POLICY CONSIDERATIONS FOR THE DEVELOPMENT OF DATA PROTECTION AND PRIVACY LEGISLATION IN THE EASTERN CARIBBEAN CURRENCY UNION (ECCU)

EASTERN CARIBBEAN CENTRAL BANK
ST KITTS

Table of Contents

POLICY CONSIDERATIONS FOR THE DEVELOPMENT OF DATA PROTECTION AND PRIVACY LEGISLATION IN THE EASTERN CARIBBEAN CURRENCY UNION (ECCU)

1. PREAMBLE

This document seeks to reflect a revised position of the existing data protection and privacy policy of the ECCU[1] drafted in 2020.

Data can be categorised into many forms and each may also require a certain level of technical or legislative protection. However, for the purpose of this document, the policy's scope or terms of reference is centred on the protection and privacy of personal data.

Data protection and data privacy are often used interchangeably to generally describe the protection of personal data. However, data protection and data privacy encapsulate two interrelated components, i.e., approaches or measures:

(a) to protect personal data, specifically in relation to the diverse forms of processing; and

(b) to safeguard the fundamental right to privacy enshrined in many constitutions, more specifically regarding the right to privacy of an individual's personal data.

The policy considerations for the data protection and privacy (hereinafter referred to as "data protection") policy are based on this underlying perspective.

2. KEY MESSAGES

There is a strong correlation between the need for a data protection legislation and the level of technology use and dependence of a country. As the ECCU moves towards a more digital society a robust data protection regime can serve as a key driver in safeguarding the privacy rights of individuals while fostering innovation and the secure processing of personal data.

[1] Document entitled "Policy Considerations for Data Protection Legislation in the Eastern Caribbean Currency Union"

Data, including personal data, is now recognised as an important business and national asset. In that regard, it requires the necessary legislative safeguards to ensure, among other things, the lawfulness of processing.

Data protection legislation facilitates improved levels of safeguards concerning the privacy of individuals and the protection of personal data through the imposition of certain obligations on businesses and governments while outlining clear rights of an individual and the baseline requirements in processing an individual's data.

The ECCU must take into account its own specific requirements, such as its technological progress supported by insights and lessons from other jurisdictions in the continued development of its data protection regime.

3. BACKGROUND

a. Data is an Asset

The value of data has exponentially increased over the last decade to the extent that data is referred to as the new gold. A significant cause is attributable to technological advances in processing capabilities that gave rise to big data and big data analytics. As a result, companies can easily transform massive structured and unstructured data sets of customer data, financial data and other forms of data, and infer patterns and predict trends. These capabilities directly result in driving increased customer demands, attracting new customers and increasing profitability. The recognition of this viable business and national asset however, is not only by good actors but also by bad actors thus giving rise to increased security and privacy risks to data, particularly personal data.

b. Increasing Threats to Data

Some notable incidents include:

- **Android users**. Over 100 million Android users were exposed as a result of several misconfigurations of cloud services. The threat

actors were able to access sensitive and personal data including names, email addresses, dates of birth, chat messages, location, gender, passwords, photos, payment information, telephone numbers and push notifications.

- **Facebook.** 533 million accounts were affected as a result of a leaked database belonging to Facebook. The leak included the personal data of Facebook users from 106 countries.
- **LinkedIn**. Researchers have reported that the personal data of 700 million LinkedIn users were on sale online, with samples from 2020 and 2021. The personal information included names, telephone numbers, physical addresses, email addresses, geolocation data, usernames, profile URLs, gender and personal and professional experience and backgrounds.

These and other breaches not only accentuate the escalating risks to privacy, irrespective of the location or nationality of the data subjects, but they also highlight the diversity of the types of personal data and the need for strong legislative, technical and organizational safeguards.

c. Notable Sanctions

Since the coming into operation of the EU General Data Protection Regulation (GDPR), there have been hundreds of monetary penalties imposed on data controllers established in the EU member states. Common violations include:

(a) non-compliance with general data processing principles (which are linked to the privacy by design principles[2]);
(b) the insufficient basis for data processing;
(c) the insufficient fulfilment of information obligations;
(d) the insufficient technical and organisational measures to ensure security; and
(e) the insufficient fulfilment of data subject rights.

[2] Refer to sub-section 5.d regarding details on the privacy by design concept.

To date, the highest GDPR fines and monetary penalties have been levied on global corporations such as Amazon, Facebook, Google and Facebook.

Given the embryonic nature of data protection regimes in the Caribbean, the aforementioned obligations and sanctions can serve as useful insights for the ECCU in the development of cogent obligations regarding the processing of personal data and enforcement measures that are ***effective, proportionate and dissuasive***.

d. Policy Implications

There is little doubt that data will continue to be attractive to bad actors. Therefore, there is a strong obligation for governments, other data controllers and data processors to implement appropriate and sustainable measures to detect, prevent and respond to data threats and breaches.

Having regard to data being a key business and national asset, data controllers and data processors must proactively adopt good standards and practices to minimise privacy and security risks to their businesses, customers and employees. Regulation of such requirements and standards is a legitimate expectation of many data subjects.

Thus, safeguarding the privacy interest of citizens as a fundamental human right, subject to certain constitutional restrictions such as national security is paramount. This is increasingly essential as the ability to collect and otherwise process identifiable information of citizens in today's digital society can be done with greater ease or without the individual freely or affirmatively giving permission to collect, or further process their identifiable information.

Having regard to the escalating privacy risks, complexities of data processing and value of personal data, a data protection regime must

contemplate these and other complexities in a technology-neutral manner. Legislative matters to be considered are:

(a) the scope of application of the legislation;
(b) the constituents of "personal data" and "sensitive personal data";
(c) obligations regarding the processing of personal data and the safeguarding of that personal data;
(d) the rights of data subjects in respect of the processing of their personal data;
(e) adequacy of data protection measures; and
(f) effective, proportionate and dissuasive enforcement measures.

Based on the foregoing, the objectives of harmonised data protection legislation in the ECCU should seek to protect the fundamental rights and freedoms of its citizens in respect of the processing of its citizen's personal data, establish baseline standards in respect of data processing, promote improved accountability in respect of the processing of personal data, while signalling the presence of adequate data protection measures.

4. The State of Data Protection Legislation in the ECCU

Data protection laws that were enacted between 2003 and 2018 are likely to have gaps that impede their effectiveness in today's environment.

Table 1: State of Data Protection Legislation in the ECCU

ECCU	Legislative Framework
1. Anguilla	No distinct law
2. Antigua and Barbuda	Data Protection Act, 2013 (No. 10 of 2013)
3. Commonwealth of Dominica	No distinct law
4. Grenada	Data Protection Act, 2023 (No. 1 of 2023)
5. Montserrat	No distinct law
6. St Kitts and Nevis	Data Protection Act 2018 (No.5 of 2018)
7. Saint Lucia	Data Protection Act 2011 (No. 11 of 2011) Data Protection (Amendment) Act (No. 2 of 2015)
8. St Vincent and The Grenadines	Privacy Act 2003 (No. 18 of 2003)

Some countries have encountered challenges in the operationalisation of their laws which underscore the necessity of a harmonised approach to good practice measures to enable the effective working of new laws; and a protection regime to enable the ECCU to experience the full benefits of a digital society while undertaking strong and practical measures to minimise the risks to privacy and the processing of personal data.

5. Policy Considerations

a. General

According to a technical article highlighting the Caribbean's data protection journey[3], countries must take into account certain matters in designing their respective laws:

(a) a clear scope that is reflective of issues such as the extra-territorial nature of the digital society, how and where local data are stored and otherwise processed;

(b) all types of individuals or data subjects including minors, employees and consumers;

(c) account for international transfers to promote international trade and harmonization among trading partners;

(d) different types of businesses and their respective requirements and obligations, including micro and small businesses, non-profits, government agencies, and educational institutions;

(e) practical enforcement provisions that strike the balance between promoting compliance and promoting trade and innovation;

(f) mandatory breach notification provisions to help resolve under-reporting of breaches and improve response capabilities;

(g) exemptions to take into account matters such as fairness, necessity and accountability;

(h) guidelines and mechanisms to enable effective and efficient implementation and enforcement of provisions such as establishing a supervisory authority and requirements for a data protection officer.

[3] Corlane Barclay, 2018, Data Protection Laws in the Caribbean and the Way Forward, https://www.linkedin.com/pulse/data-protection-laws-caribbean-way-forward-corlane-barclay?trk=public_profile_article_view.

In concurrence, these and other matters should form the basis for the ECCU's data protection policy.

b. Scope

Determining matters such as the types of processing of personal data, categories and location of data controllers that are applicable under the legislation enables fidelity of the law.

Data protection laws are generally predicated on computer-aided or automated means of processing. However, manual processing is also contemplated, subject to certain conditions. Recital 15 of the GDPR, provides the following guidance:

> the protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system.

A filing system is any structured set of personal data which is accessible according to specific criteria, regardless of storage classification or location.

The following matters may also be contemplated:

(a) **Exclusion of application**, in respect of the processing of personal data -

- solely for personal or household activity;
- by competent public bodies for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to national or public security.

(b) **Restrictions of application** -

- of single one-time collection of personal data, subject to certain conditions such as whether that personal data is stored;
- in relation to certain obligations, where the processing of personal data is solely for journalistic purposes, or for the purposes of academic, artistic or literary expression;

- in relation to certain obligations, a data controller or data processor is of a certain size[4].

(c) In terms of **territorial scope**, the current jurisprudence reflects an extraterritorial nature of application in that the legislation shall apply to -

- a data controller or data processor that is lawfully established in a country of the ECCU;
- a data controller or data processor not established in a country of the ECCU that processes the personal data of data subjects of the ECCU, where that processing is related to the offering of goods or services to data subjects within the ECCU [whether payment is required or not], or the monitoring of the behaviour of data subjects as far as their behaviour takes place within the ECCU;
- in relation to the processing of personal data by a controller not established in the ECCU, a state where the law of a participating government of the ECCU applies by virtue of public international law.

c. Key Definitions

Certain key terms are centred on the main actors and activities within the data protection ecosystem. These include the data subject, categories of personal data, data controller, data processor, data protection officer and data protection authority.

"consent" means any freely given, specific, informed and unambiguous signal or indication of a data subject's agreement to the processing of the personal data relating to the data subject by a data controller;

"data controller" means any person[5] who, solely or collectively with another person, determines the purposes and means of the processing of personal data;

[4] For example, the GDPR has a derogation for organizations with fewer than 250 employees with regard to record-keeping (recital 13).
[5] A person means a natural or legal person including an authority, subject to the Interpretation Acts of countries of the ECCU.

"data processor" means a person, other than an employee of the data controller, who processes personal data on behalf of a data controller;

"data protection authority" means the authority in charge of administering data protection legislation established within ECCB;

"data protection officer" means a suitably qualified and competent person appointed with responsibility for the monitoring of compliance, in an independent manner, with the relevant provisions under the data protection legislation;

"data subject" means, in relation to the processing of personal data, a natural person, whether living or deceased for a specified period[6] and who is a citizen or ordinary resident of a country in the ECCU;

"personal data"[7] mean any information relating to a data subject that may, directly or indirectly, lead to that data subject being identified or identifiable;

"personal data breach" means a breach of security resulting in the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;

"'processing"[8] means any operation or set of operations which is performed on any personal data or set of personal data whether or not by automated means;

---

[6] Jamaica's Data Protection Act provides for less than thirty years after the deceased data subject (s.2). Contrastingly, the GDPR does not apply to the personal data of deceased persons, however their Member States may provide for rules regarding the processing of personal data of deceased persons (recital 27).

[7] Personal data is generally referred to as any information that relates to an identified or identifiable individual.

[8] Processing may include operations such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, according to the GDPR (article 4). However, the main takeaway is any operation performed on any personal data, across a data lifecycle, from collection or creation through to deletion, archiving or destruction. It also takes into account the flow of personal data from one point or country to another.

d. Data Processing Requirements

Data Processing requirements represent elements of privacy by design and serve as a central theme in contemporary data protection legislation. The adoption of privacy by design signifies that privacy considerations are embedded in the operations of a data controller or data processor[9]. Therefore, certain obligations are placed on data controllers and data processors to implement appropriate technical and organisational measures to ensure that the data they collect, use and otherwise process throughout the data lifecycle are processed in a manner that is consistent with sound and fair information practice principles such as lawfulness, fairness, security and accountability. These and other principles are further elucidated herein:

- **The Collection Limitation Principle**. The collection of personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **The Data Quality Principle**. 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.
- **The Purpose Specification Principle**. The purposes for which personal data are collected should be specified at the time of data collection and any subsequent change in processing should be limited to those specified purposes.
- **The Use Limitation Principle**. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject, or by the authority of law.

[9] The 7 principles of Privacy by Design are: Privacy as the Default; Privacy is Proactive and Preventative; Privacy is Embedded into Design; Full Functionality is Positive Sum; End to End Security; Visibility and Transparency in Operations; and Solutions are User-centric.

- **The Security Safeguards Principle**. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
- **The Openness Principle**. There should be a general policy of openness about developments, practices and policies with respect to personal data. Personal data management practices must be clear, easy to understand and be readily available. This may include the existence and nature of personal data and the main purposes of their use, as well as the identity and official address of the data controller.
- **The Individual Participation Principle**. Any data subject should have the right:
  (a) to obtain from a data controller information pertaining to whether or not the data controller has data relating to that data subject;
  (b) to have data relating to that data subject communicated in a form that is readily intelligible to that data subject, within a reasonable time;
  (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and
  (d) to challenge data relating to that data subject and, if the challenge is successful, to have the data erased, rectified, completed or amended.
- **The Accountability Principle**. A data controller should be accountable for complying with measures which give effect to the fair information practice principles as described above.

e. Lawful Processing of Personal Data

There must be a lawful basis for the processing of personal data. The lawful bases for processing are centred on consent or being necessary for a specific purpose. The most appropriate basis will depend on a data

controller's purpose and relationship with the data subject. These lawful bases for processing are[10]:

- **Consent**. The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- **Performance of a contract**. Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- **Compliance with a legal obligation**. Processing is necessary for compliance with a legal obligation to which the data controller is subject;
- **Protect vital interests**. Processing is necessary in order to protect the vital interests of the data subject or of another individual;
- **Public interest**. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- **Legitimate interest**. Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by another person authorized to process personal data. Legitimate interest does not apply where:
  (a) such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (e.g. a child); and
  (b) the processing is carried out by public authorities in the performance of their tasks.

f. Rights of Data Subjects

The rights of a data subject should be linked to the principles of consent, openness, transparency, and respect for user privacy in the processing of personal data. The legislation should consider the different types of data

[10] Article 6, GDPR.

subjects who may be employees or customers who may be minors. It should also contemplate the mental and legal capacity of these data subjects, and specific needs and circumstances in relation to the processing of their personal data. In that regard, the rights of a data subject include:

- **Right of access**. The right to know about the personal data that a data controller collects about them and how it is used and shared;
- **Right to be forgotten** (to delete). The right to delete personal data collected from them (with some exceptions);
- **Right to opt-out of specific processing** The right to opt-out of certain processing such as the sale of their personal information. The GDPR provides for, the **right to object** to certain processing such as direct marketing or profiling;
- **Right to rectification**. The right to rectify the processing or personal data due to inaccuracies or incompleteness;
- **Right to non-discrimination**. The right to non-discrimination for exercising their rights under the legislation.
- **Right to data portability**. Right to receive and transmit his or her personal data to another controller without hindrance.
- **Rights in relation to automated decision-making**. Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects that data subject.

g. Obligations of Data Controllers and Data Processors

The legislation should contemplate practical and reasonable obligations to meet its intent of protecting the rights of the data subjects and protecting the processing of personal data. The obligations of both data controllers and data processors should be linked to the general data protection principles, security and privacy of processing as a default. In addition, certain requirements may also include:

(a) the appointment of a data protection officer;
(b) the appointment of a data protection representative where a data controller is established outside of the ECCU;
(c) the maintenance of a record of processing activities under its responsibility;
(d) the undertaking of data protection impact assessments;
(e) the adherence to certain standards regarding the security of the processing of personal data;
(f) the compliance with certain data processing standards, including privacy by design requirements;
(g) personal data breach notifications in a timely manner to the DPA and the data subject;
(h) obligations to data subjects such as those described in para f;
(i) restrictions in relation to international data transfer.

h. Role of the Data Protection Authority

The DPA shall be an independent public body, vested with powers of investigation and enforcement, and be able to engage in mutual cooperation with other similar international and regional bodies, subject to the necessary legal provisions in ECCU's countries.

The principal activities of the DPA should include managing adherence to the legislation by data controllers and data processors, providing cogent guidance on the interpretation and application of the legislation, investigating complaints and breaches, and enforcing the relevant legislative provisions in an effective proportionate and dissuasive manner.

Insights from other jurisdictions relating to the powers and functions of the DPA should help to inform the design and operations of the ECCU's DPA. For example, Jamaica 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. Barbados provides for a Data Protection Tribunal that can hear appeals regarding

notices served under the Act. The ECCU may contemplate these models or variations thereof in the determination of the powers and functions of a DPA.

i. Transfers outside of the ECCU

When personal data is transferred outside the ECCU, the legislation should contemplate providing special safeguards to ensure that the protection travels with the personal data.

The countries within the ECCU will have a presumption of adequate data protection processing standards on the basis of the coming into operation of the harmonized legislation. The ECCU should also take into account data flows to other countries in the Caribbean and other countries or regions, and the conditions to which that country is deemed to have an adequate level of protection in relation to the processing of the personal data of citizens of the ECCU. To make that determination, certain matters may be taken into account: whether there are clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in that other country[11]. Additional conditions may include cooperation mechanisms between the ECCU's DPA and the DPA of the other country and the provision of enforceable rights to the data subjects.

j. Enforcement Measures

Certain powers shall be vested in a DPA to impose effective, proportionate and dissuasive measures, particularly where a data controller or data processor violates certain provisions in relation to the processing of personal data.

Where a DPA concludes that a violation has taken place, the data controller or data processor may become liable to fines. The DPA shall

[11] The GDPR is a useful reference point in this situation. For instance, it advises that a third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where data are processed in one or several specific sectors (recital 104).

also have at its disposal the power to give notices, such as enforcement or fixed penalty notices.

The principal position is to design and implement effective, proportionate and dissuasive measures that are suitable for the ECCU's environment.

6. Summary

To achieve the objective of building a strong data protection regime, it is recognized that sound legislation that is effectively operationalized is a significant first step. This will signal the ECCU's growing commitment to providing adequate levels of data protection measures and protection of the fundamental rights and freedoms of individuals.

In that regard, the primary policy considerations in developing a harmonized data protection legislation are summarized herein.

(a) Cogent scope of application that takes into account the facets of the processing of various forms of personal data and the flows of such personal data of ECCU's citizens.

(b) A transitional period[12] of at least one year should be contemplated under the legislation to allow affected natural and legal persons the opportunity to prepare for compliance with the impending legislation.

(c) The establishment of a strong DPA within the ECCB. This should take into account full matters relating to establishing appropriate institutional arrangements to enable a positive impact on the local environment, effectively monitor the key actors, utilize practical and transparent investigatory powers, and apply timely effective proportionate and dissuasive measures.

(d) Exemptions and derogations that are determined based on the practical nature of the specific processing of data while balancing the requirement to safeguard the privacy and the protection of personal data being processed.

[12] Many data protection regimes provide for 2 years.

(e) Robust data protection requirements, including security standards, contextualised within contemporary data protection principles where data controllers and data processors have a responsibility and obligation to comply.
(f) The rights of the data subjects, taking into account the diversity of individuals, their mental capacity, competency to give consent, forms of personal data concerning an individual, and their potential needs in relation to the processing of their personal data.
(g) Enforcement measures that are effective, proportionate and dissuasive.
(h) Promote a judicious balance of protection and responsible processing to facilitate continued technological development, innovation, trade and flows of personal data across borders.

7. Conclusion

Data protection legislation is considered a complex instrument. In that regard, policymakers and legislators must take into account:

(a) the multi-faceted and evolving data protection ecosystem;
(b) the nuances of the developing forms of personal data;
(c) how and where personal data are processed, particularly with the growth of new technologies such as artificial intelligence;
(d) who, and in some instances what, is determining the processing of personal data; and
(e) the possible risks to such processing,

as principal considerations in implementing adequate legal measures to protect the privacy of individuals (particularly its citizens) and safeguard the processing of personal data.

To help ensure that data protection legislation is robust and effective, the legislation must: fit the specific needs of the ECCU and its evolving technological landscape; reflect contemporary jurisprudence and perspectives; have cogent provisions to reflect adequate levels of protection of personal data of data subjects, regardless of where that personal data may flow or be processed.