 5 years, misuse of data obtained carries a fine up to $100,000 or imprisonment for up to 2 years.

Conclusion

This Act broadly addresses two forms of processing that would relate to the typical data protection law. The first is to prohibit certain forms of data processing, particularly those that were performed without lawful authority or having other criminal aspects. The second is to affirmatively require certain procedures (e.g., judicial order) for police and other authorized persons to obtain data (which would include personal data) in the context of investigations and prosecution. In doing so, the Act establishes a framework for combating cybercrimes and incorporates some sparce provisions that align with data protection principles. However, it does not include many typical data protection provisions, e.g., security standards and institutional structures, which are essential for effectively safeguarding personal data involved in the prohibited or authorized processing activities.

A generally applicable data protection framework that aligns with international good practices would address these gaps in providing the necessary supplementary measures to ensure robust protection of personal data.

4.H.3 Consumer protection

Introduction, scope of application and key terms

The Consumer Protection Act of 2020 governs the promotion and protection of consumer interests in relation to the supply of goods and services and promotes the protection of life, health and safety of consumers. The Act focuses on consumer rights, duties of supplies, and consumer safety, and establishes a consumer department to oversee and enforce the provisions. However, it focuses on non-personal data related to goods and services. It covers processing of personal data on certain very limited occasions:

- Section 58 states that individuals and business entities may conduct business, advertise, promote, supply goods or services, and engage in consumer agreements only under their legally recognized identity. Individuals are required to use the name recorded on their official identification documents, while businesses and juristic entities must operate under a legally registered name. This provision ensures transparency, helps prevent fraud, and enhances business accountability by ensuring that all commercial activities are conducted under verifiable legal identities.
- Section 59 requires that the name(s) of the producer(s) be included in the "trade description" of products and services. This serves as a prerequisite for displaying, offering, and supplying goods and promotes clear identification of the producer and enhancing consumer transparency and accountability in the marketplace.
- Section 63 requires suppliers of goods and services to maintain a durable record of various types of information, such as the names of the supplier and the relevant VAT number.
- Section 74 requires that suppliers who offer repair services shall keep a record of the name, address and telephone number of the consumer.
- Section 108 requires suppliers to share their name and address with consumers.

Disclosing, sharing, displaying and maintaining individuals' names in the context of commercial transactions constitutes processing of personal data.

Lawful basis of processing

As established in the previous section, personal data is processed to fulfill the purposes outlined in Sections 58, 59, 63, 74, 108, and the Schedules of the Act. This processing is conducted in compliance with the requirements of the Act and in fulfillment of the legal obligations derived from it.

Obligations of the entities processing personal data

The Act does not impose any obligations on entities processing personal data, including consumer or supplier information. The only reference to confidentiality appears in Section 29, which stipulates that confidentiality and non-disclosure of privileged information are required as part of a mediation proceeding.

Data subject rights

The Act does not address any data subject rights.

Cross border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act establishes the Consumer Department and defines its powers and functions under Sections 8 and 9. However, it does not include any offences relating to the processing of personal data.

Conclusion

This Act lacks most aspects of personal data protection, such as obligations for confidentiality, non-disclosure, rights to rectification and provisions related to technical and operational measures for security. Therefore, it would not conflict with a generally applicable data protection law, and rather it would be appropriately supplemented by all of the provisions of such a law.

4.H.4 Freedom of information requests

Introduction, scope of application and key terms

The Freedom of Information Act 2003 provides the right of access to official documents of the government and public authorities to the public. The Act covers the processing of personal data and places limitations to accessing personal data contained in official documents.

It defines personal information as any data concerning an identifiable individual, regardless of the form in which it is recorded. This includes, but is not limited to, details about race, sex, national origin, religion, age, and marital status; information about the individual's education, medical history, criminal record, or employment background; data related to financial transactions; any identifying number or symbol assigned to the individual; and contact details such as addresses, fingerprints, and blood type. Additionally, it covers any correspondence sent to public authorities, as well as information that is explicitly or implicitly private or confidential, including an individual's views or opinions.

Lawful basis for processing

The Act grants individuals the right to access public and official documents and sets out the relevant procedures. When these documents contain personal information, the act of accessing them qualifies as personal data processing, carried out in compliance with the legal obligations established by the Act. However, as established below, the Act also imposes certain limitations and restrictions on accessing records that contain personal information to ensure privacy and data protection.

Obligations of the entity processing personal data

The Act imposes specific limitations on the sharing of records containing personal information, classifying them as “exempt” from disclosure.

- Section 30 states that a document is considered exempt if its disclosure would result in the “unreasonable disclosure” of personal information about any individual, including deceased persons. Additionally, under Section 30(3), if a public authority grants access to a document containing information about an individual other than the requester, the authority must notify the person whose information is being disclosed.
- Section 31(1) outlines further categories of exempt documents, including information related to an individual’s business or professional affairs or details concerning a business’s commercial or financial activities.

These provisions collectively impose restrictions on the disclosure of personal data, reinforcing confidentiality and protection of privileged information. The Act places certain limitations to the sharing of records that contain personal information, qualifying them as “exempt” from disclosure.

Data subject rights

The right to access official documents held by public authorities is established under Section 10. Additionally, Sections 13 and 14 require public authorities to process individuals' requests, assist applicants, forward requests to the appropriate authorities, and respond in a timely manner. These provisions reinforce openness, accountability, and accessibility in public information handling.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act does not establish institutions for the enforcement of its mandate or penalties related to violation of the obligations related to processing of personal data.

Conclusion

The Act is designed to promote governmental transparency and accountability by establishing provisions, such as the right to access information, which place obligations on public authorities. At the same time, it seeks to protect personal information contained in official documents by restricting access where necessary. Rather than conflicting with a broader data protection law, this Act would complement it—benefiting from its provisions on personal data security and enhanced rights for data subjects.

4.H.5 Health

Introduction, scope of application and key terms

The health sector in Saint Vincent and the Grenadines is governed by many Acts, including the Hospitals Act, Medical offices Act, Kingston General Hospital Act and Medical Registration Act.

Among the aforementioned Acts, only the Medical Registration Act explicitly addresses the processing of personal data. This Act stipulates that individuals applying for registration as medical professionals, dentists, or druggists in Saint Vincent and the Grenadines must submit their credentials to the Registrar for evaluation by the relevant Boards.

The registration and certification process under the Act requires applicants to submit personal information, including their name and professional background. The specific details necessary for registration are outlined in the Schedule of the Medical Registration Act.

Lawful basis of processing

The processing of personal data under the Medical Registration Act is conducted on the lawful basis of compliance with a legal obligation. The Act mandates the submission of specific information as a requirement for registration with the relevant Boards.

Obligations of the entities processing personal data

The Acts do not address obligations to entities processing of personal data.

Data subject rights

The Acts do not address data subject rights.

Cross-border transfers of personal data

The Acts do not address cross-border transfers of personal data.

Institutions and penalties

The Acts do not establish institutions or impose penalties relating to the processing of personal data.

Conclusion

The legal framework governing the health sector in Saint Vincent and the Grenadines lacks key elements of a data protection framework and adequate safeguards for processing personal data. Implementing a comprehensive data protection law aligned with international good practices would significantly enhance this framework by introducing clear obligations, rights, and safeguards to ensure the proper handling and protection of personal health data.

4.H.6 Education

Introduction, scope of application and key terms

The Education Act Cap 202 of 2006 governs the provision of educational services in Saint Vincent and the Grenadines by the public as well as private sectors. The Act governs the collection and processing of students' personal information as part of the admission process and their participation in the national

educational system. Although the Act does not explicitly define the terms "student data" or "personal data," the processing of personal data is mandated under the following provisions:

- Sections 23 and 31: School principals are required to establish and maintain a record for each student enrolled in the school. Students over the age of eighteen or the parents of students under the age of eighteen may receive a copy of such a record.
- Section 31: The student records maintained by principals shall include students' names, their parents' addresses, and other information which, when combined, could identify the student.
- Section 43-44: School attendance officers are authorized to enter any premise, question students and collect information such as names, ages, addresses, and other identifying details. This information is used to assess whether a child of compulsory school age is not attending school, thereby facilitating timely interventions.
- Section 46: School principals are required to report on the names of students who have not attended school in order to monitor attendance. They are also required to give to the Chief Education Officer any information required for the enforcement of compulsory school attendance.
- Section 65: The School's board of management, after consulting the principal, shall submit a statement to the Chief Education Officer, within one month after the academic year ends. This report shall cover issues related to student discipline, attendance, academic attainment, curriculum application, school infrastructure, property maintenance, and any other relevant matters affecting the school's development. This information requires the disclosure of students' personal information, which is shared to promote transparency, and improve school operations. Under Section 68, the board management shall keep proper accounts of its transactions which shall be audited annually by the Director of Audit.
- Section 113: Principals, in consultation with professional staff and student parents may determine whether a student has special needs in order to provide the appropriate educational resources. This determination is likely to involve the processing of sensitive personal data of the student.

The activities described above, including the collection of student personal data by school principals, storage of personal data in official records, sharing of student records with students or their parents, and providing students information to authorities and auditors, represent distinct forms of personal data processing.

Lawful basis for processing personal data

The Act implies that the processing of personal data is only lawful when it is utilized for student administration, the disclosure of student's personal data is restricted since information from student records is deemed to be privileged and cannot be shared without consent under section 23.

- Sections 23, 31, 43, 44, 46, 65, 115: As described in the previous section, personal data of students are processed by principals, student officers, auditors and ministers for various purposes provided in the Act, including managing student records, monitoring attendance, and performing other administrative functions. Therefore, the various forms of personal data processing, under the Act, is compliance with the legal obligations under the Act.

Obligations to the entity processing personal data

The Act imposes obligations on entities' processing of personal data, reflecting key principles of data protection:

- Under Section 23(9)-(12) principals are required to establish and maintain accurate student records and timely respond to requests for correction of student data. This obligation reflects the principle of accountability. Specifically, Section 23(7) provides that a student's record is

considered privileged information and shall be used for limited purposes by the school and of Ministry officials in the performance of their functions. Student records are not available to any other person or institution without the written permission of the parent or, if the student is eighteen years of age or older, the student. This provision reflects the principle of personal data confidentiality and promotes the right to privacy.

- Under Section 22(6), information contained in student records, including personal data, may be accessed by specific persons. The Act imposes limitations on third-party access without consent, which promotes confidentiality and integrity of personal data.

The Act does not contain a requirement for implementing technical or organizational measures to maintain the security of personal data.

Data subject rights

The Act provides the data subjects right to access and to rectification of personal data:

- Under Section 43-44, students over the age of eighteen and the parents of students below the age of eighteen have the right to access the students' records, which reflects the right to access.
- Under Section 23(9), an individual authorized under subsection 23(6) may, upon reviewing a student's record, request that the principal rectify any inaccuracies or incomplete information. This right reflects the data subject's right to rectification, ensuring the accuracy and completeness of personal data.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act provides that the Chief Education officer is responsible for overseeing the administration of the Act and ensuring compliance with its provisions. The Education Advisory Board also assists by advising the Minister on educational matters and further policy development.

Under Section 23(12), a person who discloses information from a student's record in contravention of subsection 23(7) commits an offence and is liable on summary conviction to a fine of four hundred dollars.

Conclusion

The Act regulates the provision of education in Saint Vincent and the Grenadines and establishes the framework for the rights and responsibilities of students, parents and educational authorities. While it provides certain basic safeguards over personal data, it does not address issues related to personal data security, cross-border transfers and data retention periods. This Act would not conflict with a data protection framework that would align with international good practices. Rather it would benefit from the additional safeguards, rights and obligations such a framework would impose over personal data.

4.H.7 Financial services (including digital financial services)

Introduction, scope of application and definition of key terms

The financial services sector in Saint Vincent and the Grenadines is governed by the Finance Administration Act, the Finance Act of Saint Vincent, the Money Service Business Act and the Banking Act of 2015. From the aforementioned frameworks, the Money Service Act and the Banking Act refer to the processing of personal data and will be analyzed below.

- The Money Service Business Act covers the processing of personal data by money service businesses. Section 2 defines money service business as a business providing any or all of the

following services "transmission of money or monetary value in any form, cheque cashing, currency exchange, the issuance, sale or redemption of money orders or traveler's cheques, and any other services the Minister may specify by notice published in the Gazette; or the business of operating as an agent or franchise holder of a business."

Under Section 5, any individual or entity seeking to operate as a money service business must apply for a license, by submitting a written application to the Authority. The Authority is responsible for reviewing applications and may conduct further inquiries or communicate with relevant individuals, as necessary. The information required for the application is outlined in Schedule 1 of the Act and includes personal details such as name, occupation, date of birth, citizenship, and national insurance numbers. The collection, review, and storage of such personal information constitute forms of personal data processing.

- Additionally, the Banking Act of 2015, which regulates the banking sector and facilitates the creation of a unified banking space in Saint Vincent, covers the processing of personal data by requiring the collection and handling of depositor and customer information, their financial transactions, and related financial data. The Act also requires the processing of personal information related to shareholders and officers holding positions within financial institutions. While the Act does not establish a comprehensive data protection framework, it imposes a duty of confidentiality and upholds the "secrecy of information" principle, offering some level of protection for personal data within the banking sector.

Lawful basis of processing

Under both the Money Service Business Act and the Banking Act, the personal data provided by individuals or entities in the context of their applications are assessed by the Authority and the Central Bank. This is processing carried out on the lawful basis of compliance with a legal obligation under the Act.

Section 178(1) of the Banking Act sets out the conditions under which personal data related to depositors or customers may be processed lawfully. They specify that individuals who have access to such data in their professional capacity must not disclose them unless one of the following legitimate bases is met:

- Consent: Disclosure may occur if the depositor, customer, or their authorized representatives provide written approval.
- Legal Obligation: Information may be shared when required by the Act itself or by a lawful order of a court with proper jurisdiction.
- Regulatory and International Agreements: Disclosure is permissible under relevant laws of Saint Lucia or agreements among Participating Governments (i.e., members of the ECCU), ensuring compliance with broader legal frameworks.
- Legitimate Business Interests: Certain exceptions allow for limited data sharing in response to legitimate business requests, such as providing a general credit rating, or when conducting due diligence in the context of potential acquisitions, so long as appropriate safeguards are in place.

Obligation of the entities processing personal data

- The Money Services Act does not place any obligations to entities processing personal data.
- Under the Banking Act, licensed financial institutions have obligations under the Act to maintain the confidentiality of data. Section 178 prohibits unauthorized disclosure of customer information, which includes identity information and transactions. Disclosures are permitted if the customer gives written consent or where needed for legitimate business purposes such as credit ratings. It does not provide an obligation for establishing and maintaining a certain level of security measures to safeguard financial information, including financial data. Nor does it address

personal data breaches. Given the substantial amounts of financial information and sensitive personal data managed by financial institutions, it would be appropriate for such data to be subject to such data protection obligations.

Data subject rights

The right does not provide and data subject rights.

Cross-border transfers of personal data

The Money Services Act does not address the cross-border transfer of personal data.

Section 94 of the Banking Act authorizes the Central Bank to establish agreements with foreign supervisory authorities and resolution agencies to collaborate and share information. This cooperation is essential for overseeing and managing financial institutions, including banks and financial holding companies, particularly in scenarios where these institutions fail or are at risk of failure. Such agreements may only be entered into if the Central Bank is assured that the foreign authority will maintain the confidentiality of all shared information. Although generally not focused on personal data, this provision underscores the Act's recognition of the necessity for international cooperation within the banking sector. It highlights the importance of reciprocal safeguards to ensure the confidentiality and integrity of data exchanged between jurisdictions.

Institutions and penalties

- Under Section 25 of the Money Services Act "a licensee, director or an officer of a licensee who knowingly or willfully supplies false or misleading information to the Authority commits an offence and is liable on summary conviction to a fine of two thousand dollars or to imprisonment for a term of three months, or both."
- Under Section 96 of the Banking Act, any licensed financial institution that knowingly supplies false or misleading statements, returns, information, or data in any material is subject to a penalty of $25,000. This is aligned with typical data protection obligations to maintain the accuracy of personal data.

Conclusion

The financial services sector in Saint Vincent and the Grenadines, although is governed by multiple laws, has limited provisions covering processing of personal data, identified in the Money Services Act and the Banking Act. While they offer certain limited obligations of confidentiality, these Acts lack provisions for data security measures, the rights of data subjects, and the regulation of cross-border personal data transfers. A generally applicable data protection law, aligned with global best practices would complement this framework and provide provisions imposing obligations of confidentiality, security and transparency regarding the processing of personal data to financial institutions.

4.H.8 National identification (including digital and functional forms)

There is currently no legislation in this area in Saint Vincent and the Grenadines.

4.H.9 Passports

The legal framework governing passports in Saint Vincent and the Grenadines is outlined in the Immigration (Restriction) Act, Cap 114, as amended by the 2017 Amendment Act. However, this Act does not address the processing of personal data.

4.H.10 Civil registration

Introduction, scope of application and definition of key terms

The Registration of Births and Deaths Act Cap 242 provides the process governing the registration of births and deaths in Saint Vincent and the Grenadines. It defines the duties of the Registrar-General and sub registrars and establishes procedures for registration and penalties for non-compliance.

The registration of births, deaths, and the rectification of civil status records is carried out by Registrars and Sub-Registrars and involves the collection and handling of personal data. This process requires the disclosure of individuals' names, addresses, and personal status, as specified in the various forms outlined in Schedule 1 of the Act.

The collection, maintenance, and storage of personal data related to births and deaths constitute "processing" under data protection laws.

Lawful basis for processing personal data

The lawful basis for processing personal data stems from the public interest as well as the administrative necessity for accurate civil registration. Under section 10A the Act allows for the maintenance of records on electronic form which complies with modern data management.

Personal data provided by individuals or their parents are processed by the Registrar-General and other parties in order to register births and deaths. The requirement for registration of these events is a legal requirement under the Act, which mandates that it "shall be the duty" of the parents or occupiers of the place of the child's birth to provide the registrar with the required information for the registration of the child (Section 17), and that a person's death "shall be registered" according to Section 31. Subsequently, the relevant officials process this personal data in accordance with the statutory mandate of the Act and subsequent regulations to maintain accurate and official records of civil status.

Obligations of the entity processing personal data

The Registrar General as well as the other authorized officials shall maintain accurate and durable register books and electronic records and make annual reports to the Governor-general on the births and deaths. The Act does not impose obligations of confidentiality, security and non-disclosure of personal data.

Data subject rights

The rights of the data subjects include the correction of data upon the provision of statutory declarations and access to searches and indexes to obtain certified copies of the entries under sections 25, 26, and 30 respectively.

Cross-border transfers of personal data

The Act does address cross-border transfers of personal data.

Institutions and penalties

The Act does not expressly mention the established institution. However, the Governor General may appoint a Registrar-General who will operate under the Births and Deaths Registrar General Office.

Also, the district registrars are responsible for managing the local registrations, maintaining the indexes and allowing for searches of the same. The penalties for non-compliance include false statements or forgeries which carry fines up to $500.00 or imprisonment for 5 years, destruction or injury of registers which carries the penalty of up to 15 years imprisonment, failure to notify/ register births or deaths which carry fines

ranging from $100 to $250 and withholding registers from the register- General which attracts a fine of $250.00.

Conclusion

The Act provides several provisions governing the collection, administration, and management of civil status records, and contains processes that promote their accuracy. However, it offers limited safeguards and protections for personal data. The absence of data subject rights, obligations for data security, safeguards against breaches, and adequate penalties poses significant risks to individuals' personal information. Addressing these gaps by implementing additional clauses would ensure the Act's compliance with international data protection standards.

Introducing a comprehensive data protection law that does not exclude the processing activities under this Act would enhance the overall protection of personal data within the civil registration process. Importantly, the Act does not contain any provisions that would contradict or be inconsistent with a generally applicable data protection law.

4.H.11 Electronic communications

Introduction, scope of application and definition of key terms

Telecommunications Act No. 2 of 2001 governs the telecommunications services in Saint Vincent and the Grenadines and regulates the licensing and oversight of telecommunications networks and services. Key provisions of the Act deal with the protection of personal data, confidentiality of communications and prohibition of unauthorized interception of communications. Saint Vincent and the Grenadines is a signatory to the Treaty establishing the Eastern Caribbean Telecommunications Authority (ECTEL), a regional agreement designed to foster competition in the telecommunications sector and harmonize policies across the region.

The Act addresses the processing of personal data in several instances:

- Under Sections 27-28, the Telecommunications Commission (“Commission”) is responsible for receiving and evaluating applications submitted by entities and individuals seeking a license to operate as a communications network or provide communication services. These applications include personal information such as names, business addresses, email addresses, and phone numbers.
- Under Sections 52-55 inspectors have the right to enter and search vehicles, ships, vessels, aircraft, or premises, if there is reasonable suspicion of non-compliance. They may remove or copy documents and, with a court order, seize telecommunications apparatus. Entry without consent requires a search warrant, and inspectors must present both the warrant and their identity card. After a search, a receipt listing seized items must be provided. Additionally, magistrates may issue search warrants allowing inspectors, with or without police assistance, to examine, test, or seize relevant equipment. Seized items must be returned if no legal proceedings commence within 30 days, unless they are required for an ongoing case.
- Additionally, the Act states that operators themselves receive and process subscriber personal information as part of their service delivery and grants the right.

Lawful basis for processing

The Act mentions different types of data processing, specifically personal data related to subscribers and communications.

- Entities that establish or operate a telecommunications network or provide telecommunications services are required to submit personal data as part of their application for obtaining, modifying, or renewing a license under the Act. The Commission subsequently shares this information with

ECTEL and processes it in accordance with the Act to assess the applicant's suitability for licensure.

- Telecommunications network operators and service providers, in turn, process subscribers' personal data as part of their contractual obligations to deliver telecommunications services.

Obligations of entities processing personal data

The Act provides certain obligations concerning confidentiality and protection of personal data.

- Section 59 requires confidentiality of messages transmitted over a public telecommunications network. It prohibits the interception or interruption of such communications unless explicit consent is given by the sender or a court order is issued under this Act or another relevant law.
- Section 60 reflects the confidentiality of personal information belonging to telecommunications subscribers. It prohibits telecommunications providers from disclosing subscribers' personal data unless the subscriber gives consent, or a court order mandates disclosure under this Act or another legal provision.

Together, these provisions emphasize data privacy and the protection of communications, ensuring that both messages and personal subscriber information remain confidential unless legally authorized otherwise.

Data subject rights

The Act mentions minimal data subject rights:

- Under section 12(1) a data subject may request to inspect records maintained by the commission, which reflects the data subject right to access.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act establishes the National Telecommunications Regulatory Commission, which is responsible for overseeing compliance with the Act, it outlines powers of inspectors to investigate and enforce compliance. The Act contains certain penalties related to the processing of personal data. Under Sections 62 a person committing unlawful interception and disclosure of personal data is liable on conviction on indictment, to a fine not exceeding fifteen thousand dollars or to imprisonment for a term not exceeding one year. Additionally, under Section 64, a person who knowingly gives false or misleading information to the Commission commits an offence and is liable, on conviction to a fine not exceeding five thousand dollars or to imprisonment for a term not exceeding six months.

Conclusion

Although the Act requires personal data to be treated with confidentiality, it does not provide adequate measures to ensure its security and protection. To address these shortcomings, the Act would benefit from the implementation of additional safeguarding and security protocols. Furthermore, it should be complemented by a comprehensive data protection framework to enhance the security and integrity of the personal data involved.

4.H.12 Electronic transactions

Introduction, scope of application and definitions of key terms

The purpose of the Electronic Transactions Act of 2015 is to give legal effect to electronic documents, records and signatures. Its main objective is to ensure that electronic transactions are not denied their validity, enforceability or legal effect solely because of its electronic nature. The Act does not specifically

address personal data, but it is implied that some electronic records may contain personal data or information.

This Act regulates personal data in the context of electronic communications between two persons, designated as "the originator" and "the addressee". As defined in Section 2:

- "*originator*" in relation to an electronic communication, means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that communication; and
- "*addressee*" in relation to an electronic communication, means a person who is intended by the originator to receive the electronic communication, but does not include a person acting as an intermediary with respect to that electronic communication.

Electronic communications between an originator and addressee will often include the following personal data: their names, email addresses, metadata such as the time and location of an email, identifiers included in a signature (phone numbers, physical addresses, and other contact details may be shared directly within the email content), along with any information revealed in the context of their communication.

According to the definition of "electronic communications", which cover information being "*communicated, processed, recorded, displayed, created, stored, generated, received or transmitted by electronic means*", personal data undergo "*processing*" as they are transferred by the originator and subsequently received and stored by the addressee.

Lawful basis for processing personal data

Personal data involved in electronic transactions, as defined under the Act, are processed under several lawful bases:

- Processing personal data performed in the context of electronic transactions is performed in compliance with a legal obligation under this Act, or due to the necessity of performing a public task. Section 7 and 8 provide for the legal recognition of electronic communications and electronic records. Specifically, Section 8 allows information that is normally required by law to be given or recorded in writing (or in printed form) to be provided electronically, as long as the electronic version is the same or substantially the same as the non-electronic form, it is accessible to the other person, and it is capable of being retained by the other person.
- Under Sections 16-21, the processing of personal data involved in the formation and enforcement of electronic contracts is performed under the lawful basis of contractual necessity. In the context of automated contracts, personal data is required to fulfill the terms and obligations outlined in the contract, such as providing services, delivering goods, or managing transactions.

Obligation of the entities processing personal data

The Act provides several obligations that reflect data protection principles.

- Section 26, it allows parties involved in a transaction to state the use of information security procedures, this allows for some form of control over the security measures. This places the responsibility on the parties themselves to negotiate appropriate security measures.
- Section 36 mandates that anyone selling goods or services to consumers via electronic communication must provide clear, accurate, and accessible information, including their legal name, principal geographic address, and an electronic means of contact or telephone number. This provision reflects the principles of data accuracy and data quality.

Data subject rights

The Act does not address data subject rights.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

The Act mentions that the Minister shall make regulations for the purpose of having an effect on this act. With regard to the offences section 39 stipulates that where a person files information under this Act that contains false or misleading information or provides a consumer or a user of an electronic signature with false or misleading information commits an offence.

Under Section 40, any person who submits false or misleading information required by the Act, or provides consumers with deceptive information or falsified signatures, commits an offense. Upon summary conviction, the offender may face a fine of up to two hundred thousand dollars, imprisonment for up to three years, or both. If convicted on indictment, the penalties increase to a fine of two hundred and fifty thousand dollars, imprisonment for up to five years, or both. These penalties may also apply to cases involving personal data if the false or misleading information pertains to personal information.

Conclusion

While the Electronic Transactions Act provides a framework for regulating electronic communications and ensuring the validity of electronic documents and signatures, it addresses inadequately several aspects pertaining to data protection. The Act does not impose any obligations on the originator, addressee or the carrier of electronic communications regarding the protection, maintenance of integrity, or safety of personal data. Additionally, there are no provisions concerning data subject rights, cross-border data transfers, or relevant institutions authorized to oversee electronic communications. As a result, electronic transactions would benefit from a comprehensive data protection framework that imposes obligations, rights, and responsibilities regarding the processing of personal data on both originators and addressees.

4.H.13 E-signatures

Introduction, scope of application and key definitions

The Electronic Transactions Act 2015, Parts 4 and 5 refer to electronic signatures. It mandates that the requirements for signature are satisfied in relation to an electronic record, if a method is used to identify the person and to indicate that person's intention in respect of the information contained in the electronic record. It stipulates that unless otherwise provided by law, there should be equal treatment of signatures and the parties themselves may agree to use a particular method or form of electronic signature. This section does not specifically address processing or collection of personal data.

Under Section 2 of the Act, "electronic signature" is defined as "data in electronic form that are attached to, incorporated in or logically associated with other electronic data, and serve as a method of authentication."

Also, the Act defines "encrypted signature" as a "means an electronic signature that is encrypted by means of a private key or other encrypted signature creation device".

An individual using electronic signatures is a "signatory" and is defined as "a person who may or may not hold a signature creation device and acts either on his or its own behalf or on behalf of another person to create an electronic signature."

The use of electronic signatures would typically constitute processing of personal data under a data protection law.

Lawful basis for processing

Where an electronic signature is used to enter into or perform contractual obligations, this would be a lawful basis for processing the personal data embedded within these signatures (e.g., name, email address, unique identifiers).

Obligations of the entities processing personal data

Section 26(2) and 27(2) requires that electronic signatures are protected by security procedures, which are considered as "commercially reasonable", based on various factors, including the nature of the transaction, sophistication of the parties, the volume of transactions, availability and cost of alternatives offered to parties and procedures in general use for similar transactions.

Data subject rights

The Act does not address data subject rights.

Cross-border transfers of personal data

The Act does not address cross-border transfers of personal data.

Institutions and penalties

Under Section 40, any person who submits false or misleading information required by the Act, or provides consumers with deceptive information or falsified signatures, commits an offense. Upon summary conviction, the offender may face a fine of up to two hundred thousand dollars, imprisonment for up to three years, or both. If convicted on indictment, the penalties increase to a fine of two hundred and fifty thousand dollars, imprisonment for up to five years, or both. These penalties may also apply to cases involving personal data if the false or misleading information pertains to personal information.

Conclusion

The Electronic Transactions Act, as it pertains to governing electronic transactions, lacks several key requirements covering processing of personal data. This framework would not conflict but would benefit from a generally applicable data protection framework developed in alignment with international good practices.

5 Conclusions of the data protection gap analysis

We turn here to our conclusions of the data protection gap analysis, summarizing in Section 5.A the weaknesses of the national data protection laws and the OECS Model Bill reviewed in Sections 3 and 4, respectively. Not only do they have substantive weaknesses, but considered as a whole across the region, they undermine cross-border data flows, as we explain in Section 5.B. We conclude in Section 5.C that this results in significantly adverse prospects for the development of the digital economy.

5.A Weaknesses of the data protection laws

The table below weighs the relative alignment of each national and regional data protection instrument against global good practices. We have used the "Harvey Balls" symbols to indicate the degree of completeness and alignment of each attribute:

Lesser strength → Greater strength

○ ◔ ◐ ◕ ●

Of the eight ECCU member states, five have enacted data protection laws, though the majority have yet to enter into force, e.g., because the necessary order of the relevant Minister has not been issued. Some have entered into force in part but omitting elements, such as the establishment of the data protection authority.

The influence of the OECS Model Bill, including its weaknesses, is particularly evident in Antigua and Barbuda, Grenada, and Saint Kitts and Nevis. Saint Vincent and the Grenadines were, commendably, a first mover, enacting their law in 2003, but their law has naturally become very outdated with the passage of time.

Table 1. Strengths and weaknesses of OECS data protection frameworks

Countries/regions	Scope of applicability	General elements of data protection law	Principles governing the processing of personal data	Individual rights concerning personal data	Data security	Cross border transfers of personal data	Institutions	Enforcement
Anguilla	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Antigua and Barbuda	◕	◐	◕	◕	◔	○	◐	◐
Dominica	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Grenada	◕	◐	◕	◕	◔	○	◐	◐
Montserrat	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Saint Kitts and Nevis	◕	◐	◕	◕	◔	○	◐	◐
Saint Lucia	◕	◐	◕	◕	◔	◔	◐	◐
Saint Vincent and the Grenadines	◔	◔	◔	○	◔	○	◐	○
OECS Model Bill	◕	◐	◕	◕	◔	○	◐	◐

5.B Barriers to cross-border data flows

As the ECCU embraces the digital economy and aims to attract foreign investment and service providers to the region, it will be essential to establish legal and regulatory frameworks that enable and safeguard information flows. Personal data constitute a significant portion of the information exchanged in digital economy activities. An effectively harmonized personal data protection framework will be key to enable such information to flow in trusted manner, i.e., with appropriate protections, with minimal impediments.

Figure 14. The importance of trusted data flow

The sections below examine barriers to the flow of personal data arising from the ECCU countries' national data protection laws:

- Section 5.B.1 considers the effect of the lack of provisions on cross-border data flows in the laws.
- Section 5.B.2 considers the challenge of harmonization where there are multiple jurisdictions having different levels of maturity in their laws and institutions.
- Section 5.B.3 highlights the problems arising from differences among such laws as have been passed.

5.B.1 Lack of provisions on cross-border data

National data protection laws can impede or enable cross-border data flows in the digital economy. They may legitimize data transfers, impose localization requirements, establish standards and conditions under which cross-border transfers may occur, and provide tools and mechanisms to facilitate the seamless flow of information. (See Section 2.F of this report.)

As explained in Section 4 of this report, only five of the ECCU countries have a generally applicable data protection law and most of these have not entered into force. Only Saint Lucia's law contains provisions on cross border transfers of personal data. Saint Lucia's cross-border transfer provisions do not establish a framework that would enable the *trusted* flow of personal data, such as adequacy decisions and other data protection mechanisms. (See Section 4.G.1 of this report.)

As such, there are few legal prohibitions that are express, direct barriers to the cross-border transfer of personal data in the region. However, this is far from ideal, as it also means that personal data can cross borders without protection, and so there is no provision ensuring *trusted* cross-border data flows. Given the small size of the countries, their domestic tech industry will inevitably be limited in scope and scale. Countries are likely to have to rely very extensively on service providers and processing outside the region. A very large proportion of personal data in these countries is likely to have to be transferred abroad for ECCU member states to benefit from the digital economy. The lack of provision for cross-border data flows effectively strips the data of protections (to the extent they are provided for) upon transfer. This fundamentally undermines the entire data protection framework such as it is today.

5.B.2 Varying levels of maturity

The varying levels of maturity in national data protection frameworks among the ECCU member countries adds complexity to the barriers:

- Anguilla, Dominica, and Montserrat lack formal data protection laws altogether.
- Antigua and Barbuda, Grenada, and Saint Kitts and Nevis have largely adopted versions of the OECS model bill.
- Saint Lucia has a more recent and comprehensive law.
- Saint Vincent and the Grenadines' law is now quite dated and applies solely to public sector entities.

These differences exist despite regional efforts to promote the adoption of the OECS Model Bill. The inconsistencies risk deterring businesses from operating across the region, as they have to research, navigate and comply with each country's unique requirements. Providers have to develop different compliance strategies for each jurisdiction. This can be particularly burdensome for small businesses. Additionally, the difficulty in accessing national laws online and the absence of operational data protection authorities in countries with existing frameworks further complicate the process. The incomplete patchwork presents a region that is not ready for the personal data protection realities of the digital economy. This signals an overall discouraging uncertainty for service providers.

5.B.3 Differences among national laws

There are various important differences among the ECCU member states' national laws that could result in barriers to personal data transfers within the region. We mention only two examples below for the purpose of illustration.

Diverse definitions of the term "personal data"

The term "personal data" is defined differently across the national data protection laws that have been enacted. As a result, information deemed as personal data in one country may not be recognized as such in another.

Antigua and Barbuda's, Grenada's, and Saint Kitts and Nevis's definitions of the term personal data reflect that of the OECS Model Bill. This limits personal data to information "related to commercial transactions." This would exclude any information that is not "in respect of commercial transactions," including personal data collected by public bodies and processed for government administration, public policy, research, and scientific operations, as well as situations where personal data is collected by a government entity and subsequently shared with a private sector entity that is not engaged in "commercial transactions."

Conversely, Saint Lucia's data protection law defines personal data as "information about a data subject that is recorded in any form" and does not limit it to "commercial transactions." As a result, information processed outside the scope of "commercial transactions", such as by public authorities, is considered personal data in Saint Lucia and is therefore protected under its national data protection framework. The same information is not regarded as personal data in Antigua, Grenada, and Saint Kitts and Nevis.

The approach to personal data in Saint Vincent and the Grenadines adds another layer of complexity to the regional landscape. Although its national law provides a comprehensive definition of personal data, its scope is restricted to *public authorities*, thereby excluding any personal data processing conducted by private entities. These are fundamental differences and problems that go to the heart of the effectiveness of a data protection framework.

Varying enforcement mechanisms

The enforcement mechanisms provided across the national data protection frameworks within the ECCU region constitute an additional discrepancy on how rights, and obligations on personal data are implemented and enforced, thereby disincentivizing cross border flows across the region.

For example, Antigua and Barbuda's Act does not provide a clear procedure for data subjects to file complaints with the authority when they suspect or experience a violation of a data controller's obligation under the Act. Similarly, in Saint Vincent and the Grenadines, although the Act outlines a process for seeking remedies in the event of a violation by a data controller, it does not empower the data protection authority to impose penalties for breaches of its provisions.

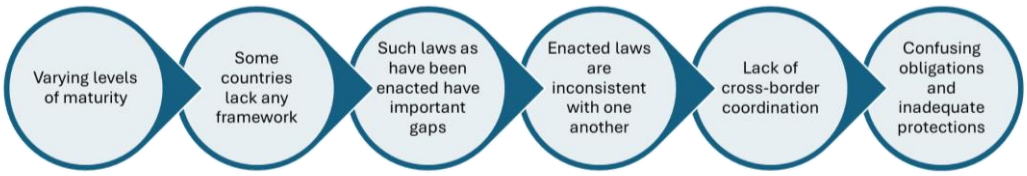
In contrast, Saint Lucia, Grenada, and Saint Kitts and Nevis have provisions that establish data subjects' rights to file complaints, which can lead to investigations and, where appropriate, the imposition of fines and penalties.

Inconsistent enforcement mechanisms for data protection laws among countries within the region can impede the prosecution of cross-border violations, complicating the establishment of mutual adequacy agreements, and placing additional obstacles in efforts for seamless and secure cross-border data transfers.

5.C Implications for the digital economy

A framework for coherent and efficient handling of cross-border transfers of personal data would aim to produce coherent and consistent application of shared data protection principles, and to minimize duplicative supervisory processes in multiple countries. (See Section 2.F.7 of this report.) The absence of such a framework will impede the development of the digital economy across the region. Controllers and processors will face different results in different countries. Their costs of dealing with multiple authorities, and the cost to multiple authorities of dealing with the same controllers or processors, will burden the region's economy, public and private sectors. There is a significant risk that several countries will simply not devote the public resources to regulate effectively, and that private firms will not pay attention to those that try to. The resulting loss of confidence in the effectiveness and seriousness of the regulatory framework will undermine confidence in data protection, and in the digital economy itself.

Figure 15. Impediments to digital economic development



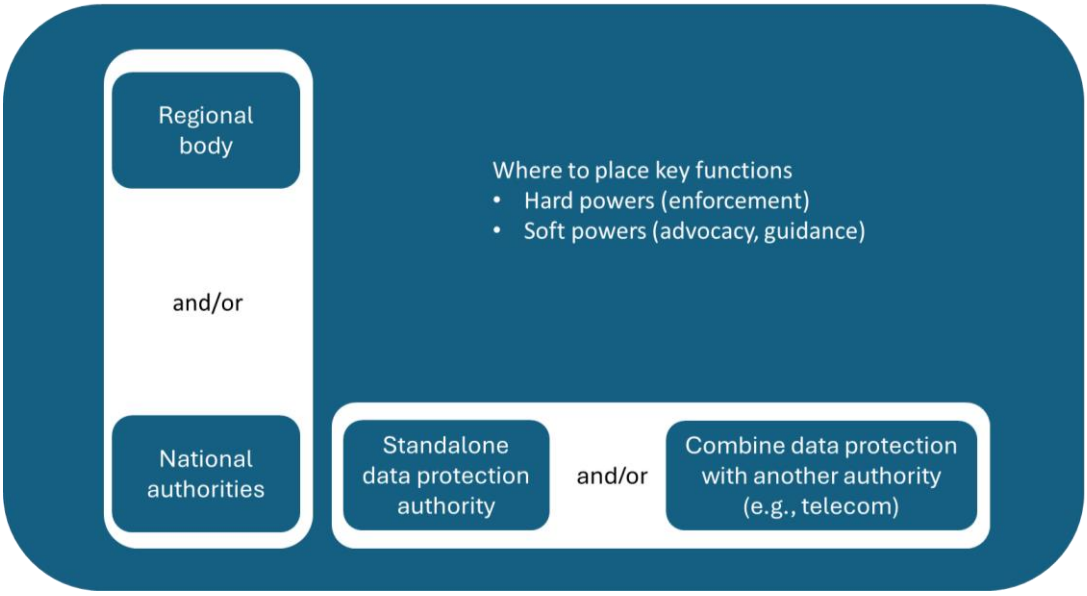
6 Considerations for regional and national legal frameworks

We turn now to consider how best to address the gaps identified. We briefly outlined our approach to harmonization in Section 1, focusing on:

- ***reasonable alignment*** among the legislation and its application in the region;
- ***institutional effectiveness*** and coherence among national and any regional authorities; and
- overall alignment with ***good international practice***.

In considering the best approach to a new legal and regulatory framework that will include a data protection authority, we begin next by considering the nature of obligations and rights involved, and of the powers and functions of a data protection authority. Section 6.A discusses these legal features and how they necessarily frame the options for the design of a data protection framework, particularly how the national and regional levels might interact. However, there are functions of a data protection authority that do not strictly depend on the exercise of legal powers. Section 6.B discusses options for how these functions might be distributed between national and regional bodies. Section 6.C discusses the option of building data protection laws and institutions onto existing regulatory frameworks in adjacent areas (e.g., telecommunications or consumer protection) rather than having standalone data protection authorities.

Figure 16. Legal, vertical, horizontal and functional considerations



6.A Legal drivers in design of a data protection framework

6.A.1 Rights, obligations and powers

As explained in Section 2, data protection laws establish obligations for data controllers and data processors, rights for data subjects, and powers for data protection authorities. We look first at this legal structure, and then consider its implications for designing a regional framework.

Under a typical data protection law, controllers and processors are statutorily obligated to respect various requirements relating to privacy and security of information. These concern how they collect and otherwise process data, how they deal with data subjects, and how they deal with data breaches. Failure to fulfil these is a breach of statutory obligations subject to investigation by the authorized authority, and potentially obligations to pay penalties ordered by the data protection authority or by a court. Such an investigation might be initiated pursuant to a complaint by a data subject to the data protection authority (where a complaints process is provided for) or on the authority's own initiative (where it has reason to suspect a violation). Many of the statutory obligations of controllers and processors imply corresponding data subject rights. For instance, a controller's obligation to inform a data subject about the purpose of processing personal data about him or her may correspond to a right of the data subject to be so informed.

Conversely, data subjects' statutory rights will imply corresponding obligations of controllers and processors owed to the data subjects. Data subjects' statutory rights typically include, for example, to verify what personal data relating to them are being processed, rights to have erroneous data corrected, rights to object to processing in certain circumstances, and rights to complain. Data subject rights should generally be specifically enforceable by data subjects, either by complaint to a data protection authority that may order compliance, or in the appropriate court. Damages for loss suffered by a data subject caused by a violation by the controller or processor might be claimed by the data subject, and the controller or processor might have an obligation to pay. Whether or not the data protection authority (as opposed to a court) can order compensatory remedies as opposed to ordering compliance or payment of a fine for noncompliance will depend on the approach taken in the given country's law.

For our purposes, a data subject wishing to enforce his or her rights will in most cases be located in the jurisdiction in which the relevant national data protection law applies. This location of the data subject is one of the necessary elements of the territorial connection that brings the relevant processing within the scope and jurisdiction of the law. For a data subject to be able to exert his or her rights, it will be necessary for there to be a means of raising them before a data protection authority (in the case of a complaint of

nonfulfillment of a statutory obligation) and a court (in the case of a claim for specific enforcement or damages), or both. In each case, the authority to which the data subject has recourse must have a means of enforcing its orders resolving the matter.

For a data protection authority to be able to hear complaints and issue orders with legal force over a controller or processor, it must have the power to do so under an applicable law. That law, or other laws, must provide not merely that it may issue orders, but the overall framework must have a way to ensure that its orders are enforced. For instance, if the data protection authority orders payment of a penalty, this must be recognized under law as a legally binding debt on which the authority can collect. Ultimately, it may need to use the applicable debt collection machinery, ultimately such as seizing bank accounts and assets. Similarly, if the data protection authority orders a controller or processor to take, or cease taking, certain actions, it may depend on the ability to back this up with the order of a court ordering compliance with the authority's order, and then on contempt of court in the case of noncompliance. These are typically found in national law and not regional law.

All of the above may sound obvious but where more than one country is involved, it has implications for the design of a regional framework. We will return to the legal framework after considering the functions of data protection authorities.

6.A.2 Implications for institutional design

Where a data subject resides in one country but a controller is in another, the rights of the former and obligations of the latter need to be coherently addressed together in one forum. Otherwise, there is a risk of forum shopping, and duplicate and possibly even conflicting processes. This requires an arrangement on allocation of cases among forums that might each have jurisdiction over the matter. Such an arrangement would have to bind controllers, processes, data subjects and the authorities.

The authority charged with leading supervisory function for a given matter could be:

- a national authority;
- a regional authority; or
- a combination of national and regional authorities.

National authorities

Under this model, each ECCU member state would establish its own data protection authority under a national law. This was the approach to the current OECS Model Bill and national data protection laws. It is also how consumer protection laws currently work in OECS countries.

Each authority's powers would be grounded in national legislation, avoiding the complexities of establishing a regional entity with institutional structures and international negotiations. Their direct connection with the national legal order and business community would support the legitimacy of their activities and possibly facilitate enforcement actions.

However, a national authority is costly for a small country to establish in terms of the governance machinery, needed leadership status and required technical and legal expertise.

A purely national approach also leaves no means of coordination where controllers or processors are active in multiple countries and the same conduct could be addressed by a single authority rather than every affected country's authority. It would still be desirable to have a coordinated or even a "one-stop-shop" arrangement whereby one national authority takes the lead over others in cases affecting multiple countries. The choice of the lead authority could be made according to specified criteria (e.g., jurisdiction where the controller or processor is established, per the EU GDPR) agreed among the countries. Resolving uncertainties and conflicts over which authority might take the lead would depend on a system. That could be a council or committee of Ministers of the countries involved, or it could be another regional body, with national law providing that such a decision is binding under the national law. In any case, all of the above would depend on some form of agreement among the countries.

Regional authority

A second approach could be to establish a regional authority with direct powers to hear complaints, carry out investigations and issue orders resolving them (whether ordering conduct, ordering conduct to cease, or ordering a penalty). This would require the rights of data subjects and the obligations of controllers and processors to be established by or recognized in a regional legal instrument. That could be a treaty agreement among countries, or legislation authorized to be issued under a treaty providing for such legislation (e.g., an OECS Act).

Absent regional enforcement authorities and mechanisms (e.g., debt collection and seizure powers), the powers of such a regional authority must in turn be given effect in national law. This can be achieved broadly in one of two ways:

- A regional body's decisions may have the force of law in the state parties' national laws if the treaty agreement so provides and if national law accepts the treaty as having force as national law. As we will see in Section 7.B, OECS member states have not accepted the OECS treaty as having force in national law.
- Alternatively, the national law could provide that an order of the regional body shall have force of national law, whether directly upon issuance, or pursuant to a process of domestication, e.g., publication in the national official gazette, or endorsement by a national authority (as is the case with ECCB regulations).

Establishing a regional data protection authority within the ECCU region could offer several financial, strategic and operational advantages. ECCU member states share a comparable economic state, cultural background, formal language and economic and commercial objectives, allowing the data protection authority to fulfil its mandate and serve equally the respective member states. Additionally, they have established a record of successful institutional integration in several levels of the economy, such as in banking, monetary policy and telecommunications.

Member states would jointly bear the cost of establishing and maintaining a regional authority, instead of duplicating this cost across their national budgets, and would leverage collectively their expertise and resources. This would also promote a unified regional approach and shape a consistent voice in international data protection dialogues, enabling the ECCU to advocate more effectively for its interests and negotiate agreements on cross-border data transfers, security safeguards and other impactful topics for the digital economy.

On an operational level, a regional authority could oversee the implementation of respective national data protection laws and offer harmonized solutions to regional data protection challenges, thereby avoiding the fragmentation and inefficiencies that arise from multiple national authorities addressing the same issues independently. It would also promote consistent enforcement across all ECCU member states by harmonizing redress procedures and administrative requirements, which would promote a predictable framework for the digital economy. Additionally, it would facilitate cross-border data transfers by negotiating adequacy decisions amongst the ECCU member states and establishing data transfer tools and mechanisms. This role would be particularly important because, as analyzed above, most ECCU member states lack such frameworks.

However, it is not clear that ECCU member states would be willing to yield the necessary sovereignty to such a regional authority.

Combination of national and regional authorities

A combination of national and regional authorities could be involved in data protection enforcement. For example, national authorities might treat some cases, and the regional authorities might treat others. Criteria for allocating cases between national authorities and the regional authority might depend on whether there were a cross-border aspect to it, or the matter were of a certain scale or importance. Alternatively, national authorities might receive all cases but refer some (again, according to agreed criteria) to the regional authority for recommendation or decision to be implemented by the national authority. This is the approach taken with ECTEL, for example. Again, it will be necessary for the original jurisdiction of the regional

authority or referrals to it from the national authority (as well as the effect of its decision) to be given effect in the regional and national law.

We will see (see Section 7.B) that despite the Treaty of Basseterre, Acts of the OECS Authority do not have direct effect because most countries expressly reserved against Article 5.3 of that Treaty that provided that they would. Similarly, decisions of the ECCB do not have direct effect under national law, having effect only when the necessary steps to give legal effect to them in each of the territories. ECCB regulations have to be published in the Official Gazette of each of the participating governments and notified to the public.

Before turning to consider the region's various legal frameworks in detail, we look now at other factors affecting the design of national and regional data protection frameworks.

6.B National and regional allocation of functions

This report has focused largely on matters of law – rights, obligations and powers. This necessarily leads the approach because rights, obligations and powers have to be established by law. As mentioned in Section 2.G.2 and above in Section 6.A, data protection authorities have a number of important enforcement and regulatory functions that require them to have legal powers, and which affect the approach to national and regional arrangements.

However, enforcement and regulation are not the only activities of a data protection authority. As also mentioned in Section 2.G.2, a data protection authority typically has numerous functions that may not require the exercise of legal powers but are very important.

Legal powers are not necessarily required for an agency to issue guidance, or carry out promotion, awareness raising, training and research, or develop and suggest policy and new legislation to policymakers. Naturally, an agency with enforcement powers will do these things with much greater "authority," but these activities do not strictly need the power of law. As a result, the design of institutional responsibilities for activities that do not require legal powers is not as driven by the legal interplay between regional and national legal systems (see Section 66.A of this report) as those that do require legal powers. The incursion of a regional framework into national sovereignty is much lighter where the regional body does not exercise substantial legal powers.

There is a tension between the benefits of centralization of functions at the regional level and placing functions at the national level. Some consolidation of resources can make it possible to carry functions out more efficiently even where it is not possible to consolidate the legal powers in the same way. This could mean that while *legal powers* strictly remain at the national level, some of the guidance and promotional activities could be pooled in a regional body. This is akin to the approach taken with ECTEL. (See Section 7.D of this report.) Other than with respect to radio spectrum management, ECTEL itself is not accorded regulation-making powers to issue instruments with binding impact at the national level. It appears to have been delicately designed to avoid yielding hard national legal powers to the regional entity, while nevertheless giving the regional entity very important roles in a number of very important areas. These include managing licensing processes for the more important individual licenses and giving recommendations on key regulatory matters such as interconnection and universal service, on which national authorities appear to be expected to act.

In the case of data protection, it could be that all countries could benefit from sharing a regional body that pools expertise and gives guidance on the implementation of data protection law, while leaving the direct exercise of legal authority at the national level. Some degree of regional centralization may, then, be helpful together with carrying out these functions at a national level.

At the same time, however, there are benefits to having the guidance, promotional and policy functions of data protection authority at a national level. The national authority has a beneficial physical and administrative proximity to regulated entities and individuals. This can allow for better engagement with local companies, non-profits, government agencies and citizens. Such proximity can enhance outreach efforts, education on data protection matters, day-to-day oversight and foster a sense of accountability. Additionally, when operating effectively, national authorities can develop regulations, guidelines, and tools that closely align with each country's specific legal framework, social norms, and administrative structures.

6.C Standalone or multi-domain authorities

It is common internationally for countries to enact standalone data protection laws and establish data protection authorities to monitor conduct and enforce the statutory obligations. Indeed, this was envisaged in those Eastern Caribbean countries' laws that have been passed but not entered into force or not implemented. Each provides for its own data protection authority.

This is not, however, the only way to provide for the rights, obligations and powers, and the principles, of data protection described in Section 2. An alternative approach could see the data protection function added onto the mandate of another authority. The most obvious existing candidate authorities for this could either be:

- a telecommunications regulatory authority, because it deals with technology and already deals with consumer protection and privacy to some degree in the telecommunications context; or
- a consumer protection authority, because it has the aim of protecting individuals in a generally asymmetric situation, including ensuring that individuals are informed, have abilities to make choices, and effective recourse to hold organizations accountable.

These possibilities will be considered when we turn in Section 7 to review existing legal and institutional frameworks in the region.

7 Relevant existing regional frameworks

7.A Introduction

Section 6 explored conceptually the legal drivers for the design of a regional data protection framework, including options for the distribution of powers and functions between national and regional authorities, and for building data protection onto existing laws and institutions.

We turn here to consider how the gaps described in Section 5 and the key considerations discussed in Section 6 of this report translate to the ECCU context. Our aim in this Section is to understand to what extent existing legal and institutional frameworks familiar to ECCU member states can be leveraged to develop a harmonized and enforceable data protection framework.

We begin by reviewing the most relevant regional organizations and institutions in the ECCU and OECS in order to understand their legal and institutional structures, and how the regional and national levels work together. We do this because an existing framework could potentially be a useful mechanism for enacting data protection legislation (e.g., the OECS and its legislative organs). Alternatively, an existing framework might be one on which data protection could piggyback by adding data protection supervisory powers to an existing authority (e.g., the ECCB, ECTEL and national telecommunications regulatory authorities, or national consumer protection departments).

We review the following:

- ***OECS:*** We review the OECS legislative organs because all of the ECCB member states are members of the OECS, and because the OECS has a clear legislative framework.
- ***ECCU:*** We review the ECCB and ECCU framework because, although this project is about data protection and not monetary policy and banking, our Terms of Reference focus on ECCU member states.
- ***Telecommunications:*** We review the ECTEL telecommunications framework because telecommunications could be a natural subject matter candidate for expanding the remit of existing laws and the mandates of ECTEL and the national telecommunications regulatory authorities (although only five OECS members are members of ECTEL).
- ***Consumer protection:*** Like telecommunications, this area of law is a natural candidate for expanding remits to include data protection, and so we review the framework of consumer protection laws in the region.

- ***New treaty:*** The region has extensive experience developing new regulatory frameworks using treaties and national laws. We thus review the possibility of preparing an entirely new treaty, which could take the form of the ECCB Agreement and ECCU Banking Act or the ECTEL treaty and national telecommunications laws.
- ***Model law:*** The region also has experience developing model laws for adoption by member states, not least the OECS Model Bill, but also the Electronic Transactions Bill and the Electronic Signatures Bills. We therefore also explore the possibility of preparing a model law that would not itself have legal effect but be intended for adoption in national law by ECCU member states.

7.B OECS Framework

The OECS was established by the Treaty of Basseterre in 1981 and revised in 2013 (the "Treaty"), which serves as its founding charter. The OECS comprises eleven member states of the Eastern Caribbean, and aims to promote economic integration, collective political cooperation, and coordinated foreign policy among its members.

Articles 4 and 5 of the Treaty set out the functions of the OECS and the responsibilities of the member states. Under Article 4, one of the OECS's key functions is to serve as an institutional forum where member states can discuss and facilitate the constitutional, political, and economic changes necessary for their successful development and participation in both regional and global economies.

The Treaty provides for the organs of the OECS. Of these:

- ***The OECS Authority*** comprises Heads of Government of the member states (Article 8.1). It is the supreme policy-making organ of the OECS. The OECS Authority may enact Acts within the sphere of competence of the organization (Article 8.10). It can also issue recommendations and directives (Article 8.11).
- ***The OECS Council of Ministers*** comprises Ministers named by the Heads of Government (Article 9.1). The Council of Ministers is responsible for considering recommendations of the OECS Commission regarding Acts, and for reporting on these to the OECS Authority. The Council of Ministers may also make Regulations and Orders to give effect to Acts adopted by the OECS Authority.

The Treaty also refers to institutions of the OECS, including the Eastern Caribbean Supreme Court, as well as the ECCB and the Eastern Caribbean Civil Aviation Authority (Article 6).

Under Article 5.1, member states are obligated to take all necessary measures – whether general or specific – to fulfil the obligations arising from this Treaty or from decisions made by the OECS's institutions. They must also actively support the achievement of the OECS's objectives. Article 5.2 states that each member state shall take all steps to secure the enactment of such legislation as is necessary to give effect to the Treaty and decisions taken thereunder.

Under Article 5.3:

> *a full Member State which is independent undertakes to enact the legislation necessary to -*
>
> *(i) delegate to the Organisation the said Member State's authority to legislate in the areas of competence of the Organisation outlined in Article 14; or*
>
> *(ii) receive Acts of the Organisation made by the OECS Authority, and Regulations and Orders made by the Council of Ministers, from the Organisation in the areas of competence of the Organisation outlined in Article 14;*
>
> ***with the intention that the Acts, Regulations and Orders have a direct effect in the laws of the Member State****;*

Article 14 of the Treaty sets out of OECS's legislative powers. Under Article 14.1, Member States agree to accord to the Organisation, under Article 5.3 and subject to Article 5.4, legislative competence in certain areas:

> *(a) common market including customs union;(b) monetary policy, the competence in this category to be exercised on the recommendation of the Monetary Council; (c) trade policy; (d) maritime jurisdiction and maritime boundaries; and (e) civil aviation, the competence in this category to be exercised on the recommendation of the Board of Directors of the Eastern Caribbean Civil Aviation Authority; provided that a Member State need not take steps to repeal its laws in relation to such matters (which laws are otherwise compatible with this Treaty) in advance of the enactment of any Act of the Organisation, but shall refrain with effect from the date of coming into force of this Treaty from enacting any new legislation in relation to such matters save with the approval of or under powers delegated by the OECS Authority.*

Under Article 14.2, the legislative authority of the OECS is further extended:

> *The Member States agree to accord to the Organisation under Article 5.3 and subject to Article 5.4 legislative competence in relation to – (a) common commercial policy; (b) environmental policy; and (c) immigration policy; reserving their right to legislate in relation to those matters within aspects of such policy not pre-empted by or under the authority of any Act of the Organisation.*

Under Article 14.3:

> *In the areas of legislative competence of the Organisation which do not fall under Article 14.1, the Organisation shall enact Acts of the Organisation only if and in so far as the objectives of the proposed action cannot, in the opinion of the OECS Authority, be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the proposed action, be better achieved by enacting an Act of the Organisation.*

It would not be unreasonable to take the view that data protection is so fundamental to the functioning of the digital economy that harmonized legislation is essential to the development of the common market. This would provide a basis under Article 14.1(a) for the adoption by the OECS Authority of an Act on the protection of personal data. There might be a view that data protection would be a matter of common commercial policy under Article 14.2 and so within OECS legislative competence, but with reservation of national legislative powers unless an OECS Act is enacted. To the extent that data protection were not to be viewed as sufficiently within the legislative competence under Article 14.1, it could be argued (and disputed) that the scale and effects of legal and regulatory integration in data protection can only be sufficiently achieved by an OECS Act under Article 14.3.[5]

On the terms of Article 5.3, an OECS Act would be expected to have direct effect in the laws of the member states. We understand that the meaning of "direct effect" has not been the subject of any definitive decision of the OECS institutions, including the Eastern Caribbean Supreme Court.[6] A reasonable interpretation, indeed the plain meaning, of "direct effect in the laws of member states" would be that an OECS Act has effect in national law, i.e., would be enforceable in a national court without requiring an intervening step.

Whether an OECS Act would also have precedence over a national law (i.e., that an OECS Act would prevail in case of conflict, including if a subsequent national law conflicted with a prior OECS Act) is unclear. The reference in Article 14.2 to pre-emption by OECS Acts and the limitation of the reservation of national legislative power in that Article could suggest that, on the terms of the OECS treaty, OECS Acts would indeed pre-empt national laws.

Regardless of the question of precedence and pre-emption, however, the very notion of "direct effect" itself appears not to have been accepted by member states. We have reviewed the national laws of the member states that adhered to the Treaty as revised in 2013. All but one derogated in their national laws from Article 5.3. Their national laws provide that Article 5.3 shall *not* have the force of law in their respective countries. As a result, while the countries committed in signing the Treaty to enact legislation to give direct effect to

[5] To reach this determination, the OECS Authority would assess the necessity for regional data protection legislation by evaluating factors such as cross-border data flows, the risk of large-scale data breaches, and the benefits of unified standards for the digital economy. Recognizing the interconnected nature of data management and its significant economic implications, the Authority could determine that a centralized data protection framework is essential.

[6] See, Zachary Allen Roy Phillips, Interpretation of the Meaning of 'Direct Effect' in the Revised Treaty of Basseterre, *International Community Law Review* 21 (2019) 147–169.

OECS Acts, Regulations and Orders, they largely declined to accept this when they legislated to give effect to the Treaty in national law.

We have been unable to locate any OECS Act issued pursuant to the OECS legislative procedure. This apparent lack of use of the legislative mechanism, combined with the lack of direct effect, suggests that the adoption of an OECS Act is unlikely to be embraced as a means of legal and regulatory harmonization of data protection among OECS (or ECCU) member states.

7.C The ECCB/ECCU and ECSRC frameworks

After prior cooperation, seven OECS member states agreed in 1981 to establish the Eastern Caribbean Central Bank (ECCB) and deepen economic integration through the Eastern Caribbean Currency Union (ECCU). Today, eight OECS member states are members (British Virgin Islands (BVI), Guadelupe and Martinique are not). The participating states entered into a treaty, the ECCB Agreement of 2016, providing for collaboration in central banking and credit. The ECCB Agreement was adopted and enacted into national law as the ECCB Agreement Act by each participating state's national legislature. In parallel, the national legislatures also enacted the ECCU Banking Act of 2015.

The combination of the ECCB Agreement treaty and these national laws comprise the legal framework that empowers the ECCB to formulate and implement regulations essential for the effective governance and stability of the ECCU. This establishes its own regional framework in that it operates on its own terms. While connected to the OECS, legislation made under the ECCB Agreement and Acts are not OECS Acts, Regulations or Orders.

Under Article 45 of the ECCB Agreement, the ECCB is authorized to issue regulations necessary to give effect to the provisions of the Agreement. Article 45(1) states:

> *The Bank may make such regulations as may be required from time to time for giving effect to the provisions of this Agreement.*

This broad authority allows the ECCB to address emerging financial and monetary issues by creating regulations that support the objectives of the ECCU.

Article 45(2) further provides:

> *Regulations made by the Bank shall have full force and effect when all steps have been taken as are necessary to give legal effect to them in each of the territories. All regulations made by the Bank shall promptly be published in the Official Gazette of each of the Participating Governments and notified to the public in such other manner as the Bank shall decide.*

The ECCB holds significant regulatory authority over financial institutions within the ECCU, including ensuring financial stability, regulating banking operations, and overseeing monetary policy. It acts as the central regulatory authority, issuing and enforcing regulations under the Banking Acts adopted in national laws (see Section 3.B.6 of this report) and the ECCB Agreement. The ECCB is empowered to issue regulations that apply specifically to licensed financial institutions, including banks, credit unions, and insurance companies, to maintain uniform standards and protect the integrity of the financial system. It requires all licensed commercial banks and banking institutions to comply with standardized financial practices. It conducts regular supervision through mandatory financial reporting and periodic inspections to assess the performance, risks, and asset quality of these institutions. Additionally, the ECCB provides guidance and technical support to national regulatory bodies, facilitating the harmonization of banking standards and practices with global good practices.

ECCU member states are required to adopt ECCB regulations within their national legal frameworks by enacting or amending relevant legislation. Once adopted, regulations must be published in the national Official Gazette and made accessible to the public. This process ensures that ECCB regulations have legal standing and can be effectively enforced within each territory.

The member states do not have their own national financial regulatory authorities as counterparts to the ECCB.[7] However, additionally, Section 183 of the Banking Act (which was adopted in national law by ECCU member states) provides:

> *The Minister* [Minister responsible for finance in the respective country] *upon the recommendation of the Central Bank may make Regulations as may be required from time to time for giving effect to the provisions of this Act […]*

The institutional framework, then, consists of a combination of the (regional) ECCB and (national) Ministers. This collaborative arrangement should help ensure that the ECCB's regulatory initiatives are supported at the governmental level, facilitating seamless integration into national legal frameworks. However, the ECCB is the principal regulatory authority and, as mentioned above, its regulations are required to be adopted into law in each country.

The ECCB issued the Policy Considerations document discussed in Section 3.A.2. That document is framed as setting out an approach to harmonized data protection legislation across all economic sectors in member states, not only the financial sector. It has not been suggested that the region-wide data protection law would be issued under the ECCB and ECCU legal framework.

That said, the ECCB may and does implement data protection standards within the financial sector it oversees. For instance, the proposed Payment System and Services Act, which we understand has not yet been adopted, includes a brief data protection provision requiring payment service providers to protect personal data.

It is unlikely that member states would wish to append a general economy-wide data protection role to the mandate of the ECCB, as it is a financial authority. Nevertheless, the ECCB Agreement could serve as an example if designing a regional data protection authority, as discussed in Section 6.A.2.

A framework similar to the ECCB was established for the Eastern Caribbean Securities Regulatory Commission (ECSRC). An Agreement Establishing the ECSRC was entered into among ECCB member states in 2000, and updated in 2020. The member states then enacted nationally a Securities Act that gave the ECSRC legal status and regulatory powers in their countries, including licensing and enforcement.

7.D ECTEL framework

Although telecommunications are not explicitly mentioned in Article 14.1 or 14.2 of the Treaty of Basseterre (See Section 7.B of this report), the OECS can facilitate legislation through regional agreements and the adoption of common policies under the broader scope of Common Commercial Policy. The telecommunications sector serves as an example of a sector in which the OECS has facilitated legislation.

The Eastern Caribbean Telecommunications Authority (ECTEL) was established by the Treaty Establishing the ECTEL, signed in 2020 by five members of the OECS: Dominica, Grenada, St. Kitts and Nevis, Saint Lucia, and St. Vincent and the Grenadines. It thus covers only just over half of the members of the ECCU and OECS. It comprises its own regional framework in that it operates on its own terms, and legislation made under it is not OECS Acts, Regulations or Orders.

The treaty was signed in response to the need for a more coordinated and efficient regulatory framework for telecommunications services in the Eastern Caribbean. These countries sought a harmonised regulatory approach to promote fair competition, protect consumers, and stimulate economic development in the sector. ECTEL, the regional authority, was established under treaty with the support of the OECS Telecommunications Reform Project. The ECTEL Treaty has been amended from time to time.

[77] The legal and institutional framework for monetary policy and banking regulation (and other financial services) for which the ECCB is responsible is distinct from that for *offshore* financial services. These are regulated in each member state at a national level by national regulatory authorities (e.g., St. Lucia's Financial Services Regulatory Authority) under national laws (e.g., St Lucia's Financial Services Regulatory Authority Act and International Banks Act). The national authorities have a connection with the ECCB in that the latter appoints a board member to the national authorities, but overall, the ECCB regime deals with financial services in the region as opposed to provision of offshore services, i.e., they are different regulatory frameworks for separate markets.

Under Articles 1 and 2 of the Treaty, contracting states undertake to:

> *put in place all the appropriate measures, including the enactment of the appropriate legal and regulatory framework to promote the purpose of the treaty, the performance of their obligations under the Treaty,*
>
> and also, to
>
> *put in place in their respective jurisdictions a telecommunications regulatory body to be known as the National Telecommunications Regulatory Commission, which shall co-ordinate and liaise with the ECTEL.*

The institutional model differs from that of the ECCB because it expressly intends for ECTEL to have a national authority counterpart in each country. ECTEL's role under Article 5 of the ECTEL Treaty largely concerns recommending policies, standards, procedures, licences, fees and other matters to the national authorities, and coordinating with them.

The implementing legislation for the ECTEL Treaty was enacted in each of the Contracting States as the legal framework for telecommunications, either by a standalone ECTEL Act or embedded in the Schedule of its Telecommunications Act. ECTEL operates in close collaboration with national telecommunications regulatory authorities within each contracting state. These national bodies are responsible for the direct implementation and enforcement of ECTEL's regional policies within their jurisdictions.

Typically, the national Minister is responsible for making regulations and issuing the more important ("individual") licences after receiving the advice of ECTEL. The national telecommunications authorities have the powers to issue a variety of procedures and rules, and the less important ("class") licences, and to authorize various matters (e.g., equipment). The national authorities have powers in various regulatory matters such as interconnection and universal service, but acting pursuant to the recommendation of ECTEL. ECTEL is authorized to conduct licence tenders for individual licences and giving recommendations to the Ministers on their issuance. ECTEL manages all radio spectrum for the contracting states, and receives applications for spectrum licences. (See Article 11 of the Treaty.)

There is, then, an allocation of functions among ECTEL at the regional level and the national authorities and Minister. This gives ECTEL an important role in strategically important matters (individual licences) and those having a regional dimension (spectrum). The national authorities in turn manage the bulk of day-to-day regulation, much of it under the guidance of ECTEL. The national authorities are also responsible for enforcement of the law at national level, having powers to appoint inspectors.

It would theoretically be conceivable for the ECTEL framework to be expanded to add data protection. There is a reasonably close relationship between telecommunications and data protection. Each deals with technology and privacy. In many ways, the allocation of functions between national and regional bodies in the ECTEL framework is attractive for the requirements of data protection. (See Section 6 of this report). However, the ECTEL framework has the important drawback that only five states participate in it. This may also indicate the limits of states' readiness to cede powers to a regional body in this manner.

7.E Consumer protection

Data protection has much in common with consumer protection. Both concern protection of the individual who is often in a weaker position than those collecting and otherwise processing data about him or her in ways that are beyond his or her control and understanding. Indeed, in some countries, such data protection law arises from application of consumer protection laws. The US Federal Trade Commission (FTC) has brought many data protection- and privacy-related cases under section 5 of the Federal Trade Commission Act, which protects consumers against unfair and deceptive practices.

It is thus worth considering whether the ECCU member states' consumer protection framework could be a basis for data protection law – whether by using the consumer protection framework as an example when designing the data protection framework, or by building data protection onto the consumer protection framework itself.

There is, however, no legal and regulatory framework for consumer protection in the OECS or ECCU at the regional level. There are exceptions to this, such as consumer protection in banking and other financial services under the ECCB's mandate, and to some degree in telecommunications under ECTEL. (Even in the case of ECTEL, consumer protection is largely addressed by the national telecommunications regulatory authorities and not under the regional agreement or by the regional authority ECTEL.) The member states have enacted their own national consumer protection laws, ranging widely in age and content, though typically providing for a national Department of Consumer Protection having powers to hear complaints and investigate violations.

There is little by way of provision for regional cooperation in the national consumer protection laws. Section 138 of the St Lucia Consumer Protection Act of 2016 provides that the Minister responsible for administering the Act may cooperate with similarly authorized consumer protection authorities in other member states to establish a regional alert system for defective goods. This is a very basic level of cooperation.

Thus, the approach to consumer protection is not particularly useful for developing data protection, whether to be coopted for that purpose or to serve as an example.

7.F New framework under a regional data protection agreement

A new regional data protection framework could be prepared and introduced under a binding agreement among states willing to adopt it. It could be prepared among ECCU member states or the broader OECS member states. Following the approaches taken in the region, it could comprise a harmonized data protection agreement which would establish consistent personal data protection standards across the region. It could create a regional agency that would have a role in overseeing implementation, compliance monitoring, and dispute resolution.

This could be similar to the centralized regional form of the ECCB (see Section 7.C of this report) or provide for a combination of regional and national agencies (see Section 6.A.2 of this report). The agreement would set out the division of functions between the regional and any such national authorities. The agreement would be adopted into national laws, with scope for derogations in certain areas to allow countries flexibility if they are so required. The national laws previously adopted would all be repealed and replaced in their entirety with the new legislation.

Such a harmonized framework would be intended to enhance regional trust, facilitate the free movement of data, attract investment, align the ECCU with global good practices, foster economic integration, improve global competitiveness, and ensure consistent and effective data protection across the region.

7.G Model law for willing countries

An alternative approach would be for those countries, a coalition of the willing, to work through the ECCU or OECS institutions on a model data protection law that they would each intend to adopt in national law but without a formal agreement committing themselves to do so. The model would be a new and improved version of the OECS Model Bill, updating it to complete the gaps identified in Section 3.A.1 of this report, and in the national data protection laws reviewed in Section 4 (summarized in Section 5.A).

This approach would have the merit of flexibility and speed. However, without a formal agreement among the countries or a regional agency, it would lack the regional element that is important to enable trusted cross-border data flows and arrangements for resolving jurisdictional duplication and conflicts discussed in Section 5.B of this report.

7.H Overview of the frameworks

The table below summarizes the benefits and drawbacks of each of the relevant existing frameworks in the region, as well as the option of developing a new treaty agreement or a model law.

Table 2. Appropriateness of existing regional frameworks

	OECS framework	ECCU/ECCB	ECTEL	Consumer protection	New treaty	Model law
Coverage of member states	All OECS and ECCU member states covered	All ECCU member states covered (BVI not covered)	Only covers five OECS/ECCB member states (excludes Antigua and Barbuda, Anguilla and Montserrat)	Most if not all ECCU member states have a consumer protection law	Would be adopted by those choosing to commit	Would be adopted by those choosing to adopt the model law
Legal framework	Robust framework on paper, but OECS Acts are not given direct effect in national laws and appear not to be a mechanism.	Strong legal framework with track record.	Robust and carefully designed legal framework with reasonably arranged powers at regional and national levels.	National laws are in place and would have only to be amended to add data protection responsibilites. But there is no regional law.	Would have to be developed and negotiated formally. Could be modelled on ECCB, ECTEL or another approach.	Unclear what obligation member states would have to adopt it. Would apply at national level only. The partial adoption of the previous OECS Model Bill is not encouraging (some states did not enact the law, others had only part enter into force)
Institutional framework (regional and national)	Robust regional institutions and organs.	Strong and tested central authority of the ECCB.	Carefully orchestrated combination of central guidance from ECTEL and implementation and enforcement by national authorities.	Consumer protection departments have already been established in most countries. No regional institutional framework beyond OECS Commission's general regional integration activities.	Would have to be developed from scratch. Could provide for a regional authority (like ECCB) or a combination of regional and national authorities (like ECTEL)	Would only provide for establishment of national authorities, i.e., no regional body. Track record of the previous OECS Model Bill is not promising with states not setting up the data protection authorities.
Potential mandate for data protection	Potentially covered under the common market mandate in Article 14.1.	None beyond the financial sector.	None beyond the telecommunications sector, but the scope could be expanded to cover data protection (as other countries have done).	Currently no mandate, but consumer protection could be expanded to cover data protection.	Would be set in the new treaty.	Would be set in the laws adopted.

8 Conclusions

8.A Findings

8.A.1 Gap analysis

We reviewed international good practices in data protection law in Section 2. We considered the OECS and ECCU regions' various legal frameworks in terms of alignment or not with such practices in Section 3. We then considered the ECCU member states' laws on data protection and laws in various economic sectors in Section 4, evaluating them in light of international good practice in data protection described in Section 2.

We summarized the weaknesses of the regional frameworks and national laws in Section 5. We noted in Section 5.A their gaps in substantive data protection law (obligations and rights) compared with international good practices. We focused then in Section 5.B on the cross-border dimension of these laws. We considered the lack of provisions on cross-border data flows, the varying level of maturity of different countries' laws, and differences among those that had introduced data protection laws. We concluded in Section 5.C that the combination of the gaps identified will result in important impediments to the flow of personal data in the region, and to the growth of a regional digital economy.

8.A.2 Considerations in approaching the gaps

In Section 6, we took a step back to consider how to approach the gaps identified. We discussed in Section 6.A the legal nature of data protection law and the implications for institutional design. We considered the possibilities of dealing with data protection through:

- national authorities only;
- a regional authority; or
- a combination of national and regional authorities.

We noted the difficulty of achieving regional integration and inefficiencies of relying only on national authorities (like the current approach to consumer protection). We noted also the benefits and challenges of relying solely on a regional authority (like the ECCB in banking) as well as the alternative of relying on a combination of national and regional authorities (like ECTEL and the national telecommunications authorities).

We observed in Section 6.B that not all functions of a data protection authority involve the exercise of legal powers and legal enforcement of legal obligations. As a result, it may be possible to distribute some roles between regional and national authorities depending on which is expected to exercise direct legal authority as opposed to providing guidance, carrying out promotional and advocacy activities, or resolving inter-jurisdictional issues. (ECTEL is an example of this approach.)

We also observed in Section 6.C that, while internationally common, it is not necessary for data protection functions to be placed only in an authority focused solely on data protection. Agencies dealing with adjacent subject matters, such as telecommunications or consumer protection, might be better placed than establishing a new data protection authority.

8.A.3 Relevant existing regional frameworks

Having identified the gaps and set out considerations for approaching them, we explored in Section 7 the existing legislative frameworks in the region. We did this in order to understand whether any of them is suitable to be, or could serve as an example for, a harmonized data protection framework.

We found that an OECS Act made under the OECS Treaty appears not to be viable because it is not the administrative practice to adopt such Acts, and even if it were, the national authorities would not accept it as having direct effect.

We found that the ECCB/ECCU framework itself is not suitable for addressing data protection. It is limited to monetary and financial services matters and it is unlikely that its member states will wish to make the ECCB responsible for economy-wide data protection (as opposed to only in the financial sector). However, the ECCB framework could serve as a model for a centralized regional approach in data protection if that were preferred.

We also found that the ECTEL framework itself is not suitable, even if it has some attractions. One could add data protection to the mandates of ECTEL and the national telecommunications authorities, and establish complementary regional and national roles. However, ECTEL comprises only five member states. Thus, ECTEL serves more as an example for an approach involving a combination of regional and national authorities.

The current approach to consumer protection does not offer much at this time because it comprises only national laws and national authorities (and these are only ministerial departments). Even if national laws were introduced and expanded national institutional mandates, the important regional integration dimension would be lacking.

In our view, the preparation of a model law alone for willing countries to adopt and build national authorities would not sufficiently result in a harmonized data protection framework. There would be no assurance that they would adopt it. Even if all countries adopted an identical law, there would be inadequate provision for the cross-border dimension of data flows and regional integration.

Simply providing for national authorities acting under identical national laws is insufficient to achieve the intended outcome. Even if the role of data protection is bundled with an existing national institution (e.g., a telecommunications regulatory authority or a consumer protection authority), it is vital for the countries to face the international market in a consistent and coordinated manner. This requires a regional element.

8.B Recommendations

In order to achieve an effective single digital economy with a common approach to data protection enforced consistently in all jurisdictions, we recommend that the solution include a regional body. This will be important for dealing with outsourcing of processing to firms abroad (e.g., foreign vendors and cloud services) and for data controllers and processors providing services from outside the region (e.g., social media and many other apps). It will be particularly important to streamline enforcement where more than one member state is involved, avoiding the duplication by national authorities of guidance and enforcement relating to the same behaviour.

At the same time, it is useful and in some cases may be necessary for the solution to include a significant national component in the legislative and institutional framework. This may be valuable in ensuring political legitimacy with member states and proximity to data subjects seeking enforcement.

We suggest adopting one of three approaches described in the following sections.

8.B.1 Option 1 – Regional authority with satellite offices

Under Option 1, a regional institution is provided for pursuant to a regional agreement among participating member states in a manner similar to the ECCB. Under the agreement, each member state undertakes to adopt a national law in the form of a bill appended to the agreement. The national law creates harmonised obligations for data controllers and processors, and rights for data subjects.

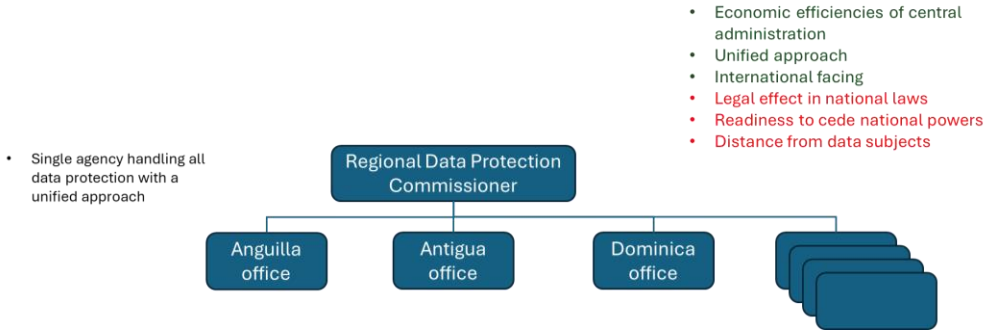
The agreement and national law provide for a regional institution to be the enforcement authority for data controller and processor obligations and data subject rights. As with the ECCB, the regulations and enforcement activities of the regional authority have force in national law. If necessary, the regional agreement could provide for some domestication steps (e.g., registration of its regulations and decisions in the national gazette), although this may create inefficiencies and risks enforcement delays and possible enforcement gaps.

The regional institution has national satellite offices (branches) in participating member states. These receive complaints from data subjects in the relevant member state, conduct local promotional and advocacy efforts, and liaise with data controllers and processors in the member state. Where required for the purposes of a member state's national law or political preference, the satellite office (branch) may be a legally separate entity controlled by the regional institution, but with legal personality to enable it to sue (and be sued) under national law in national courts.

The regional institution has a governing board on which each member state has representation, alongside the ECCB and any other institutions as agreed among the member states (e.g., ECTEL). There are two broad options for the regional institution's establishment:

- The regional institution could be a new standalone body, with all of its legal existence and governance set out in the regional agreement, much as how the ECCB and the ECSRC were established. It could have its own governance structure and be funded by annual contributions from those member states that sign up to it, possibly supplemented by the proceeds of any fines it levies. The OECS Commission could also have representation on the governing board.
- The regional institution could, alternatively, be a directorate (or department or unit) of the existing OECS Commission within the existing OECS legal framework. Its powers in data protection would be set out in the data protection agreement and national laws, but its legal existence would be already provided for in the Treaty of Basseterre. Its budget could be funded as part of the OECS Commission budget. The appointment, accountability and other governance features of the directorate within the OECS Commission would be provided for in a manner appropriate for its enforcement function. This would mean the OECS Commission having an enforcement role alongside the OECS Commission's traditional administrative role. This could work in a similar manner to the way the European Commission's Directorate General for Competition (DG-COMP) functions in pursuing competition law enforcement.

Figure 17. Option 1 - Regional authority with satellite offices



Option 1 achieves harmonized national laws and uniformity of enforcement, political legitimacy from national representation on the board, and in-country proximity to data subjects. It has the efficiency of a streamlined regional institution with local presence through its in-country satellite (branch) offices.

However, Option 1 also involves a sizeable budget commitment to a regional institution. This may in the end be significantly more economically efficient than the duplication of having multiple national authorities, but it is often challenging to build sufficient consensus for devotion of national resources towards regional institutions. Option 1 also results in an institution with less direct connection with national populations than having national institutions. Whether this presents a concern depends on how strongly the member states consider national sovereignty and how willing they are to pass responsibility for such matters to a regional body.

8.B.2 Option 2 – Combination of a regional and national authorities

As in Option 1, a regional institution is provided for pursuant to a regional agreement among participating member states. Under the agreement, each member state undertakes to adopt a national law in the form

appended to the agreement. The national law creates harmonised obligations for data controllers and processors, and rights for data subjects.

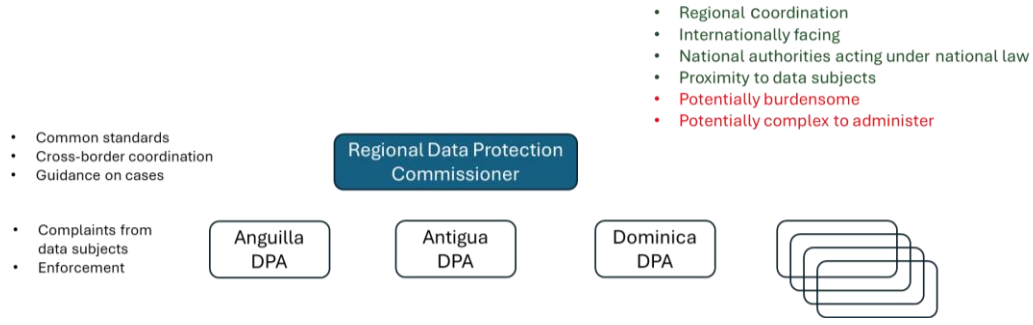
Unlike Option 1, but with similarities to ECTEL, the regional institution works alongside national authorities established under each member state's respective national law. The regional agreement and national law allocate functions, powers and duties between the regional institution and national authorities. The regional institution has no direct enforcement power in national law and before national courts except in the regional cases mentioned below.

Each national authority is appointed by the national government and is accountable to and subject to governance of the national law and courts. The regional agreement and appended bill could leave it open to national policy makers and legislatures to choose whether the national authority would be a new agency or whether the powers and functions could be assigned to an existing agency (such as a national telecommunications authority). It receives complaints from data subjects in its country and enforces the obligations of data controllers and processors in the country. The national authority conducts local promotional and advocacy efforts, and liaises with data controllers and processors in its member state. For this purpose, it draws on the regional institution.

The regional institution has the following functions:

- The regional institution coordinates and manages data protection cases that involve more than one member state. This includes any investigations of international controllers and processors whose services and practices are similar in more than one member state, such as social media, and other digital service and cloud providers. It also covers processing by a controller or processor in one member state of personal data of a data subject in another member state. The regional institution guides the national authorities' requests for information and initiation of investigations and enforcement proceedings, and coordinates and allocates the imposition of penalties in such cases. National authorities apply the regional institution's guidance in such multi-member state cases. Purely domestic cases are left to the national authorities.
- The regional institution is also the outward facing body for such international data controllers and processors, giving them a single point of contact for information about data protection law in the region, and confidence in a harmonised approach. It also participates in international organizations' data protection activities.
- The regional institution issues guidance to national authorities, controllers and processors on the details of application of data protection law. These cover the full range of data protection law in order to ensure a harmonized approach to enforcement across all member states. This may include, for example, guidance on the requirements of consent of data subjects to process personal data about them, privacy requirements, data security measures, data breach notification requirements, and data privacy impact assessments. It may cover health, education, commerce and other vertical economic sectors.
- The regional institution also provides centralized training and advocacy support to the national authorities.

Figure 18. Option 2 - Combination of a regional and national authorities



As in Option 1, the regional institution could be an entirely new body, with all of its legal existence and governance set out in the regional agreement and the national law. It could, alternatively, be a directorate (or department or unit) of the existing OECS Commission within the OECS legal framework.

Like Option 1, Option 2 achieves harmonized national laws and uniformity of enforcement. It has political legitimacy from national representation on the regional institution's board, the legal establishment of national authority and its in-country proximity to data subjects. Option 2 favours national sovereignty concerns in providing for national authorities. However, it is considerably more complex, less efficient, and more costly than Option 1. It runs a significant risk that national authorities are not established, as was the case with those countries that did previously enact national legislation.

8.B.3 Option 3 – National authorities with regional coordination

Option 3 retains the bare essential roles of a regional institution while minimizing its scale and scope, and relying largely on national authorities for the activities of data protection enforcement and promotion. Here, national authorities have full powers over all matters. The regional institution only acts as a sort of facilitator-adjudicator coordinating designation of the lead authority in cases involving multiple countries.

As in Options 1 and 2, a regional agreement is entered into among participating member states under which each member state undertakes to adopt a national law in the form appended to the agreement. The national law creates harmonised obligations for data controllers and processors, and rights for data subjects.

The agreement and each national law provide that where a matter involves more than one participating country, one national data protection authority will lead the case (the "lead authority"). Such cases might involve cross-border data transfers between participating countries within the region, or a global controller or processor from outside the region serving multiple countries (e.g., media, social media, search, AI chatbox, clouds services, or other services).

Unless the participating countries agree otherwise, the lead authority would be the one in the location where the data controller or processor is established or has its principal administration in the region. If the data controller or processor has no such presence in the region, then the lead authority could be the authority in the country having the largest number of data subjects likely to be affected by the processing. (This has the disadvantage that it will tend to result in larger countries repeatedly taking the lead, but it is the simplest approach and places the burden on the larger countries, and countries would be at liberty to agree otherwise.)

Any national authority identifying an enforcement action that may involve more than one participating country would notify the matter to the regional institution. The regional institution would act as a secretariat for consultation with national authorities and facilitating the designation of the lead authority. It would indicate the lead authority for the case in accordance with the criteria for designation.

The process and criteria for designation of the lead authority, and the role of the regional institution, would be set out in the regional agreement and national laws. This would be binding on national authorities. In case of objections or disputes, the regional institution would provide its opinion, and this would be binding under the national law in each country.

The lead authority would carry out the investigation in close cooperation with national authorities of the other member states to ensure it addresses violations and compliance in every relevant country. It would consult with the other national authorities on its findings, giving them an opportunity to comment and supply information and evidence. It would also consult with them on appropriate remedies, including fines. It would consult with the national authorities on any orders to be issued, such as orders requiring controllers or processors to take or refrain from taking actions, or to pay a fine. The lead authority would have power to impose interim remedies, for example ordering a controller or processor to cease certain processing that

appears on its face (but subject to investigation) to violate the data protection laws and causes irreparable harm.

Under mutual recognition provisions in the regional agreement and by operation of each country's national law, the other national authorities and courts would be required to recognise and enforce the lead authority's decisions in their respective jurisdictions.

Fines received could be applied first to cover the costs of the lead authority relating to the relevant investigation, and then to the regional institution towards its costs of its facilitation and adjudication functions. Any surplus could be distributed among the national authorities. The distribution could be set automatically according to a simple objective criterion such as population size or, with a little more complexity, according to the estimated number of data subjects affected by the case in each country. Alternatively, the regional institution could allocate the remaining amount of the fine among authorities with a view to developing capacity and a sustainable enforcement system.

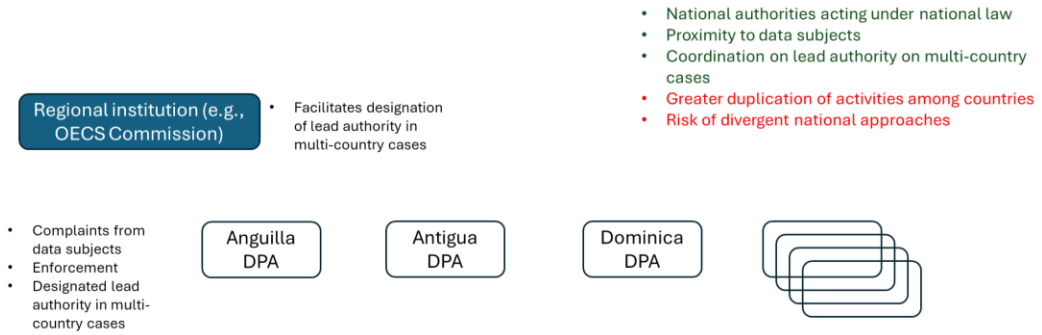
If agreed among national authorities (including sufficient allocation of budget), the regional institution could also play a support role to national authorities in various ways:

- supporting and coordinating among national authorities in an investigation, such as requesting and gathering evidence;
- developing regulations for adoption by national authorities;
- developing best practice guidelines on the application of the national data protection laws; and
- facilitating training and capacity building.

These activities would only be carried out by the regional institution if budget allows and national authorities agree.

The regional institution could be a new organisation set up for this specific role, but its limited functions makes it far more sensible to use an existing institution. The most obvious candidate would be the OECS Commission because it already deals with numerous aspects of regional economy and legal harmonisation.

Figure 19. Option 3 - National authorities with regional coordination



Option 3 maintains regional harmonisation. It does not have the overall efficiencies of a regional institution acting alone (with satellite offices) under Option 1 or playing the substantial role under Option 2. However, it has the benefit of respecting national sovereignty and a presenting light load at regional level. As time passes, and as confidence grows (and with it regional budget), the role of the regional institution could be upgraded.

8.B.4 Summary of options

The following summarises the options described above:

	Option 1	Option 2	Option 3
Regional level			
Regional institution	Yes	Yes	Minimal role
Regional institution's "hard law" enforcement role and powers	Regional and national cases	Leads and coordinates cases involving more than one member state	Coordinates among national authorities in cross-border cases, and adjudicates if there is disagreement on which should be the lead authority
Regional institution's "soft law" roles	Issues guidelines, provides advocacy and training	Issues guidelines to national authorities which they will enforce, provides advocacy and training	Minimal unless requested by national authorities and budget is provided
Regional institution's legal basis	Either a new standalone institution funded by member states, or a division of OECS Commission funded from the OECS Commission budget		OECS Commission
Regional institution's governance	Member state and ECCB representation on a supervisory board		OECS Commission
National level			
National authority	None, but regional institution has satellite (branch) offices in member states	Yes, enforcing purely domestic cases, and accepting regional institution's coordination and leadership in multi-member state cases	Yes, enforcing purely domestic cases, and accepting regional institution's coordination and decisions of the lead authority in multi-member state cases
National authority's "hard law" enforcement role and powers	N/A	Enforcement powers under national law	Enforcement powers under national law, and mutual recognition of the lead authority's decisions
National authority's "soft law" roles	N/A	Accepts and promotes regional institution's guidelines, advocacy and training	Full role in advocacy and training but allowing for reliance on the regional authority if budgeted
National authority's legal basis	N/A	Established under national law, may be an independent authority or could be the national telecommunications or consumer protection authority	
National authority's governance	N/A	According to national law and the form of the authority	

The selection of approach is a matter for the client and member states to discuss and agree in light of:

- countries' appetite to authorise a regional authority with legal powers effective in national laws;

- countries' preference to maintain legal powers at the national level and their readiness to fund and implement national authorities;
- the possibility of establishing a new standalone regional body or assigning data protection responsibilities to the OECS Commission; and
- the possibility of assigning data protection roles to existing national authorities such as telecommunications or consumer protection.

9 Annex: Matrix of legal instruments reviewed

9.A Regional framework

- Data Protection
  - OECS Model Bill of 2016
  - Policy Considerations for the Development of Policy Considerations for the Development of Data Protection and Privacy Legislation in the Eastern Caribbean Currency Union (ECCU)
- Cybersecurity & Cybercrimes
  - N/A
- Consumer Protection
  - Payment System and Services Bill of 2024
- Freedom of information requests
  - N/A
- Health
  - Department of Health Services Act of 2024
- Education
  - N/A
- Financial Services (including digital financial services)
  - Banking Act of 2015
  - Credit Reporting Bill of 2016
- National Identification (including digital and functional forms)
  - N/A
- Passports
  - N/A
- Civil registration
  - N/A
- Electronic communications
  - Telecommunications Act of 2006 (revised in 2020)
- Electronic transactions
  - Electronic Transactions Act of 2011
- E-signatures
  - Electronic Evidence Act of 2011

9.B Anguilla

- Data Protection
  - N/A
- Cybersecurity & Cybercrimes
  - N/A
- Consumer Protection
  - N/A
- Freedom of information requests
  - N/A
- Health
  - Department of Health Services Act of 2024
- Education
  - N/A
- Financial Services (including digital financial services)
  - Financial Services Commission Act of 2022 (Cap F28)
- National Identification (including digital and functional forms)
  - N/A
- Passports
  - N/A
- Civil registration
  - Registration of Births, Deaths, and Marriages Act of 2010 (Cap R35)
- Electronic communications
  - Telecommunications Act of 2004 (Cap T6)
- Electronic transactions
  - Electronic Transactions Act of 2006 (Cap E38)
- E-signatures
  - Electronic Evidence Act of 2022

9.C Antigua and Barbuda

- Data Protection
  - Data Protection Act of 2013
- Cybersecurity & Cybercrimes
  - Electronic Crimes Act of 2013 (amended by Act no 25 of 2018)
- Consumer Protection

  - Consumer Protection and Safety Act of 1988 (Cap 97)
- Freedom of information requests
  - Freedom of Information Act No 19 of 2004
- Health
  - Medical Practitioner's Act of 2009
- Education
  - Education Act of 1973 (Cap 145) (amended by Act No 21 of 2020)
- Financial Services (including digital financial services)
  - Banking Act of 2015
  - Finance Administration Act of 2006
  - Financial Services Regulatory Commission Act of 2013
- National Identification (including digital and functional forms)
  - N/A
- Passports
  - Immigration and Passport Act of 2014
- Civil registration
  - Civil Registration (Vital Statistics) Act of 2020 (No. 6 of 2020)
  - Civil Registry Act of 2019
- Electronic communications
  - Telecommunications Act of 2021 (Cap 423)
- Electronic transactions
  - Electronic Transactions Act of 2013
- E-signatures
  - Electronic Transactions Act of 2013

9.D Dominica

- Data Protection
  - N/A
- Cybersecurity & Cybercrimes
  - N/A
- Consumer Protection
  - N/A
- Freedom of information requests
  - N/A

- Health
    - Medical Act of 1991
    - Hospital and Healthcare Facilities Act of 2002
    - Hospitals Authority Act of 2021
- Education
    - Education Act of 1997
- Financial Services
    - Banking Act of 2015
    - Offshore Banking Act of Dominica of 1996
- National Identification (including digital and functional forms)
    - N/A
- Passports
    - Passport Act of 1978 (Cap. 18.01)
- Civil Registration
    - Registration of Births and Deaths Act (Cap. 35:30) (amended by Act 14 of 1993)
- Electronic Communications
    - Telecommunications Act of 2000
- Electronic Transactions
    - Electronic Transaction Act of 2013
- E-signatures
    - Electronic Transaction Act of 2013

9.E Grenada

- Data protection
    - Data Protection Act of 2023
- Cybersecurity and cybercrimes
    - Electronic Crimes Act No 23 of 2013
- Consumer protection
    - Consumer Protection Act of 2018 (amended by Act no. 5 of 2020)
- Freedom of information requests:
    - N/A
- Health
    - Health Practitioner's Act of 2010
- Education

- Education Act of 2002 (Cap 132 A)

- Financial services (including digital financial services)
  - Banking Act Grenada of 2015
- National identification (including digital and functional forms)
  - N/A
- Passports
  - Passports Act of 1980 (amended by No. 52 of 1991, Act No. 15 of 1993, Act No. 6 of 2001, Act No. 6 of 2011)
- Civil registration
  - Registration of Births and Deaths Act of 1904. (Amended by Act no.10 of 196 & Act no. 45 of 1991)
- Electronic communications
  - Telecommunications Act of 2000
- Electronic transactions
  - Electronic Transactions Act of 2013
- E-signatures
  - Electronic Transactions Act of 2013

9.F Montserrat

- Data Protection
  - N/A
- Cybersecurity & Cybercrimes
  - Penal Code Amendment Act of 2022
- Consumer Protection
  - N/A
- Freedom of Information requests
  - N/A
- Health
  - Public Health Act of 1981 (Cap 14.01)
  - Medical Act of 1937 (Cap 14.02)
- Education
  - Education Act of 2004 (Cap 16.01)
- Financial Services (including digital financial services)
  - Financial Services Commission Act of 2008 (Cap 11.02)
- National Identification (including digital and functional forms)

- N/A

- Passports
  - N/A
- Civil Registration
  - Registration of Births and Deaths Act of 1867 (Cap 6.13)
- Electronic Communications
  - Telecommunications Act of 1949 (Cap 18.07)
- Electronic Transactions
  - Electronic Transactions Act of 2009 (Cap 11.32)
- E-signatures
  - Electronic Transactions Act of 2009 (Cap 11.32)

9.G Saint Kitts and Nevis

- Data Protection
  - Data Protection Act of 2018
- Cybersecurity & Cybercrimes
  - Electronic Crimes Act of 2009 (Cap 4.41)
- Consumer Protection
  - Consumer Protection Act of 2023
- Freedom of Information Requests
  - Freedom of Information Act of 2018
- Health
  - Public Health Act of 1969 (Cap 9.21)
- Education
  - Education Act of 2005
- Financial services (including digital and financial services)
  - Banking Act of 2016 (Cap 21.01)
  - Financial Services Regulatory Commission Act (Cap 21.10)
- National Identification (including digital and function forms)
  - N/A
- Passports
  - Passport and Travel documents Act of 2002 (Cap 6.04)
- Civil Registration
  - N/A

- Electronic communications
    - Electronic Communications Act of 2021
- Electronic transactions
    - Electronic Transactions Act of 2011 (Cap 18.44)
- E-signatures
    - Electronic Transactions Act of 2011 (Cap 18.44)

9.H Saint Lucia

- Data Protection
    - Data Protection Act of 2011 (amended in 2015)
- Cybersecurity & Cybercrimes
    - Computer Misuse Act of 2011 (Cap 8.14)
- Consumer Protection
    - Consumer Protection Act of 2022 (Cap 13.24)
- Freedom of information requests
    - N/A
- Health
    - Health Practitioners Act of 2006 (amended in 2015)
- Education
    - Education Act of 2005 (Cap 18.01)
- Financial Services
    - Banking Act of 2015 (Cap 12.01)
- National Identification (including digital and functional forms)
    - Citizenship of Saint Lucia Act of 1979
    - Elections Act of 2008 (Cap 1.02)
- Passports
    - The Passport Act of 2003 (Cap. 10.03)
- Civil Registration
    - Civil Status Act of 2010 (Cap 4.02)
- Electronic Communications
    - Telecommunications Act of 2000 (Cap 8.11)
- Electronic Transactions
    - Electronic Transactions Act of 2011 (Cap 8.17)
- E-signatures

- Electronic Transactions Act of 2011 (Cap 8.17)

9.I Saint Vincent and the Grenadines

- Data Protection
  - Privacy Act of 2003
- Cybersecurity & Cybercrimes
  - Cybercrime Act of 2016
- Consumer Protection
  - Consumer Protection Act of 2020
- Freedom of Information Requests
  - Freedom of Information Act of 2003
- Health
  - Medical Registration Act of 1886. (Cap 293)
- Education
  - Education Act of 2006 (Cap 202) (amended Act No. 19 of 2010, Act No. 29 of 2016)
- Financial services (including digital and financial services)
  - Money Service Business Act of 2005 (Cap 260)
  - Banking Act of 2015
- National Identification (including digital and function forms)
  - N/A
- Passports
  - Immigration (Restriction) Amendment Act of 2017 (Cap 114)
- Civil Registration
  - Registration of Births and Deaths Act of 1910 (Cap 242)
- Electronic communications
  - Telecommunications Act of 2001
- Electronic transactions
  - Electronic Transactions Act of 2015
- E-signatures
  - Electronic Transactions Act of 2015