Impact of Data Protection and Privacy on Regulating Competition and Consumer Protection for Digital Markets within CSME

The Commonwealth

CARICOM competition commission

Impact of Data Protection and Privacy on Regulating Competition and Consumer Protection for Digital Markets within CSME

The Commonwealth

CARICOM competition commission

Commonwealth Secretariat
Marlborough House
Pall Mall
London SW1Y 5HX
United Kingdom

www.thecommonwealth.org

Published by the Commonwealth Secretariat.

Contents

List of figures and tables

Figures

Tables

Acknowledgments

This report was prepared under the overall guidance and funding of the Commonwealth Connectivity Agenda Section of the Trade, Oceans and Natural Resources Directorate, Commonwealth Secretariat, and managed by the CARICOM Competition Commission.

The report was authored by London Economics Ltd, an international development consultancy firm.

We would like to acknowledge the invaluable contributions of the numerous agencies and stakeholders who provided information and feedback during the course of this study. Their insights, knowledge and engagement significantly enriched the quality and depth of our research. Special thanks to the following organisations for their active participation in the stakeholder meeting held in August 2023, including the Caribbean Telecommunications Union, the Jamaica Fair Trading Commission, the Trinidad and Tobago Fair Trading Commission, the Consumer Affairs Commission (Jamaica), the Eastern Caribbean Telecommunications Authority, and the Office of the Information Commissioner (Jamaica). Your input and expertise have been integral to the success of this study, and we are grateful for your collaborative spirit and dedication to data protection and privacy in the CSME and the Commonwealth nations. Together, we strive towards a more secure and responsible digital future.

Acronyms and abbreviations

APEC	Asia–Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
AI	Artificial Intelligence
B2B	Business-to-Business
B2C	Business-to-Customer
BCRs	Binding Corporate Rules
CARICOM	Caribbean Community
CCC	CARICOM Competition Commission
CCI	Competition Commission of India
CCPA	California Consumer Privacy Act
CJEU	Court of Justice of the European Union
CMA	Competition and Markets Authority (UK)
CPS	Core Platform Service
CSME	CARICOM Single Market and Economy
DMA	Digital Markets Act (EU)
DMU	Digital Markets Unit (UK)
DPA	Data Protection Authority/ Act
DSA	Digital Services Act (EU)
EC	European Commission
ECLAC	Economic Commission for Latin America and the Caribbean
EEA	European Economic Area
EU	European Union
FCO	Federal Cartel Office (Germany)
FTC	Federal Trade Commission (US)
GDPR	General Data Protection Regulation
HIPCAR	Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (model law)
ICT	Information and Communication Technology
ITU	International Telecommunication Union
M&A	Mergers and Acquisitions

OECD	Organisation for Economic Co-operation and Development
POPIA	Protection of Personal Information Act (South Africa)
SACC	South African Competition Commission
SCCs	Standard Contractual Clauses
SIDI	Systemically Important Digital Intermediaries
SMS	Strategic Market Status

Executive Summary

The increasing ubiquity of digital technologies that use and produce data on a vast scale has garnered much attention from policy-makers, regulators and competition authorities across the world. The interplay between data, consumer protection, competition, and trade in the market for digital technologies has given rise to ongoing debates on the legislation, initiatives and new approaches to regulating digital markets and enforcing existing consumer protection and competition rules.

This study, which was commissioned by the CARICOM (Caribbean Community) Competition Commission (CCC) and funded by the Commonwealth Secretariat, presents baseline information collected on data protection and privacy in the region to determine whether the legislative and regulatory frameworks in the CARICOM Single Market and Economy (CSME) member countries can address modern competition, consumer protection and international trade concerns.

Competition issues in digital markets

Digital markets can be conducive to anti-competitive outcomes. While the features that facilitate this are not unique to digital markets, they can take on a different quality in digital markets (for example, network effects, the exploitation of user data), resulting in dominant firms gaining significant durable market power.

Competition authorities worldwide are improving their understanding of digital markets and are developing enforcement practices to address the new challenges.

While existing competition laws are being used effectively, there is widespread concern that new instruments may be needed. Countries such as those in the European Union (EU), the United Kingdom (UK), India and Brazil are developing special competition frameworks for digital platforms based on:

- increased market monitoring and *ex ante* rules to prevent markets from tipping to monopolisation (including increased monitoring of merger and acquisition (M&A) proposals by the largest digital platforms):
- conduct requirements;
- tougher enforcement tools, including large fines and breaking up of businesses; and
- the creation of specialised regulatory units with a focus on digital markets and commercial practices of the largest digital platforms.

To date, only four out of thirteen CSME member countries have competition laws. This is a significant gap in the legal framework applying to digital markets. The CCC should continue to promote the establishment of a minimum common framework for addressing anti-competitive behaviour by businesses in the CSME. Those CSME member countries that have competition laws (Barbados, Guyana, Jamaica, and Trinidad and Tobago) have so far not embraced the trend seen in the EU and UK (and under discussion at the federal level in the United States) towards a specific *ex ante* regulation of large digital platforms. We judge that this is an appropriate stance for CSME member countries, owing to the resource requirement and the unproven effectiveness and efficiency of such an approach. Instead:

- CSME member countries could adopt a *fast-follower* approach to digital market regulation. That is:
  - Leverage on the regulatory output of leading jurisdictions to ensure consumers and businesses in CSME member countries face similarly favourable terms in digital markets without incurring the full costs of replicating the regulatory efforts of leading jurisdictions. This could involve:
    - ongoing monitoring of relevant developments in key global jurisdictions and a regular review of insights and lessons applicable to the CSME; and
    - participation of CCC representatives in global forums and conferences.
  - Co-operate with agencies with advanced frameworks to strengthen own enforcement, including through personnel exchanges/secondments.

- Competition authorities should:
    - Be vested with more powers to require large digital platforms to mirror any pro-competitive conduct remedies they had to implement to the benefit of firms and consumers in other jurisdictions in CSME member countries' markets.
    - Be vested with more powers to enforce more punitive fines in case of non-compliance.
    - Explore increased co-operation with adjacent regulatory authorities (telecoms, data protection, consumer protection, cybersecurity) on competition issues in digital markets to make the best use of scarce resources. A low-cost approach concentrating on channels for information exchange and informal collaboration is recommended.
- The CCC should encourage CSME member countries to align their approaches to regulating competition in digital markets, including closing gaps in the existing legislation, as:
    - Regional heterogeneity in regulatory frameworks can significantly undermine welfare gains in the form of foregone trade and innovation.
    - Heterogeneity might also undermine the effectiveness of the enforcement process given the transboundary nature of digital products and services.
- An effective competition policy for the CSME digital sector should be based on a thorough understanding of the prevalence and impact of the issues faced by businesses and consumers. The CCC should conduct research on the relevant issues. This should include surveys businesses and consumers in the CSME.

Data protection

- Data protection laws aim to protect individuals' personal information from unauthorised collection, storage, processing and disclosure. These laws aim to balance the need for personal information with the need to protect individual privacy, while promoting responsible data practices and encouraging trust and confidence in digital technologies.
- While data protection laws are typically concerned with the fundamental human right to privacy, they have significant effects on economic activity, specifically competition and business models in the digital economy.
- The European General Data Protection Regulation (GDPR) was introduced in 2018 and has since become a template for international data protection laws.
- Besides providing for standard data protection rights to consumers, the GDPR contains elements of economic regulation with implications for competition in data-intensive digital markets. These elements include the right of access and the right to data portability (which reduce barriers to switching and limit market power due to exclusive access to user data), and rules for international transfers of personal data (which place a significant administrative burden on firms engaging in the international transfer of personal data, see below).
- While the implementation of GDPR is costly and its economic effects are not clearly positive, digital businesses have been able to transition to the new legal landscape without significant difficulties.
- Eight CSME member countries have enacted data protection and privacy laws: Antigua and Barbuda (2013), Barbados (2019), Belize (2021), Jamaica (2020), St Kitts and Nevis (2018), Saint Lucia (2011), St Vincent and the Grenadines (2003), Trinidad and Tobago (2011).
- At the time of this report, CSME countries exhibited some gaps in data protection regulation relative to the GDPR, which is currently the template for international data protection law. As a result, citizens of CSME member countries enjoy more limited rights in some dimensions. The gaps also potentially limit the ability of CSME-based firms to compete in areas that require the processing of personal data of data subjects covered by the (EU and UK) GDPR and similar frameworks. While international data transfers are still possible under various legal mechanisms, the burden is on individual firms to identify the relevant mechanisms and ensure compliance.

- Data protection law should as a priority address the data protection needs of citizens in the CSME.
- However, fully replicating the GDPR in CSME member countries could be overly complex and costly to both companies and regulatory authorities responsible for enforcing the regulation.
- Harmonising the legislation also does not eliminate risks regarding mutual recognition, whereby adopting a data protection framework modelled after the GDPR might still not be sufficient to be accepted as providing adequate protection by other nations or regional blocs.
- On the other hand, heterogeneity of data protection rules within the CSME can negatively affect the regional digital economy.
- The HIPCAR (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean) model law could be amended to reflect the key innovations of the GDPR and to be more prescriptive with regard to rules pertaining to cross-border data transfers.

International data transfers

- Data localisation rules aside, all jurisdictions in principle allow cross-border data transfers to take place.
- The EU GDPR framework represents the most articulated international framework and is likely to be the most relevant for businesses in the CSME. Other relevant international frameworks are the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Additional Protocol to the Council of Europe Convention 108. The key principles are that data can be transferred:
  - 'if the recipient State or international organisation is able to afford an adequate level of protection', or
  - if 'adequate safeguards, in particular resulting from contractual clauses, are provided by the data exporter in accordance with domestic law'.
- With the proliferation of data protection laws worldwide, frictions resulting from adequacy assessments have started to emerge, even in cases where legislation is seemingly aligned.
- Pursuing European Commission (EC) adequacy would involve a determined whole-of-government effort (as seen recently in the cases of Japan and South Korea) with uncertain benefit for citizens in the CSME.
- Binding corporate rules (BCRs) establish uniform internal rules for transferring personal data within a corporate group. BCRs are used for the internal business processes of the group. While some firms that are active in the CSME have registered BCRs, there were no CSME-headquartered firms with registered BCRs at the time of writing.
- Standard contractual clauses (SCCs) are open to CSME-based firms, but they are generally viewed as being relatively costly and inflexible measures. The SCCs do not fit each type of data transfer, must be used without change, and are considered as imposing terms that 'are relatively onerous to meet and can lead to high administrative costs'. Association of Southeast Asian Nations (ASEAN) model contract clauses (MCCs) and cross-border privacy rules (CBPRs) provide analogous mechanisms.
- The other options are explicit consent and contractual necessity as the key derogations (Art. 49 of the GDPR) that are relevant for commercial enterprises and are likely to be a viable alternative for businesses that enter into direct contractual relationships with EU individuals (business-to-consumer [B2C]).
  - Contractual necessity and consent are often appropriate, for example, in e-commerce and the travel industry.
  - Derogations are less likely to be appropriate for firms using personal data in bulk (business-to-business [B2B]).
- The CSME can strengthen its international position as a participant in international data markets by harmonising data protection law and practice internally, while advocating for a trade-friendly data protection system globally – for example, in the form of a Global Privacy Enforcement Treaty under the World

Trade Organization (WTO) architecture and enforced via the WTO dispute settlement process.[1]

Consumer protection

- Some CSME member countries are missing relevant legislation on one or more areas; that is, Belize on consumer protection; Suriname on consumer protection and cybercrime legislation; and Dominica on consumer protection and cybercrime. This gap should be closed to ensure a consistent level of protection for consumers across the CSME.
- Digital markets can give rise to specific types of consumer harm, including data breaches and manipulation of the choice environment ('dark patterns').
- While there is no firm evidence on the prevalence of digital harms in the CSME member countries, they are likely to be present to some degree.
- Existing consumer protection frameworks in CSME member countries are not set up to protect consumers from the complex forms of digital harms that occur in digital markets.
- Legislation on consumer protection, data protection, electronic transactions and cybercrime/computer misuse is in place in Barbados, Antigua and Barbuda, and Jamaica.
- The risk of digital harms to consumers is potentially exacerbated by the remaining gaps in digital literacy in the CSME.
- A useful first step would be for the CCC to investigate the prevalence of digital consumer harms in the CSME, in fulfilment of its mandate to providing support to CSME member countries in promoting consumer welfare.
- As a second step, the CCC may issue guidance on the treatment of digital consumer harms under the existing consumer protection legislation to ensure a level playing field for consumers and businesses within the CSME. On this basis, the CCC could support member countries' review of consumer protection legislation to determine whether updates are needed to address specific digital consumer harms.
- Developing new legislation should also involve assessing its potential impact on digital innovation and ensuring it would not impede the development and availability of digital products and services that are beneficial to consumers.
- Providing consumers with information on digital harms (for example, on the CCC website and/or through publicity campaigns) and embedding such information in a wider digital skills strategy are useful auxiliary steps.

Conclusions and recommendations

The CSME data protection regime is progressing towards a comprehensive and self-sustaining framework that is in line with international best practices.

Data protection policy in member countries should continue to prioritise the interests of citizens of the CSME in terms of substantive protections and rights and economic implications.

Regional heterogeneity in data protection policy, especially regarding elements relevant to cross-border data flows, could be problematic. It could reduce cross-border data flows, as data protection rules in one country could prohibit data transfers to another in the CSME. This could have a negative impact on trade and innovation in the regional digital economy.

The CCC could play an important role in advocating for regional harmonisation across the CSME regarding data protection regulation where it has direct competition implications. It could provide guidance in the development of an aligned approach to data protection regulation, in particular with respect to measures to increase contestability of data markets such as data access and portability.

This study recommends a 'fast-follower' strategy for enforcing competition law in digital markets in the CSME. A fast-follower strategy involves smaller players adopting the best practices and latest developments of larger players or leaders in the field. The benefits of this approach are:

- Efficient use of resources: By following established best practices and guidelines, the competition authorities in the CSME

1 For details on this approach, see Chander and Schwartz (2023).

can use their limited resources efficiently to address the complex issues arising from digital markets.

- Flexibility: A fast-follower strategy allows the competition authorities in the CSME to adapt to changing market conditions and new developments in technology quickly, which is important in the rapidly evolving digital economy.
- Access to expertise: By leveraging the knowledge and experience of other jurisdictions, CSME authorities can gain access to expertise and innovative methods and tools that might not be available domestically.
- Enhanced credibility: By demonstrating a commitment to enforcing competition laws and regulating digital platforms consistent with internationally recognised standards, the CSME can enhance its credibility and influence in regional and global economic forums.
- Better positioning for future regulatory co-operation: By closely following the approaches of larger jurisdictions, the CSME can better position itself for future regulatory co-operation and co-ordination, which may become increasingly important as the digital economy continues to grow.

1. Introduction

1.1 Background and context

The increasing ubiquity of digital technologies that use and produce data on a vast scale has garnered much attention from policy-makers, regulators and competition authorities across the world. The interplay between data, consumer protection, competition, and trade in the market for digital technologies has given rise to ongoing legislative debates and initiatives, and new approaches to regulating digital markets and enforcing existing consumer protection and competition rules.

Leading competition authorities across the world have attempted in recent years to understand how companies operating within the digital space can use data to their competitive advantage and how this can distort competition and cause consumer detriment, but also how data protection laws themselves affect competition in digital markets.[2] However, although the digital economy in the CSME is growing, there have been no similar attempts to understand these issues in the region.

Additional concerns relate to the effects of data protection on international trade and investment. Data will flow across borders unless governments enact barriers. Data protection legislation that is too restrictive could, therefore, result in data protectionism and restrict international data flows, affecting productivity, innovation and competition in digital markets. This is of great concern for CSME member countries, some of which have successfully pursued foreign direct investment (FDI)-led development strategies that centre on attracting foreign investment in data-intensive services, such as business process outsourcing (BPO) and international financial services (IFS).

1.2 Purpose of the study

The CARICOM Competition Commission (the 'CCC' or 'the Commission'), in collaboration with the Commonwealth Secretariat, commissioned this study as a first step in exploring the relationship between protection and privacy, competition and consumer protection law, and digital trade.

The study approaches this issue from two perspectives. First, it provides an up-to-date overview of the international developments in this area and benchmarks the current CSME legislative framework against these international precedents. Second, the study also collects and presents baseline information on data protection and privacy in the region, to determine whether the legislative and regulatory frameworks in CSME member countries can address modern competition, consumer protection and international trade concerns.

The information provided in the study aims to help the CCC shape its enforcement and advocacy role and define its priorities for digital markets. The recommendations offered will also feed into a programme/project to build the capacity of the competition and consumer protection authorities and trade officials in the region, to better equip them to address these matters.

As part of the study, the Commission sought input from key stakeholders to help:

- determine whether data protection legislation and regulatory frameworks provide barriers to liberalisation and full economic realisation of the CSME market in the digital markets, through a legislative and policy review and phased outreach to all relevant stakeholders;
- determine its enforcement and advocacy role and/priorities in digital markets; and
- develop a programme/project to build the capacity of the competition and consumer protection authorities and trade officials in the region, to address these matters – as they are of growing importance to the CSME.

A stakeholder workshop was held on 04 August 2023 to garner the views of officials in the competition and consumer protection law and data protection fields across the region. These stakeholders represented the Eastern Caribbean Telecommunications Authority, the Caribbean Telecommunications Union, the Fair

2 Relevant scenarios include: (a) agreements between competitors on data protection and privacy policies that violate competition law; (b) dominant firms that justify their refusal to grant access to the data they collect by invoking obligations under data protection laws; and (c) the limits on access to information by competition authorities from online companies during investigations placed on third parties by data protection rules.

Trading Commission (Jamaica), the Consumer Affairs Commission (Jamaica), the Office of the Information Commissioner (Jamaica), and the Trinidad and Tobago Fair Trading Commission. The study incorporates feedback from the workshop from these stakeholders.

1.3 This report

1.3.1 Content and structure

This report provides research and analysis on the global trends in data protection, competition and consumer law and enforcement in leading international jurisdictions and in the CSME, to provide the Commission with a forward-looking perspective on regulatory challenges and gaps in its armoury. The report is structured as follows:

- Section 2: Competition issues in digital markets
- Section 3: Data protection issues
- Section 4: Digital trade issues
- Section 5: Consumer protection issues
- Section 6: Conclusions

The report is based on a review of secondary sources, including London Economics' own work on the respective topics and inputs received from the Commission on behalf of CARICOM member countries.

1.3.2 Limitations

The topics addressed by this report are large and complex, spanning economic, legal and policy considerations across global jurisdicitions. The depth of the analysis in this report is therefore necessarily limited to fit the purpose of a focused update on key developments and lessons from a CSME perspective.

The policy landscape is also extremely dynamic, with impactful developments occuring at a high frequency. While the report endeavours to present the most up-to-date information, important developments have occurred throughout the project's lifetime, not all of which have been reflected in the analysis.[3]

There are also constant developments in the technology underlying digital markets and their competitive dynamics. Prominently among the relevant technological developments in 2023 has been the emergence of highly capable artificial intelligence (AI) systems with broad applications across the economy and as yet highly uncertain economic impacts. Because of this uncertainty, the study did not consider these recent trends.

The Commission initially envisaged the study to include fieldwork to collect information from regional businesses. Due to time and resource constraints, this part of the scope has not been imlemented. As a result, there remians an evidence gap with respect to the experience of CSME-based businesses which should be addressed by future research.

3 For example, the decisions by the European Commission Directorate-General for Competition (DG COMP), the UK Competition and Markets Authority (CMA), and the Federal Trade Commission (FTC) on the Microsoft-Activision merger; the EU–Community of Latin American and Caribbean States (CELAC) Digital Alliance; the invalidation of the Privacy Shield Framework and the subsequent adequacy decision by the European Commission for the new US–EU Data Privacy Framework; the adoption of the Indian Personal Data Protection Bill, etc.

2. Competition Issues in Digital Markets

Key findings

- Digital markets can be conducive to anti-competitive outcomes due to features such as network effects and the exploitation of user data, which could result in already dominant firms gaining significant, durable market power.
- Competition authorities in developed countries such as the EU, UK and the US, and developing countries like India and Brazil, are establishing different types of frameworks and initiatives to address competition concerns in digital markets. Such initiatives include the establishment of specialised units to monitor large digital platforms and the enactment of ex ante regulations to prohibit anti-competitive conduct.
- CSME member countries have not yet embraced the trend of establishing frameworks to address competition concerns in digital markets. This is likely due to resource constraints.
- To address competition concerns in digital markets, CSME member countries should consider several strategies, including:
  a) a fast-follower approach to regulating digital markets, which leverages the regulatory output of leading jurisdictions to ensure consumers and businesses in the CSME face similarly favourable terms in digital markets without incurring full costs of replicating the regulatory efforts of leading jurisdictions;
  b) vesting the competition authorities in the region with more powers to prohibit anti-competitive business conduct of large digital platforms;
  c) the Commission providing a leadership role in harmonising the enforcement approaches to address the anti-competitive conduct of large platforms in the region; and
  d) further research, including surveys of firms and consumers, which is recommended to provide the CCC with accurate and up-to-date information on the prevalence and impact of the issues identified.

2.1 Background

Digital markets are often characterised by market imperfections; that is, features that may impede the efficient functioning of markets. These imperfections are not uniquely digital and can exist in all markets. However, some are commonly observed in digital markets and can make them particularly susceptible to certain forms of market power. For example:

- **Asymmetric information**: When markets operate efficiently, buyers and sellers have equal information on goods or services. Where one party to a transaction holds more information than the other, this can distort market signals and lead to inefficient outcomes. Digital firms often collect and analyse large amounts of data, which they can use to exercise market power at the expense of their users.
- **Barriers to market entry and expansion**: Where potential competitors find it difficult to enter a market and compete with the incumbent firm, or when existing competitors find it difficult to challenge the leading firm. Digital markets often exhibit:

  - **Network effects**: Users get more value from the service the more other users there are on the platform. This includes (BEIS 2021a):
    - Direct network effects: The value to platform users increases with the number of users on the same side of the (multi-sided) market (for example, social media platforms).
    - Indirect (or 'cross-side') network effects: The value to users on one side of the market increases as a new user on a different side joins the network (for example, an increase in the number of sellers benefits buyers on a retail platform).
  - **Economies of scale**: The per-unit cost falls as the number of units consumed grows. Digital services exhibit strong economies of scale, with large, fixed costs and near-zero marginal costs. This can favour incumbent firms and make it difficult for potential competitors to enter the market.
  - **Economies of scope**: Established players in the digital services markets sometimes branch out into adjacent markets (for instance, maps/location services and messaging services). This adds to the value of their data but may also raise barriers to switching for users.
- **Lack of substitutes**: Digital markets, being an area of significant innovation, can lack sufficiently close substitutes, especially when services are 'first to market'. This can limit the choices of consumers.
- **Barriers to switching and multi-homing**[4]**,** including a lack of interoperability.[5]

There are also features that impact competition that are unique to digital markets:

- **Access to data**: Data is a crucial input to digital services, being used to optimise and develop new services, in addition to target advertising. The possession of large quantities of data may therefore confer a competitive advantage, that potential competitors may not be able to replicate. In turn, dominant firms can use their market power to extract excessive amounts of data from their customers, endangering privacy.
- **Algorithmic collusion:** Any form of anti-competitive agreement or co-ordination among competing firms that is facilitated or implemented using automated systems, for example, price-setting algorithms (Gonzaga 2019). As an increasing number of companies rely on algorithms to run and optimise a wide range of operations (including pricing), regulators and policy-makers have started examining the compatibility of these algorithmic applications with competition law, and some have initiated regulatory action (the EC 'AI Regulation' proposal; European Commission 2021a). Competition authorities find algorithmic collusion challenging to assess and identify. Hence, there have only been a few cases of algorithmic collusion in digital markets (for example, *E-turas* [CURIA 2016], *David Topkins* [US Department of Justice 2015]).

4 Multi-homing generally refers to a networking or internet connectivity scenario where a computer or network is connected to multiple communication channels or networks simultaneously. In the broader context of digital services, multi-homing can refer to a strategy or situation where a user, business, or service is connected to or participating in multiple platforms, ecosystems, or digital environments simultaneously. For example, in the case of multi-homing in cloud services, companies may choose to multi-home their data or applications by using multiple cloud service providers simultaneously. In the case of online platforms, businesses might adopt a multi-homing strategy by maintaining a presence on various e-commerce platforms, like Amazon, eBay, and their own website.

5 Vertical interoperability has been the focus of policy-makers and regulatory initiatives (see OECD 2021). Vertical interoperability refers to the interoperability between *complementary* products and services. In contrast, horizontal interoperability refers to the interoperability of *competing* products, services or platforms (for example, interconnection between different communication networks) (see Kerber and Schweitzer 2017). Without interoperability, users would experience lock-in within a digital platform or ecosystem, unable to switch from complementary products and services offered by the platform operator to similar products and services offered by competing firms. Vertical integration is a common feature in the business models of large digital platforms, whereby they offer various services that are often complementary and more valuable when used together within the platform. This type of linking of different services within a platform can create significant benefits for users, such as ease of usage and convenience. However, platform operators could limit the interoperability of their main infrastructure and service with complementary services offered by competing firms to favour the use of their services (for example, closed Application Programming Interface (API)). They could lock in users to use or purchase their complementary products and services and hinder competition in corresponding markets. Rules that ensure data portability thus have a potentially important role to play in ensuring competitive digital markets.

In this context, digital markets offer the potential for dominant firms to have significant market power, leading to winner-takes-all markets or effective cartels in which dominant firms could use their market power to foreclose competition, which could lead to reduced innovation and higher prices for customers.

Data are implicated in these competition issues as a source of market power and also as the vehicle of adverse effects on consumers (for example, through algorithmic discrimination or the exploitation of behavioural biases based on data-based automated decision-making (see Section 5).

In response to concerns about competition, but also other non-economic concerns, policy-makers, competition authorities and regulators in influential jurisdictions have turned their attention to markets for digitally delivered services that function as multi-sided markets in that they connect buyers and third-party sellers and which network effects play a role in shaping competitive interactions. The common reference points are the prominent US tech platforms ('FAANG').[6]

2.2 International developments in competition law enforcement in digital markets

The standard tools of competition law enforcement, merger control (ex ante) and remedies and sanctions against anti-competitive behaviour (ex post) have been widely used to ensure digital markets are functioning effectively for the benefit of consumers.

2.2.1 Anti-competitive practices

This section lists some of the notable international cases from recent years covering anti-competitive practices, including self-preferencing, the use of exclusionary clauses, exploitative contract terms (for example, bundling), as well as auction manipulation.

Self-preferencing: *Google LLC*[7] *v European Commission* (2021)

In 2017, the European Commission (EC) found that Google had abused its dominant market position in online general search services in 13 European Economic Area (EEA) countries by favouring its comparison-shopping service over competing comparison-shopping services. The EC found that the results of product searches made using Google's general search engine were positioned and displayed in a more salient manner when they came from Google's comparison-shopping service than from competing comparison-shopping services. Results coming from competing comparison-shopping services were shown as simple generic results and, unlike results from Google's comparison-shopping service were prone to being demoted by Google's general search engine's adjustment algorithms. Google was fined about US$2.8 billion (2.4 billion euros [€]), which went on to take action (along with parent company Alphabet) against the EC's decision before the General Court of the European Union. In November 2021, The General Court issued its judgement, which dismissed the action brought by Google and Alphabet and upheld the amount of the fine imposed by the EC (CURIA 2021).

This judgement will make it difficult for Google to deviate from its traditional search engine and develop a search engine that proactively chooses what to show users and nudges them to click on certain results over others. It sets a precedent for self-preferencing practices to constitute an abuse of dominance on its terms and makes it easier for the EC to reach similar conclusions when investigating similar cases in the future (Sidley 2021).

Exclusionary agreements: *United States v Google LLC* (2020)

In 2020, the US Department of Justice (DOJ) brought an anti-trust lawsuit over Google's search engine market practices. As alleged in the complaint, Google had entered into a series of exclusionary agreements with manufacturers of mobile devices and computers requiring Google to be the default pre-installed, and sometimes the exclusive, general search engine on their devices. The complaint alleged that by such practices, Google prohibited the pre-installation of competing search engines and unlawfully maintained its monopolies in general search and search advertising. For example, Google has entered into long-term agreements with Apple that require

6 'FAANG' is an acronym that refers to five prominent American technology companies: Facebook, Amazon, Apple, Netflix and Google (Alphabet).

7 Formerly Google Inc. and Alphabet Inc.

Google to be the default, and by that exclusive, general search engine on Apple's Safari browser and other search tools. The case is set for trial in September 2023.

Monopolisation through serial acquisitions and auction manipulation: *United States v Google LLC* (2023)

The DOJ brought a second anti-trust lawsuit against Google in January 2023. The lawsuit alleges that Google has used anti-competitive, exclusionary and unlawful conduct to eliminate or severely diminish any threat to its market dominance over key digital advertising technologies, collectively referred to as the 'ad tech stack'. The alleged anti-competitive practices include (US Department of Justice 2023):

- Acquiring competitors to gain control over the ad tech stack.
- Forcing bundling or the adoption of other Google ad tech tools. For example, Google allegedly blocks its website publishers from purchasing relevant Google tools (that is, DoubleClick) by restricting their advertiser demand to Google's ad exchange and, in turn, conditioning effective real-time access to the ad exchange on the use of its publisher ad server.
- Distorting auction competition by limiting real-time bidding on publisher inventory to its ad exchange and impeding competing ad exchanges' ability to compete on the same terms as Google's ad exchange.
- Manipulating auction mechanics across several of its products to hinder competition from rival technologies and entrench its market position.

2.2.2 US reforms to strengthen existing competition laws and enforcement practice

In light of the perceived weakness of existing competition laws in curbing the abuse of market power by large digital platforms, some legal experts and policy-makers have advocated for a strengthening of existing competition laws and enforcement practice. The United States in particular has seen legislative initiatives to reverse what is seen by some as an excessively permissive approach to digital platforms. The US House Judiciary Committee's Subcommittee on Antitrust, Commercial, and Administrative Law made a set of recommendations, aiming to:

- Strengthen the country's **anti-trust laws:**
  - US Congress should clarify that the anti-trust laws are designed to protect, besides consumers, also workers, entrepreneurs, independent businesses, open markets, a fair economy and democratic ideals.
  - The law on vertical mergers should be strengthened by restoring bright-line rules and the incipiency standard and by protecting nascent competitors.
  - Section 2 of the Sherman Act should be strengthened by prohibiting the abuse of dominance, as well as by clarifying prohibitions on monopoly leveraging, predatory pricing, the 'essential facilities' doctrine, tying, self-preferencing and anti-competitive product design.
  - Additional measures to strengthen the anti-trust laws include overring problematic precedents in the case law or clarifying that market definition is not required to prove an anti-trust violation.
- Strengthen anti-trust **enforcement:**
  - US Congress should avoid deferring to courts and anti-trust agencies. Rather, it should **restore its commitment to oversee anti-trust laws and enforcement**, including market investigations.
  - **The strength of the federal anti-trust agencies** should be restored. Suggested measures to do so include triggering civil penalties for 'unfair methods of competition', requiring the Federal Trade Commission (FTC) to report on economic concentration regularly, enhancing public transparency of the agencies, requiring regular merger retrospectives, codifying stricter prohibitions on the revolving door between agencies and companies, and increasing the budgets of the FTC and its Antitrust Division.
  - **Private enforcement** should be strengthened by eliminating obstacles such as unduly high pleading standards.

2.2.3 Expanding the competition authorities' toolkit

There are examples of additional tools some competition authorities use to deal with the challenges posed by digital markets. This trend is reflected in guidance documents such as the Joint Paper on Data and its Implications for Competition Law by the German Federal Cartel Office (FCO) and the French Autorité de la Concurrence (Bundeskartellamt 2016) and the Organisation for Economic Co-operation and Development's (OECD's) work on data and competition (OECD 2016).

The trend is exemplified by the German FCO's ruling against Facebook in a case involving the abuse of dominance through the exploitation of users' personal data. In February 2019, the German FCO ruled that Facebook abused its dominance, under Section 19 of the German Competition Act, by improperly collecting and merging different sources of user data (Bundeskartellamt 2019). The FCO imposed far-reaching restrictions on Facebook's user data processing, including a requirement that the company needs 'voluntary consent' from consumers before using their data. This was perceived as an innovative enforcement approach by some and potentially over-stretching the boundaries of competition law by others (Hausfled 2019).

The decision followed mounting pressure from several data protection authorities and consumer rights groups on the FCO to use its more stringent and stronger set of sanctions under competition law[8] to push Facebook to adjust its terms and conditions in line with data protection laws.

The FCO considers Facebook to be an intermediary in a multi-sided network market and to have a dominant position in the relevant German market for social networks, with a market share of over 80 per cent.[9]

Facebook's use and implementation of its data-related terms and conditions were found to not only infringe upon Germany's data protection laws but also exploit Facebook users. While Facebook's terms and conditions did not cause any financial damage to users, the damage was determined to be the users' 'loss of control'. Users could not freely determine and oversee how their data was used from the various Facebook data sources. The FCO relied on two decisions of the German Federal Court of Justice that established that not only excessive prices, but also inappropriate contractual terms and conditions, may constitute an exploitative abuse.[10]

In this case, the FCO considered the relevance of data for competition on digital platform markets, in particular those markets that monetise through targeted advertising based on user data processing. It mentioned that Facebook's exploitative conduct would also 'impede competitors that are not able to amass such a treasure trove of data'.

Meta – the parent company of Facebook – filed an appeal with the Düsseldorf Higher Regional Court against this decision, challenging the authority of the FCO to enforce data protection rules under competition law. This eventually led the Düsseldorf court to request a preliminary ruling from the European Court of Justice (CJEU). The Düsseldorf court addressed various questions to the CJEU on whether the Bundeskartellamt may enforce GDPR rules under competition law and how to interpret certain provisions of the GDPR.

On 4 July 2023, the CJEU ruled that competition authorities in EU member countries have the authority to investigate and sanction an infringement of the GDPR, if companies exploit their dominant market position (CURIA 2023). Nevertheless, competition authorities must consult with the competent data protection supervisory authority in the case of data privacy violations. The CJEU's ruling also included provisions that significantly limit Facebook's legitimate interests in processing its users' personal data and impose strict requirements for obtaining lawful consent in the case of a company with a dominant position in the market (Grentzenberg et al. 2023).

The Facebook proceeding, which is pending before the Düsseldorf Higher Regional Court, will resume taking into account the outcome of the CJEU ruling. Nevertheless, Meta has already announced plans to introduce a new accounts

8 Relative to sanctions provided by existing data protection law and general civil law.

9 Excluding professional social networks such as LinkedIn, and services such as Snapchat, YouTube and Twitter, because they only offer parts of the services of a private social network.

10 German Federal Supreme Court, 6 November 2013, case KZR 58/11, BGHZ 199,1 – VBL-Gegenwart; 7 June 2016, case KZR 6/15, BGHZ 210, 292 – Pechstein.

centre to enable its German users to make a largely free and informed decision about whether they want to use its services separately or in a combined form. Choosing to use the services in a combined form would provide users with access to additional functionalities, while allowing Meta to use the combined data for advertising purposes (Bundeskartellamt 2023).

The CJEU's decision will likely bolster calls for stricter regulation against large tech firms. It will also influence other competition authorities in the EU to follow the steps of the German FCO and target competition issues related to data protection in digital markets. The decision has strong implications for the business models of Facebook and other online platforms that collect large amounts of data for digital advertising, including Amazon, Google and TikTok.

2.2.4 Abuse of superior bargaining position

Some jurisdictions, including Japan and Germany, use concepts of 'relative market power' or 'superior bargaining position' to address conduct deemed to be harmful to competition by firms that fall below the (absolute) dominance threshold. The purpose of the relevant legal provisions is:

- 'to protect competition from negative effects of contract terms that would not occur in the absence of an abuse of superior bargaining power (Japan)'; and
- 'to prevent negative competitive effects by non-dominant firms that may distort competition by exercising market power only to a certain extent and only in relation to certain undertakings (Germany)' (International Competition Network Task Force for Abuse of Superior Bargaining Position 2008).

Such provisions could be useful tools for ensuring competition is preserved in markets where there are great imbalances in bargaining power, which includes some digital platform markets, for example online marketplaces where many small local sellers interact with large global platforms. Art. 20 of the German Act against Restraints on Competition (ARC) directly addresses issues relating to digital markets and specifically applies to:

- 'undertakings acting as intermediaries on multi-sided markets to the extent that other undertakings are dependent on their intermediary services for accessing supply and sales markets in such a way that sufficient and reasonable alternatives do not exist' (Art. 20(1)); and
- situations where an 'undertaking is dependent on accessing data controlled by another undertaking in order to carry out its own activities' (Art. 20(1)(a)).

However, few international jurisdictions have adopted this approach. Reasons include 'reluctance to interfere with the contractual freedom between private parties' and the fact that 'contracts among non-competitors are unlikely to have anti-competitive effects and therefore do not implicate the objectives of competition law' (Ibid). Moreover, Germany and Japan are very large economies. The situation in which a firm has relative, but not absolute, market power is much less likely to occur in smaller economies such as the CSME.

2.2.5 Merger control

Another strand of the evolving regulatory approach to digital markets is a renewed focus on merger control. Specifically, there is growing concern that the current threshold criteria used by competition authorities to assess mergers and acquisitions cannot address the case of 'killer acquisitions'. 'Killer acquisitions' refers to acquisitions by firms of nascent competitors to discontinue the acquired firm's innovation projects, preventing the possibility of future competition (OECD 2020). Killer acquisitions could be uniquely harmful in digital markets, where market power can be otherwise difficult to break.

There is a high level of merger and acquisition (M&A) activity in the digital sector, with the large tech firms like Google, Apple, Facebook, and Amazon (GAFAM) involved in about 400 acquisitions between 2008 and 2018 globally (Digital Competition Expert Panel 2019). However, very few were reviewed by competition authorities, such as the Competition and Markets Authority (CMA) in the UK or the EC, under their current threshold criteria. There are calls to move away from turnover thresholds to alternative criteria, such as transaction value (Stigler Committee on Digital Platforms 2019). Nevertheless, some recent research suggests that there is limited evidence supporting the case of killer acquisitions in digital markets (Ivaldi et al. 2023).

The current debate on both sides of the Atlantic surrounding Microsoft's proposed acquisition of Activision Blizzard illustrates the difficulties faced by competition authorities tasked with safeguarding competition in fast-moving technology markets.

2.3 Regulatory policy response

While debates continue about the ability of traditional instruments of competition law to prevent harmful outcomes resulting from market power, a range of new regulatory instruments has been proposed to address the perceived problems affecting these markets.

The key concerns that motivate the new measures are the perceived lack of contestability and that large platforms are taking advantage of their position to restrict competition, including by imposing unfair conditions on their trading partners and consumers (EC 2020a). Some argue that *'the specificities of competition in the digital world [...] make market power 'sticky', and there is a legitimate fear that the market power [large platforms] have acquired will be hard to challenge. Furthermore, they have been able to build on top of their core competencies, entire ecosystems which make it hard for new entrants to compete on the merit and which, many observers feel, face little competitive pressure'* (Crémer et al. 2018).

Key jurisdictions are currently at different stages of enacting new rules to regulate digital markets and services:

- The European Commission (EC) in the EU and the Competition and Markets Authority (CMA) in the UK, each issued proposals in December 2020 aiming to enhance regulation of digital markets in their respective jurisdiction, targeting the largest digital platforms in particular. The EU Digital Markets Act (DMA) came into force in November 2022, while the UK's pro-competition regime was expected to come into effect in October 2023.
- The US anti-trust agencies have increased their scrutiny of digital markets and large tech companies. In October 2020, the US House Judiciary Committee's Subcommittee on Antitrust, Commercial, and Administrative Law issued a report following a 16-month investigation into the state of competition in digital markets. Throughout 2021 and 2022, several bills targeting tech companies and digital platforms were introduced across both US Congress chambers (Paul et al. 2022). However, these bills had not managed to be brought to a vote or win over the majority at the time of this report (Schaake 2023).

The upgrades to existing regulatory frameworks occurring in the different jurisdictions focus on a broadly similar set of measures. These include:

- Increased market monitoring and ex ante rules to prevent markets from tipping to monopolisation. This includes increased monitoring of M&A proposals by the largest digital platforms.
- Tougher enforcement tools, including large fines and breaking up of businesses.
- Creation of specialised regulatory units, with a focus on digital markets and commercial practices of the largest digital platforms.
- Introduction of regulatory rules targeting the largest digital platforms. These rules focus on ensuring that the largest digital platforms promote interoperability of systems, products and services, and data portability, while prohibiting them from vendor lock-in, taking exclusive advantage of data generated through their platforms, and exploiting business users depending on their platforms to provide them with unfair commercial terms and/or gain a competitive advantage over their business users.

2.3.1 The European Union's Digital Markets Act

The European Union's approach to digital markets policy is, alongside the US approach, the leading framework globally. Because it relies on a small number of related instruments, it is relatively clearly defined, and because of the early push for a comprehensive digital markets policy starting with GDPR, it is often seen as the global 'gold standard'.

The UK's digital markets policy has diverged institutionally, but not substantively, from the EU approach in recent years. It is discussed below as an example of a variant of the EU regime that places somewhat greater emphasis on openness and a business focus. The EU/UK and the US together represent an alternative vision to the state-led approach exemplified by Russia and China, which so far have not been internationally influential.

Table 2.1 Gatekeeper concept,[11] key areas of concern and regulatory approach in the EU, the UK and the US

	EU Digital Markets Act proposal	UK new pro-competition regime proposals	US House Judiciary recommendations
Definition of platform-specific market power	• A gatekeeper is a provider of one (or multiple) core platform service(s) (CPS) which: – has a **significant impact on the internal market;** – operates a CPS which serves as an **important gateway for business users to reach end users**; AND – enjoys an **entrenched and durable position** or it is foreseeable that it will enjoy such a position in the future.	• **Strategic market status** (SMS): Similar to the gatekeeper definition of the DMA, firms with SMS are defined as having: – **substantial, entrenched market power** in at least one digital activity; AND – a **strategic position that can give rise to harm to market competition.** • **The main difference with DMA** is that the 'platform' concept is not key in defining firms with SMS. • **The definition could be perceived as more flexible than that of the DMA** in that digital services in scope are not defined.[12] Rather, in scope is any activity for which 'digital technologies are material to the products and services provided as part of the activity'.	• Not explicitly defined in the report, but given that the report highly leverages the paper by Lina M Khan (2019), the likely definition of gatekeepers assumed in the report is that of the paper where they are described as digital platforms that: – **structure access to the market and behaviour for a large share of market participants** (gatekeepers of economic activity worth billions of dollars); and – **have integrated across business lines** such that they both **operate a platform and market their goods and services** on it.
Quantitative criteria to help identify firms in scope of the above definition	• The gatekeeper belongs to an undertaking that has an **annual EEA turnover equal to or above €6.5 billion** in the last three financial years or that has an **average market capitalisation of €65 billion** and **provides a CPS in at least three member countries.** • The relevant CPS has **45 million monthly active end users in the EU** and more than **10,000 yearly active business users** in the last three years.	• Firms with **annual UK revenue above £1 billion**, and particularly those which also have **annual global revenue over £25 billion.** • **Similarities with the DMA**: – the quantitative criteria help identify firms with potential SMS or who are gatekeepers but are neither necessary nor sufficient to having actual SMS or being designated as a gatekeeper; and – the assessment is conducted for an activity or service rather than against the entire firm.	• N/A

(*Continued*)

	EU Digital Markets Act proposal	UK new pro-competition regime proposals	US House Judiciary recommendations
Key areas of concern/harm	• Ensure digital markets remain open and contestable. • Mitigate the imbalance in competitive advantage and bargaining power between large digital platforms and third-party businesses. • Enhance regulatory framework and enforcement to ensure compliance and pro-competitive conduct of the largest digital platforms.	• **Similarities with the DMA**: – tackle growing concerns of weak competition by promoting competition and innovations for a 'vibrant digital economy'; and – ensure compliance of large digital firms with new regulatory requirements. • **Differences with DMA:** – improve understanding of digital markets and business models of digital firms; and – also address issues of power imbalance between consumers and corporations.	• **Similarities with the DMA** (and to some extent with the UK regime): – restore competition in digital markets where harmful practices could tip the markets into monopolies; and – address conflict of interests and growing unbalance in market and bargaining power between large digital platforms and third-party vendors.
Key changes in regulatory approach	• **More corrective approach:** – an increase in investigatory and enforcement powers of the EC, including enforcing **break-up of businesses**, **large fines,** and potential channel by which it could **review transactions in digital markets** that would otherwise fall outside its jurisdiction.	• **Creation of a special regulatory unit called the Digital Markets Unit (DMU)**[13] • **More preventive approach than DMA:** – perform constant market monitoring and work closely with other regulators with responsibility for digital markets, in particular, the Office of Communications (Ofcom), the Information Commissioner's Office (ICO) and the Financial Conduct Authority (FCA), as well as with regulators from other jurisdictions; and – resolutions are aimed to be done through a participatory approach. • Still, the **DMU can also take tough action,** including operational and functional separation of different units or full ownership separation.	• **Similar to the DMA**, recommendations do not seek to create a new regulatory unit but rather to **strengthen existing regulatory entities,** including the US Congress and federal anti-trust agencies, **anti-trust laws** and **enforcement measures.** • Enforcement measures also include **structural separations** and a **line of business restrictions.** • **Similar ex ante rules to the DMA and UK regime** are needed to prevent digital platforms from abusing their superior bargaining power and engaging in **self-preferencing** and **vendor lock-in,** as well as to encourage **interoperability** and **data portability.** • Recommends a shift in **presumptions for future acquisitions** by dominant platforms.

11 The gatekeeper concept is explained further in the section on the regulatory approach undertaken by the European Union with the Digital Markets Act (DMA).
12 The new UK regulatory unit in charge of the new SMS regime, the Digital Markets Unity (DMU), provides examples of digital markets that will be prioritised in identifying firms with SMS. These are online marketplaces, app stores, social networks, web browsers, online search engines, operating systems, and cloud computing services.
13 The DMU sits within the UK Competition and Markets Authority (CMA).

The EU is actively promoting its 'digital package' in international venues to establish it as the international standard and to influence the United Nation's Global Digital Compact, which will be endorsed at the UN's Summit of the Future in September 2024, which was due to be preceded by a ministerial meeting in September 2023 (Bertuzzi 2023).

The EU's digital package includes existing legislation, including the GDPR, the Digital Services Act (DSA) and the Digital Markets Act (DMA), which represent a systemic approach to set global standards for online platform regulation; as well as new instruments, namely the Data Act, which will introduce safeguards for the EU industrial data hosted on cloud infrastructure in a third country, and the Artificial Intelligence (AI) Act, the world's first attempt to regulate AI, which the EU believes needs to become the global standard if it is to be fully effective.

The EU also takes a strong position in favour of the current model of internet governance, based on an open and global multi-stakeholder ecosystem, intended to 'keep fundamentals of the Internet out of geopolitics'[14]. This section discusses the economic dimensions of GDPR and then goes into the details of the Digital Markets Act as the key pro-competition tool in the EU's digital policy package. In December 2020, the EC published two regulatory proposals, the Digital Market Act (DMA) (EC 2020b) and Digital Services Act (DSA) (Ibid). The two proposals are part of the broader EU digital strategy 'Shaping Europe's Digital Future' and present an effort by the EC to upgrade and enhance the current regulatory framework governing digital markets and services in the EU. The DSA and DMA came into force in October and November 2022 respectively.

While the DSA seeks to establish a safer digital space in which the fundamental rights of digital users are respected, the DMA's focus is on ensuring that digital markets remain open and contestable.

Shift from a preventive to a corrective regulatory approach

The DMA enhances regulatory monitoring and enforcement rules to establish effective competition in digital markets, in particular, in the domains of the largest digital platforms. The EC is concerned that the current regulatory framework[15] and enforcement rules are not adequate to keep up with fast-changing digital markets and enforce compliance among the largest digital players. With the DMA, the EC increases its investigatory and enforcement powers and shifts from its preventive regulatory approach to a more curative approach. For instance, following a market investigation, the EC could break up the businesses of platforms found to breach the rules, and impose fines on these platforms of up to 10 per cent of their worldwide turnover (Art. 26) and periodic payments of up to 5 per cent of average daily revenues (Art. 27).

Core platform services

The DMA targets the conduct of the largest digital platforms. These are designated as 'gatekeepers'. A gatekeeper is first a core platform service (CPS) provider (Art. 2.1). Types of CPS include:

- online intermediation services;
- online search engines;
- online social networking services;
- video-sharing platform services;
- number-independent interpersonal communication services;
- operating systems;
- cloud computing services; and,
- advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the core platform services listed above (Art. 2.2).

All CPSs that are provided to business users established in the EU or end users established or located in the EU are within the scope of the DMA, regardless of where the CPS provider or gatekeeper is established (Art. 1.2).

Gatekeepers

A CPS provider does not necessarily qualify as a gatekeeper. The EC is particularly concerned with providers of CPS that **most directly connect many**

14 EU (March 2023), p. 6.

15 The current EU regulatory framework for digital services is built around the e-Commerce Directive (2000), which sets out principles for cross-border provision of digital services and minimum standards of liability for online intermediaries across the EU.

business users with many end users through the multi-sidedness of their services. Concerns centre around core platform services that exhibit features such as **extreme scale economies**, **very strong network effects**, **lock-in effects**, and a **lack of multi-homing** or **vertical integration**.[16]

A gatekeeper is a CPS (or multiple CPSs) provider that:

- has a significant impact on the European Union's internal market;
- operates a core platform service that serves as an important gateway for business users to reach end users; and
- enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future (Art. 3.1).

The following **quantitative criteria** together help identify whether a CPS provider qualifies as a gatekeeper:

- it belongs to an undertaking that has an annual EEA turnover equal to or above €6.5 billion in the last three financial years or that has an average market capitalisation of €65 billion and provides a CPS in at least three EU member countries; and
- the relevant CPS has 45 million monthly active end users in the EU and more than 10,000 yearly active business users in the last three years (Art. 3.2).

These criteria are presumptive, meaning companies can rebut their identification as gatekeepers.[17] Similarly, the EC can designate as gatekeepers, CPS providers that do not meet the quantitative criteria but are found to pose similar risks to the openness and contestability of the relevant market(s) following a 12-month market investigation (Art. 15.1). In particular, the investigation will take the following factors into account to assess whether a CPS provider qualifies as a gatekeeper:

- its size, including turnover and market capitalisation, operations and position;
- the number of business users depending on the CPS to reach end users and the number of end users;
- entry barriers derived from network effects and data-driven advantages, in particular concerning the CPS provider's access to and collection of personal and non-personal data or analytics capabilities;
- scale and scope effects the provider benefits from, including data;
- business user or end user lock-in; and
- other structural market characteristics (Art. 3.6).

The EC will review every two years whether designated gatekeepers continue to meet the qualification requirements (Art. 4.2).

Obligations of gatekeepers

The EC will publish and maintain the list of gatekeepers and corresponding CPS for which they need to comply with the *ex ante* obligations laid down in Articles 5 and 6 of the DMA (Art. 4.3).

The obligations provided in Article 5 are straightforward obligations that mainly restrict gatekeepers from exercising commercial power over their business users.

The obligations in Article 6 are more complex obligations that require gatekeepers to facilitate and increase access of third-party providers and end users to one another. Implementing these obligations would likely adapt to each type of CPS and require further specification from the EC.

These obligations could significantly impact the way dominant digital (platform) services providers market, operate and make strategic decisions.

Collection and usage of data generated through the use of their platforms

The EC is concerned that a gatekeeper might take advantage of its dual role to use data generated through the transactions that business users complete through its platform to gain a competitive edge in offering similar services to that of its business users.[18]

The DMA seeks to prevent gatekeepers from 'unfairly benefitting' from their dual role. It provides several obligations to ensure that gatekeepers avoid using exclusively any data generated

16 Point (12) in the introduction of the proposal.

17 Section 2. *Proportionality* in the Explanatory Memorandum and Art. 4.1.b.

18 Point (43) and (45) of the introduction.

through their platforms to the disadvantage of their business users. These obligations include the following:

- **Art. 6(a)** Cannot use, in competition with business users, data generated through business user's activity (incl. its end users).
- **Art. 6(i)** Provide to business users (or authorised third parties) free, effective, high-quality, continuous and real-time access and use of (non-)aggregated data provided for or generated through the (use of) core platform services.

Data portability

More generally, the DMA enforces data portability:

- **Art. 6(h)** Allow for portability of and real-time access to data generated through activity on the gatekeeper's platform.

Third-party listing

The DMA could also impact the way infrastructure providers currently decide which third-party vendors' add-ons to list on their marketplaces:

- **Art. 6(k)** Accept businesses' apps on a 'fair and non-discriminatory' basis if the gatekeeper provides app stores.

Third-party transactions

The DMA could impact the current business model of large digital platform services providers, in particular, if they are charging a commission on the conclusion of transactions going through their online marketplace:

- **Art. 5(c)** Allow business users to promote offers to end users acquired on the gatekeeper's platform and to conclude contracts with end users outside the gatekeeper's platform.

Self-preferencing

The DMA could also impact the way large digital platforms currently might be designing their services, customer interfaces and online marketplaces to make their offerings more visible, accessible and easily integrable than equivalent offerings from third-party vendors:

- **Art. 6(d)** Cannot treat services or products offered by the gatekeeper more favourably in ranking than similar services or products offered by third parties on the gatekeeper's platform.

Default services lock-in

The DMA could also impact the lock-in methods that large digital platforms might currently be using on end users and business users in some cases, by subscribing them to default add-ons and services and preventing them from switching away from those:

- **Art. 6(b)** Cannot prevent end users from uninstalling any pre-installed software or app if they wish to do so.
- **Art. 6(e)** Cannot technically restrict end user from switching away from default apps and services.
- **Art. 5(f)** Cannot force business users or end users to subscribe to any other core platform services of the gatekeeper.

Interoperability

The EC is also concerned with the risk of a lack of choice, contestability and innovation in providing ancillary services. Ancillary services are defined as '*services provided in the context of or together with core platform services*' (Art. 2.14). Examples include payment, fulfilment, identification or advertising services. The EC highlights that gatekeepers have an incentive to favour their ancillary services over those of third parties to support their core platform services.[19] The EC wants to ensure that third parties are not kept away from providing ancillary services to gatekeepers' core platform services by obliging gatekeepers to provide third parties with the same conditions as are available to themselves when interoperating ancillary with core platform services:[20]

- **Art. 6(f)** Allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services.

19 Point (14) of the introduction.
20 Point (52) of the introduction.

This could impact the way certain large digital services providers currently operate an integrated digital services ecosystem (for example, cloud infrastructure providers).

Transparency requirements

The DMA also enforces several transparency requirements on gatekeepers that could impact the way large digital services providers are currently making strategic decisions:

- **Art. 13** An annually audited description of consumer profiling techniques.
- **Art. 12** Gatekeepers will have to inform the EC of any proposed transaction or 'intended concentration' involving another provider of core platform services or of any other services provided in the digital sector, regardless of whether the transaction is reportable under the existing EU Merger Regulation or EU member countries' merger control rules. This could open a channel by which the EC might more proactively review transactions in the tech space that would otherwise fall outside its jurisdiction.[21]

2.3.2 The UK's 'pro-competition regime' for digital markets

Based on a motivation similar to the EC's, the UK Government is introducing a new pro-competition regime for digital markets to be overseen by the Digital Markets Unit (DMU) within the Competition and Markets Authority (CMA). It was expected to come into force in October 2023. The DMU's approach is to prevent harm and ensure compliance proactively through an *ex ante* pro-competition framework, rather than having to correct and enforce *ex post*. The entry point is an evidence-based economic assessment of whether a firm has strategic market status (SMS) in a designated activity; that is, substantial, entrenched market power in at least one digital activity, providing the firm with a strategic position that can give rise to harm to market competition. Firms deemed to have SMS must comply with the following pillars of the SMS regime:

- Tailored conduct requirements to govern the relationships between the most powerful firms and the different users that rely on their services. These will promote fair trading, open choices, trust and transparency.
- New 'pro-competitive interventions' (PCIs) to address the underlying causes of market power and to open up digital markets to greater competition. Examples of PCIs the DMU could utilise include: promoting data portability of personal data; consumer choice and default interventions; and separation remedies.
- Merger rules requiring SMS firms to submit to the CMA a light-touch report of all transactions before their completion that meet specific criteria.

2.3.3 US investigations into issues related to digital markets and the latest corresponding legislative initiatives

In October 2020, the US House Judiciary Committee's Subcommittee on Antitrust, Commercial, and Administrative Law ('the Subcommittee') released an extensive report following its investigation assessing the state of online competition in digital markets (US House Judiciary Committee 2020). In particular, the investigation looks into the potentially anti-competitive conduct of four dominant firms in digital markets and evaluates the adequacy of current laws and regulations in addressing identified risks and issues.[22] The investigation was conducted through oversite hearings with witnesses, including executives from firms raising concerns about the dominant firms, key executives from Facebook, Amazon, Google and Apple, and experts, including academics, representatives of public interest groups and anti-trust lawyers. Detailed information from the investigated platforms, other market participants, federal anti-trust agencies and other relevant parties were also gathered as part of the investigation.

The report highlights potential concerns surrounding the increasing market power of the largest digital firms, while acknowledging that the digital economy has brought significant benefits to the US economy. The report finds that the digital

21 Using powers conferred under Article 22 of the EU Merger Regulation.

22 Online platforms investigated were Amazon, Apple, Facebook and Google.

economy has become highly concentrated, with several markets (such as social networking, online search and online advertising) being dominated by one or two firms only. Investigating Amazon, Apple, Facebook and Google highlighted that key channels of distribution have been captured by these companies, which function as gatekeepers for the rest of the market. Moreover, the high volume of acquisitions through which dominant digital platforms have acquired nascent or potential competition to eliminate potential competitive threats is one of the key contributing factors to their market power.

The investigation also leveraged the input of anti-trust and competition policy experts to examine and evaluate the adequacy of current laws and enforcement tools in addressing the identified competition issues and risks in digital markets.

The policy recommendations show the influence of a paper by Khan (2019). According to Khan, a few very large digital platforms have access to markets and act as gatekeepers for substantial economic activity. The integrative structure of these large digital platforms means they both connect end users to vendors and market their products and services. This could lead to a conflict of interest, where the digital platforms directly compete with the same third-party businesses that depend on them to market their products and services to customers. Third-party vendors face risks of discrimination, lock-in and appropriation from these large digital platforms.

The Subcommittee's recommendations fall into the following three categories: those aimed at restoring competition in digital markets; those aimed at strengthening anti-trust laws; and those aimed at strengthening oversight and enforcement of anti-trust laws.

The first set of proposed remedies aims to **restore competition in digital markets** and mitigate risks of harmful business practices leading to the creation of monopolies:

- The dominant firms investigated by the Subcommittee are integrated across multiple lines of business. This leads to concerns of these firms exploiting their dominance in one market to leverage negotiations in another market or using supra-competitive profits from one market to subsidise entry and expansion in another market. To address these concerns, the Subcommittee suggests two tools. First, structural separations can be used to prohibit a dominant platform from operating in markets that compete with firms dependent on its infrastructure to access customers. Second, line of business restrictions could limit the markets in which a dominant firm can engage.
- To prevent dominant platforms from engaging in self-preferencing, the Subcommittee recommends establishing non-discrimination rules. Such rules would require dominant platforms to offer equal terms for equal services, applying both to prices as well as terms of access.
- The Subcommittee encourages data portability and interoperability to lower entry barriers to the Infrastructure as a service (IaaS) market and reduce switching costs for consumers. Platforms would be required to make their services compatible with other networks and make data and information portable between different networks.
- According to the House report, it is unclear whether US anti-trust agencies are currently equipped to block anti-competitive mergers in digital markets. There is evidence in this area hinting at significant missteps and enforcement failures. As a result, the Subcommittee recommends a shift in presumptions for future acquisitions by dominant platforms. This means that an acquisition would be presumed anti-competitive unless the merging parties can demonstrate that the transaction serves the public interest and that similar benefits cannot be realised through internal growth.
- Dominant platforms often enjoy superior bargaining power over third-party vendors who depend on the platforms to access customers. Given such market power, there is a risk the dominant platforms can charge higher prices and extract more data from their customers than in a more competitive market scenario. For example, dominating platforms could exploit their bargaining power to charge higher prices to third-party vendors who need to market services through the dominant platforms. To alleviate these issues, the Subcommittee recommends prohibiting

the abuse of superior bargaining power. This includes targeting anti-competitive contracts, as well as introducing due process protections for individuals and businesses dependent on the dominant platforms.

Latest US federal legislative developments

Throughout 2021 and 2022, several bills targeting greater anti-trust regulation, data protection and even child protections online have been introduced across both US Congress chambers (Paul et al. 2022). However, as of the time of writing, they have not been brought to a vote or won over the majority (Schaake 2023). These initiatives include:

- **American Choice and Innovation Online Act**: This would prohibit digital platforms from self-preferencing their products over those of competitors that use their platforms. The FTC planned to create a bureau of digital markets tasked specifically with enforcing this Act.
- **American Data Privacy and Protection Act**: This would create national standards and safeguards for personal information collected by companies, including protections intended to address the potentially discriminatory impacts of algorithms (Patel et al. 2022).
- **Platform Competition and Opportunity Act**: This would prohibit any platform with 'at least 50,000,000 United States-based monthly active users' – such as Facebook, Google, Apple or Amazon – from holding more than a quarter of a competitor's stock or profits, limiting their capacity to take over a competitor entirely.
- **Ending Platform Monopolies Act**: This would prohibit dominant platforms from creating and owning business lines that present clear conflicts of interest. This bill is the most controversial, with some legal experts arguing that it could prevent the tech giants from competing against one another (Bowman 2021).
- **Augmenting Compatibility and Competition by Enabling Service Switching Act:** This would prohibit platforms from making changes that can reduce interoperability and allow consumers to easily move their data from one platform to another. This bill would also require platforms of a certain size to let users take some (or even all) of their data with them if they choose to leave the platform, while still being able to chat and check in with friends and family that use these services. It is aimed at providing consumers with more control and transparency over their data.
- **State Antitrust Enforcement Venue Act**: This would prohibit large tech corporations from shifting anti-trust proceedings to face courts that might be perceived as friendlier to corporations and/or to drive up the cost and the length of litigation.
- **Merger Filing Fee Modernization Act**: This would increase the resources to the Department of Justice and the FTC for the enforcement of anti-trust laws. It would substantially increase the fees that large corporations will need to pay for large transactions, like mergers.

2.3.4 India

In India, regulatory scrutiny over large tech firms has intensified recently, driven by concerns over data protection and competition, as well as protectionism and national security. Most recently, in December 2022, the Standing Committee on Finance submitted its report on *Anti-Competitive Practices by Big Tech Companies* (Standing Committee on Finance 2022). This report provides recommendations aimed at strengthening India's regulatory framework governing firms operating in digital markets that strongly align with the EU's DMA. These recommendations include the need to:

- Identify 'systemically important digital intermediaries' (SIDIs); that is, leading players in digital markets with market power to negatively impact competition in those markets ('gatekeepers'). SIDIs should have reporting obligations to the Competition Commission of India (CCI) to provide evidence of compliance with various mandatory obligations.
- Strengthen the CCI with the creation of a specialised digital markets unit within the CCI that would: (i) monitor established and emerging SIDIs; (ii) give recommendations to the central government on designating SIDIs; and (iii) adjudicate on cases related to digital markets.

- Introduce a Digital Competition Act that provides *ex ante* regulation targeting SIDIs aimed at ensuring a fair, transparent and contestable digital ecosystem. For example, the regulation would prohibit platforms from self-preferencing and locking out third-party payment services, as well as exploitative practices like forced exclusivity agreements.

Following up on this report, in February 2023, the CCI set up a committee to evaluate anti-trust legislation and draft a Digital Competition Act, with publication aimed to be delivered within three months (CPI 2023).

Moreover, the CCI is currently in the process of setting up a Digital Markets and Data Unit (DMDU), which will act as a dedicated interdisciplinary centre of expertise for digital markets. Key roles and responsibilities of the DMDU include (Bundeskartellamt 2022):

- facilitating exchanges between academic experts across various disciplines, industry representatives, and other regulators, departments and international agencies *inter alia*;
- undertaking analytics and management of data and information related to digital markets; and
- providing inputs and recommendations on policy issues and competition cases related to digital markets.

2.3.5 Brazil

Brazil's anti-trust authority, the Administrative Council for Economic Defence (CADE) has increased its focus over matters involving digital markets in recent years. In 2021, together with the Department of Economic Studies (DEE), it published a study analysing competition dynamics and issues in digital markets and highlighted the need to increase regulatory attention over identified issues (Conselho Administrativo de Defesa Econômica 2021). At the start of 2023, the new government of President Lula da Silva announced its intention to regulate digital platforms in its first 100 days in office and has created a new Secretariat for digital policies. A key focus of the new government unit is to regulate monetised content on digital platforms and hold digital platforms accountable for the content that disseminates or promotes misinformation, hate speech and other crimes (Government of Brazil 2023). Moreover, a digital competition bill project was presented to the Brazilian Congress in November 2022 and was under review at the time of writing. It focuses on regulating digital platforms, especially those identified as having 'the power to control essential access', which is similar to the EU DMA 'gatekeepers' concept. It defines some general principles, but more detailed rules and enforcement will be undertaken by the National Telecommunications Agency (ANATEL).

2.3.6 South Africa

The South African Competition Commission (SACC) is taking active steps aimed at assessing and addressing potential competition concerns in digital markets. In May 2021, it launched the Online Market Inquiry, which investigates potential issues and gaps in regulating competition in digital markets, with a focus on B2C platforms (for example, online marketplaces). The inquiry has recently been extended, but its outcome will likely provide a clearer view of SACC's approach to digital markets and the resulting recommendations could be binding for firms operating in digital markets. The SACC also published revised *Guidelines on Small Merger Notification* (Competition Commission South Africa 2022) in September 2022, which became effective as of December in that same year. *The Guidelines* require that parties voluntarily notify the SACC of all small mergers that meet certain financial and market share thresholds.[23] The *Small Merger Guidelines* were revised due to increasing concerns by the SACC that potential anti-competitive small mergers in digital markets that did not require mandatory notification could circumvent regulatory scrutiny (Tzarevski and Hansen 2022).

In addition, the SACC published new provisions related to dominant buyers, the *Buyer Power Enforcement Guidelines* (Competition Commission South Africa 2020), in May 2020. *The Guidelines* prohibit a dominant buyer in the e-commerce and digital services sector from requiring or imposing unfair prices or trading terms on supplier firms operated by historically disadvantaged persons (HDPs) or small and medium-sized enterprise (SME) sellers.

23 However, these small mergers do not meet the existing mandatory notification thresholds.

Table 2.2 Overview of existing CSME competition laws

Member states	Dedicated competition legislation [a]	Sector-specific competition provisions [b]
Antigua and Barbuda	N/A	Telecommunications Act
Barbados	Fair Competition Act Fair Trading Commission Act	Telecommunications Act Utilities Regulation Act
Belize	N/A	Telecommunications Act Public Utilities Commission Act
Dominica	N/A	Telecommunications Act Electricity Supply Act
Grenada	N/A	Telecommunications Act Public Utilities Regulatory Commission Act
Guyana	Competition & Fair Trading Act	Telecommunications Act Public Utilities Commission Act
Jamaica	Fair Competition Act	Telecommunications Act Office of Utilities Regulation Act
Montserrat	N/A	Info-communications development Act
Saint Lucia	N/A	Telecommunications Act Electricity Supply Act National Utilities Regulatory Commission Act
St Kitts and Nevis	N/A	Telecommunications Act Electricity Supply Act Public Utilities Act
St Vincent and the Grenadines	N/A	Telecommunications Act Electricity Supply Act
Suriname	N/A	Telecommunications Act
Trinidad and Tobago	Fair Trading Act	Telecommunications Act Financial Institutions Act Regulated Industries Act

Note: (a) 'Dedicated competition legislation' means a single enactment that contains the pillars of competition law together with institutional arrangements for enforcement. (b) 'Sector-specific competition provisions' include statutory instruments (whether as regulations, orders, codes, etc.) that contain provisions which may be interpreted or applied to address specific competition concerns in a sector or industry.
Source: CCC (2022).

2.4 The situation in the CSME

This section provides a review of CSME competition laws' rules for digital markets, leveraging on the CCC's work on competition enforcement in digital markets. The CCC recognises that:

> *the growth of the digital market has raised several competition issues discussed at the international level. Among these issues include defining relevant markets and assessing market power in platform markets; the effects of big data on competition; and the relevance of regulation. Given the discussions at the international level, in 2019 the CCC convened a meeting among the competition authorities in the region to discuss their views on defining relevant markets in two-sided markets. The meeting aimed at harmonising the enforcement practices in the region concerning digital markets.* (CCC, 2022)[24]

The CCC undertook a 2022 overview of the existing CSME competition laws (see Table 2.2), which form the basis of this analysis.

24 CARICOM Competition Commission. (2022). *State Of Competition Enforcement In The CSME (2019-2021), p.15.*

Table 2.3 Examples of data access remedies

Facilitating factors	Data-induced switching costs Network effects & platforms	Exclusive data access Exploitative data access	Economies of scale Digital ecosystems & economies of scope
Regulatory approach	**Empowering users**	**Data openness**	**Limiting data scale**
Remedies:	**Data portability & transparency**	**Access obligations & bulk data sharing**	**Data silos & structural separation**
IT artifacts:	• User interfaces • Personal information management systems • Data portability APIs and data exchange protocols	• B2B-APIs for large-scale data transfers • PETs for data sharing Security and compatibility of information systems	• Decentralized and disintegrated information systems • Data access control and user consent management • RegTech capabilities for monitoring and auditing

Note: Application Programming Interface (API), Privacy Enhancing Technologies (PETs).
Source: Schnurr, D (2023).

Our review of the competition laws of Barbados, Trinidad and Tobago, Guyana and Jamaica found that they do not include specific provisions aimed at digital markets, nor are topics that are of particular relevance for digital platforms (such as two-sided markets) explicitly addressed.[25] The laws are largely focused on *ex post* enforcement against infringements, including horizontal and vertical (retail price maintenance) restraints and abuse by dominant firms (for example, excessive prices). *Ex ante* provisions in the form of merger control provisions are included in the competition statutes in Barbados, Trinidad and Tobago, and Jamaica.[26]

This means that the CARICOM member countries have so far not embraced the trend seen in some major jurisdictions towards a specific *ex ante* regulation approach aimed at large digital platforms, as exemplified by the EU's Digital Markets Act.

Moreover, a notable feature that may weaken the power of the laws in relation to large digital platforms is the relatively low level of maximum applicable fines in case of non-compliance (1 million Guyana dollars [G$] for individuals and 10 millions for firms in Guyana;[27] 1 million Jamaican dollars [J$] for individuals and 5 million for firms in Jamaica;[28] versus up to 10 per cent of turnover in Trinidad and Tobago and Barbados – although this is not explicitly global turnover).

There is also no provision for conduct remedies, which are of particular relevance in cases where: a) even very high fines may have limited deterrence effect; and b) where restoring or safeguarding competition requires targeted measures specific to the digital activities of the firms in question (see Table 2.3).

25 However, on the enforcement level, two-sided markets are very much on the agenda: The CCC's *State of competition enforcement In the CSME (2019-2021)* report states: 'The growth of the digital market has raised several competition issues discussed at the international level. Among these issues include defining relevant markets and assessing market power in platform markets; the effects of big data on competition; and the relevance of regulation. Given the discussions at the international level, in 2019, the CCC convened a meeting amongst the competition authorities in the region to discuss their views on defining relevant markets in two-sided markets. The meeting aimed at harmonising the enforcement practices in the region concerning digital markets.' (CCC (2022), p. 15)

26 The Barbados and Trinidad and Tobago competition statutes include merger control provisions. Jamaica's competition legislation has been interpreted as including *ex ante* merger control in the UK Privy Council decision in *Fair Trading Commission v Digicel Jamaica Ltd and Another* [2017] UKPC 28.

27 Less than US$5,000 (individual) and US$50,000 (firm): 1 Guyanese dollar (GYD) is equal to US$0.0048 (as of 31/07/2023).

28 Less than US$6,500 (individual) and US$32,500 (firm): 1 Jamaican dollar (JMD) is equal to US$0.0065 (as of 31/07/2023).

Telecommunications, such as the Eastern Caribbean Telecommunications Authority (ECTEL) Electronic Communications Bill (ECTEL 2020), have their own competition and merger procedures. However, sector-specific legislation does not apply to pure providers of electronic services (that is, firms that are not involved in the provision of electronic communications networks and electronic communications services). While some large digital businesses are involved in the provision of electronic communications services,[29] this is not the rule.

2.5 Gaps and recommendations

This section provides a discussion on the gaps in competition enforcement in digital markets in CSME member countries and policy recommendations to address these gaps.

Incomplete legal framework in the CSME

The majority (9 out of 13) CSME member countries do not have competition laws. CSME-wide alignment of competition policy for digital markets requires that there are no gaps in the legal framework that can be exploited by firms' location decision within the CSME. Given the small size of some CSME member countries, the extent to which they can leverage on existing CSME sructures and specifically the capabilities of the CCC is a question for internal co-ordination within the CSME.

Lack of data on the CSME digital economy

An effective competition policy for the CSME digital sector should be based on a thorough understanding of the issues faced by businesses and consumers. To provide the CCC with accurate and up-to-date information, the CCC should conduct research on the prevalence and impact of the issues discussed in this report. This should include surveys of businesses and consumers in the CSME. Relevant research topics include:

- How active are regional businesses operating within the digital space?
- What are the views of regional businesses on data protection and privacy?
- Have regional businesses experienced anti-competitive business conduct in digital markets?
- Are regional consumers more confident sharing personal information online with companies that have websites with privacy policies?

The empirical evidence from such further research into the CSME digital market will enable the CCC to derive more effective and detailed policy recommendations.

Lack of *ex ante* competition enforcement targeting dominant firms in digital markets

CSME member countries have so far not developed specific *ex ante* competition enforcement laws aimed at regulating the behaviour of large firms in digital markets – unlike the EU with the DMA and the UK with its new pro-competition regime for digital markets. Although there is no firm evidence to support this, there is a risk that consumers in the CSME end up facing a reduced choice and more expensive and lower-quality products and services than those available in digital markets abroad, while local firms operating in digital markets could face unfavourable business terms and/or high entry barriers.

There may be limited grounds for competition authorities in the CSME to replicate the activities undertaken by the EU and UK regulators. Traditional competition law, which focuses on the investigation and punishment of anti-competitive practices (*ex post*) and the prevention of mergers resulting in less competitive markets (*ex ante*), has proved flexible and effective in many different market settings, including contemporary digital markets. All current case law, including record fines and far-reaching structural remedies against some of the biggest digital firms, has been developed under existing competiton laws.

At the same time, for the small CSME jurisdictions, the resources needed to maintain a specific regulatory unit like the UK's DMU to separately monitor the behaviour of large international tech firms and develop bespoke *ex ante* conduct

29 Including Amazon's initiative to provide satellite internet services through a constellation of low earth orbit (LEO) satellites ('Project Kuiper'); and Meta's – now discontinued – 'Free Basics' and 'Express Wi-Fi' programmes, which aimed to provide affordable internet access in partnership with local Internet service providers (ISPs) and mobile operators in 20 countries, including India, the Philippines and South Africa.

remedies to address anti-competitive concerns within its local markets are likely disproportionate to the benefit.

Instead, CSME authorities could adopt a 'fast-follower' approach to digital market regulation and leverage on what leading jurisdictions are doing to ensure CSME consumers and businesses face similarly favourable terms in digital markets. This would involve close monitoring of international regulatory developments and systematic review of lessons relevant to the CSME. Activities such as participation in international forums and conferences, as well as personnel exchanges/secondments with leading competition authorities and specialist units in charge of digital market regulation, are important components of this approach.

Competition authorities in the CSME should be vested with additional powers to require large digital platforms to mirror any pro-competitive conduct remedies they had to implement that benefit EU/UK firms and consumers in CSME markets. This will likely involve significantly increasing the maximum penalty limits that competition authorities can impose in case of non-compliance.

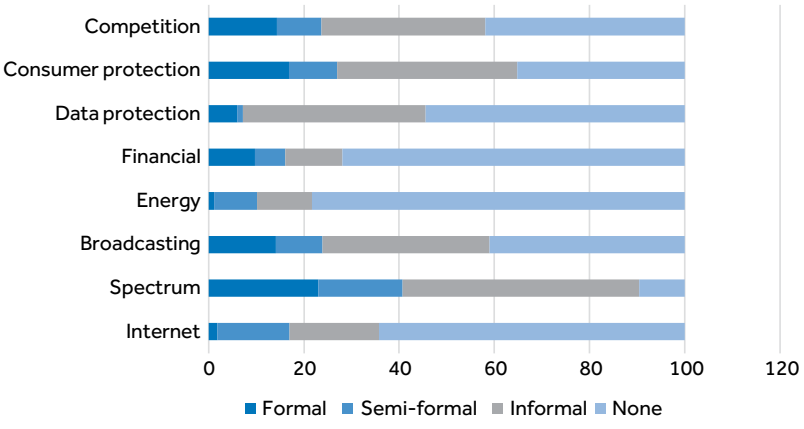
In terms of merger control, there are similarly limited grounds for competition authorities in the CSME to start reviewing transactions between large international firms – as they will have little to no impact on competition in local markets. Nevertheless, they should be empowered to review transactions in digital markets that could potentially affect local markets and consumers negatively. At the same time, the merger control regime should reserve the flexibility to allow for local businesses to be acquired by large tech firms as part of a successful exit strategy and where the adverse impact on consumers through reduced competition in the local economy is limited.

Increased regulatory co-operation

There is also an opportunity for competition authorities in the CSME to co-operate on competition issues in digital markets with adjacent regulatory authorities, such as the telecoms regulator. For example, competition issues involving digital platforms and their electronic communications services would fall within the remit of general competition law, but competition authorities may collaborate on a case-by-case basis with the telecoms regulator where its specific expertise is required. Regulatory co-operation and resulting synergies could be particularly valuable in the case of small jurisdictions like in the CSME, where resources available to regulatory authorities are relatively limited.

However, this model of co-operation remains relatively new and unproven. In the UK, the Competition and Markets Authority (CMA), Ofcom, the telecoms regulator and the Information Commissioner's Office (ICO) have only recently established a common forum, the Digital Regulation Cooperation Forum (DRCF) (Schlesinger 2022), to consult with one another and co-operate and co-ordinate on how to tackle regulatory issues in the digital space. A World Bank graphical analysis shows that formal collaboration between different

Figure 2.1 State of regulatory collaboration between ICT regulators and other authorities in cases where both exist and are separate entities, worldwide (2018)



Source: International Telecom Union (2018).

digital market regulators is currently not widespread, although some information and communication technology (ICT) regulators do co-operate with the spectrum[30], consumer protection and competition regulators (see Figure 2.1).

As the effectiveness of regulatory co-operation is unproved and might be undermined by inter-institutional competition, a cautious approach should be taken, starting with low-cost measures such as information sharing mechanisms, before progressing to more formal arrangements such as shared task forces.

Increased regional regulatory alignment

Harmonised competition laws facilitate the implementation of the CSME, while promoting and facilitating the development of the CSME internal market is a core responsibility of the CCC. The CCC has a significant role to play in ensuring that CSME countries remain aligned when developing their approach to regulating competition in digital markets and in general. Heterogeneity in regulatory frameworks across the region (and the gap in the legal framework for competition in 9 of the 13 CSME member countries discussed above) can significantly undermine welfare gains in the form of foregone trade and innovation. This is particularly the case in digital markets, where the transboundary nature of digital products and services should allow for firms to expand to new markets and potentially spread beneficial digital innovations more seamlessly (OECD 2019). Regulatory heterogeneity and the resulting complexity of complying with varying regulatory frameworks can discourage companies from entering markets in new jurisdictions. Moreover, regulatory heterogeneity can end up hindering competition, as it works to the advantage of large incumbent firms. The latter are more likely than new and smaller companies to have the resources and experience to navigate through the various frameworks and requirements (Brauer and Erixon 2016).

30 Spectrum refers to the radio frequency spectrum, i.e. the range of electromagnetic frequencies used for transmitting data wirelessly, including for various forms of communication such as radio, television, mobile phones, Wi-Fi, and other wireless technologies.

3. Data Protection

Key findings

- Data protection laws aim to protect individuals' personal information from unauthorised collection, storage, processing and disclosure. These laws aim to balance the need for personal information with the need to protect individual privacy, while promoting responsible data practices and encouraging trust and confidence in digital technologies.
- The European General Data Protection Regulation (GDPR) was introduced in 2018 and serves as a good template for international data protection laws.
- Eight CSME member countries have enacted data protection and privacy laws, though these laws contain gaps compared to the GDPR.
- Fully replicating GDPR could be complex and expensive, while harmonising legislation might not eliminate all risks. Prioritising citizens' data protection needs within the CSME is important, but regional differences can affect cross-border data flows.
- The CCC could play an important role in driving increased regional harmonisation across the CSME to ensure frictionless international data flows, using the HIPCAR model law as a potential basis for enhancing cross-border data transfer rules.

3.1 Background

Data protection laws aim to protect individuals' personal information from unauthorised collection, storage, processing and disclosure. These laws aim to balance the need for personal information with the need to protect individual privacy and maintain national security, while promoting responsible data practices and encouraging trust and confidence in digital technologies.

While data protection laws are principally concerned with the fundamental human right to privacy, they have significant effects on economic activity, specifically competition and business models in the digital economy, as well as cross-border data transfers.

3.2 International developments

3.2.1 European Union: General Data Protection Regulation (GDPR)

The European General Data Protection Regulation (GDPR) was introduced in 2018. It establishes a comprehensive set of rules for the collection, processing and protection of personal data of EU citizens, regardless of where the data is processed. This extraterritorial scope means companies worldwide must comply if handling EU citizen data. Besides providing standard data protection rights to consumers, the GDPR contains elements of economic regulation – with implications for competition in data-intensive digital markets. These elements include the right of access, the right to data portability and rules for international transfers of personal data. The EU GDPR has been globally influential and many international data protection laws share key features with it.

Data processing principles and consent mechanism

The GDPR provides principles for processing personal data including lawfulness, fairness, transparency, purpose limitation and data minimisation (GDPR Art. 5). Personal data should only be collected and processed for specified, explicit and legitimate purposes and only data that are strictly necessary should be collected and processed. Consent of the data subject to the processing of his or her personal data must be unambiguous and informed. Consent has to be requested in an intelligible and easily accessible form, using clear and plain language, be given for one or more specific purposes, and can be removed at any time (GDPR Arts. 6 and 7).

The limitations placed on data used by businesses by the GDPR provisions on consent for processing, purpose limitation and data minimisation have increasingly been incorporated into the practices of internationally operating firms, especially those that are exposed to the EU market, including the large American digital platforms. Within the EU, GDPR has had an impact on the business models of many companies, in particular those that rely heavily on collecting, processing and monetising personal data. For example, businesses involved in unsolicited marketing emails or targeted advertising have had to shift to a consent-based approach. Similarly, businesses that used to rely on monetisation of user data without users' explicit consent or awareness have had to update their terms and conditions and privacy policies and/or seek alternative revenue models. GDPR-driven changes on revenue models, coupled with the costs of implementing GDPR-compliant processes and technologies, have been costly for many businesses. There is some evidence that the GDPR has had a negative impact on the profit of firms exposed to European Union markets (Chen et al. 2022). While the evidence is not conclusive, the effects are likely more concentrated in consumer-facing industries, including digital platforms and the marketing industry. Increased friction in online transactions through consent mechanisms introduced by data protection measures can negatively impact online purchases and sales (Ibid). Other studies have found negative effects on web traffic and online sales (Goldberg et al. 2019); and early-stage investment in technology companies (Jia et al. 2021).

Right of access[31]

The GDPR provides individuals with the right to obtain various types of information relating to their data from a company or organisation, including whether the latter processes their data, the categories of personal data concerned, the source of the personal data, the purpose of the processing, and the recipients or types of recipients to whom the personal data will be disclosed. Individuals also have the right to know whether any automated decision-making (including profiling) has been involved and to obtain meaningful information about the underlying logic, the significance and the foreseen consequences of such processing for the data subject. Individuals may also obtain a copy of the personal data being processed from the relevant company, free for the first copy and in a commonly used electronic format if requested.

The right of access paves the way for individuals to exercise further rights (for example, rectification and erasure) (Intersoft Consulting n.d.). It has significant implications for the way businesses operate and engage with consumers, in particular businesses for which individual-level data processing is a key component of their activities. It provides consumers with transparency on how businesses are using their data, allowing them to make informed decisions about engaging with their products and services. This introduces a new element of comparability or product differentiation, against which:

- consumers can assess the quality of digital products and services and make choices; and
- firms can compete, for example, by innovating to provide products and services that minimise personal data collection and processing.

Right to data portability[32]

Individuals have the right to receive from a company or organisation the personal data they provided in a structured and commonly used machine-readable format and to have it sent to another company/organisation. This right applies only to cases where personal data was collected via a contract or based on consent and processed through automation (European Commission n.d.).

Data portability has been identified as one of the key pro-competitive measures in digital markets. Theoretically, data portability can empower consumers to choose among competing providers by reducing user switching costs and frictions associated with trying new services. This can stimulate competition in markets where personal user data is valuable, by making it easier for new entrants to attract users; that is, by reducing barriers of entry associated with data access (OECD 2021).

In practice, the effect of the right to data portability has been very limited. The right is rarely exercised by consumers and its usefulness is limited by the narrow scope (user-provided data) and lack of

31 GDPR, Article 15.

32 GDPR, Article 20.

specificity about how the data needs to be shared. This has led some to argue that the right of access is, in fact, the stronger enabler of data sharing (which is arguably reflected in the data sharing provisions of the draft EU Data Act concerning 'internet of things' [IoT] data).

3.2.2 The California Consumer Privacy Act (CCPA) and Privacy Rights Act (CPRA)

The California Consumer Privacy Act (CCPA) is a state law in California that came into force in January 2020 and provides Californian residents with certain rights and protections over their personal information collected by businesses (State of California Department of Justice 2023).

The CCPA applies to businesses that meet certain thresholds, including those that have annual gross revenues of at least US$25 million, that buy, receive or sell the personal information of at least 50,000 California residents, households or devices each year, or that derive at least 50 per cent of their annual revenues from selling California residents' personal information.

Under the CCPA, California residents have the right to know what personal information a business has collected about them, the right to request that the business delete their personal information and the right to opt-out of the sale of their personal information. The CCPA also requires businesses to provide certain disclosures to California residents about their data collection practices, including the categories of personal information collected, the purposes for which the information is used and the categories of third parties with whom the information is shared. It also provides California residents with a private right of action to seek damages if their personal information is subject to a data breach that results from a business's failure to implement reasonable security measures.

The CCPA shares similarities with the GDPR. Both laws:

- give individuals the right to know what personal information is being collected about them and the right to request that the information be deleted;
- require businesses to provide certain disclosures about their data collection and sharing practices; and
- apply to businesses that meet certain thresholds, such as having a certain amount of revenue or collecting a certain amount of personal data.

However, the CCPA differs from the GDPR in terms of consent requirements and penalties for non-compliance. For example, unlike the GDPR, the CCPA does not require businesses to obtain explicit consent from individuals before collecting or using their personal information. The GDPR also has requirements for data breach notification, privacy by design and data protection impact assessments, that are not included in the CCPA. The CCPA imposes fines up to US$7,500 per violation, which is substantially smaller than the fines imposed by the GDPR, which can be up to 4 per cent of a company's annual global revenue. The GDPR requires businesses to appoint a Data Protection Officer (DPO) in certain circumstances, while the CCPA does not have such a requirement.

The California Privacy Rights Act (CPRA) came into force in January 2023 to amend and expand on the CCPA, providing Californians with additional privacy rights and protections. It closes some of the previous gaps with the GDPR, with key changes and additions including:[33]

- the creation of a new regulatory agency, the California Privacy Protection Agency, dedicated to enforcing the state's privacy laws and protecting Californians' privacy rights;
- the expansion of the definition of sensitive personal information to include things like geolocation data, racial or ethnic origin, and genetic data;
- the right for individuals to correct inaccurate personal information held by businesses;
- limitations on how long businesses can retain personal information;
- enhanced protections for minors, including the right to request the deletion of personal information that was collected when they were minors; and

33 Bloomberg Law, *California Consumer Privacy Laws – CCPA and CPRA*, available at: https://pro.bloomberglaw.com/brief/california-consumer-privacy-laws-ccpa-cpra/#:~:text=The%20CCPA%20vests%20the%20California

- limitations on the use of the 'pay-for-privacy' scheme, through which businesses are prohibited from charging higher prices or providing lower-quality services to consumers who exercise their privacy rights.

3.2.3 India

India's Digital Personal Data Protection Bill was passed by the Indian Parliament on 09 August 2023 after a lengthy legislative process. The Bill has been substantially revised from its 2019 version, in particular concerning its severely restrictive stance on cross-border data traffic (that is, the data localisation requirement). It includes the now standard set of rights for data subjects ('Principals' in the language of the Bill), including the right of access, the right to correction and deletion, and the right to complain. It also includes highly specific rules on consent. However, the Bill has faced criticism for government exemptions (Human Rights Watch 2022).[34]

The Bill creates the Data Protection Board of India, with the power to impose penalties ranging from US$120 to US$30.2 million. Unusually, the Bill also provides for fines (of up to US$120) for data subjects who fail 'to ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board'.

For international data transfers, the Bill presumes that transfers may occur without restrictions, unless the central government specifically restricts transfers to certain countries ('blacklisting'). This is a significant departure not only from the previous drafts of the Bill, but from GDPR's 'whitelisting' approach.

3.2.4 Brazil

Brazil's General Data Protection Law (LGPD) came into force in September 2020. The LGPD is the first comprehensive data protection regulation in Brazil and South America and broadly aligns with the GDPR (DLA Piper 2023). Moreover, as of February 2022, data protection, including in digital media, is now encompassed as a fundamental right in the Brazilian Constitution.

3.2.5 South Africa

The Republic of South Africa promulgated its first specific data protection legislation, the Protection of Personal Information Act (POPIA)[35] in 2013. The law was finally enacted in July 2021, except for Section 58[36], which became enforceable as of February 2022.

In addition to the POPIA, the following legislation includes provisions on data privacy and protection:

- The Constitution of the Republic of South Africa (1996)[37] guarantees the right to privacy.
- The Electronic Communications and Transactions Act (2002)[38] includes provisions on data protection in the electronic collection of personal information. However, compliance with those provisions was mandatory and they were eventually repealed in June 2021.
- The Consumer Protection Act (2008)[39] prohibits unsolicited direct and telephonic marketing and communications. This may overlap with the provisions of the POPIA, which apply to unsolicited electronic communications specifically.
- The Cybercrimes Act (2020)[40] criminalises and sanctions various acts in the digital space (for example, data theft and interference, dissemination of harmful data messages, cyber fraud).

34 Similar concerns have been raised over the new telecom bill that proposes to introduce a licensing regime for telecom and internet service providers and empower government executives with the capacity of interception and surveillance of communications when deemed 'necessary or expedient' to safeguard national security or in cases of public emergencies. The latter could be exercised with limited oversight from the parliament or judiciary.

35 Protection of Personal Information Act (2013), available at: www.dataguidance.com/sites/default/files/popia_2013.pdf

36 Section 58 includes further provisions on the notification and prior authorisation mechanisms that apply to organisations looking to process more sensitive personal data (for example, personal data with unique identifiers for a purpose other than that intended at collection or information on criminal behaviour).

37 Constitution of the Republic of South Africa (1996), available at: www.dataguidance.com/sites/default/files/saconstitution-web-eng.pdf

38 Electronic Communications and Transactions Act (2002), available at: www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf

39 Consumer Protection Act (2008), available at: www.gov.za/sites/default/files/gcis_document/201409/321864670.pdf

40 Cybercrimes Act (2020), available at: www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

- Promotion of Access to Information (2000)[41] provides individuals with the right to access information held by both public and private organisations.

The POPIA broadly aligns with the GDPR, in particular in terms of the legal grounds for processing. However, there are some notable differences, including (Lucarini n.d.):

- the data subject's rights do not include the right to data portability;
- that the POPIA does not require a Data Protection Impact Assessment; and
- the POPIA does not include standard contractual clauses or codes of conduct as part of the safeguard mechanisms to allow for cross-border transfer of data.

3.3 The situation in the CSME

3.3.1 Regional initiatives

Data protection and usage provisions in the CARIFORUM–EU and –UK economic partnership agreements (EPAs)

The CARIFORUM–EU (2008)[42] and the CARIFORUM–UK (2019)[43] EPAs both include provisions related to data protection and privacy. EPAs are a type of free trade agreement for relationships with developing countries.[44]

Fourteen (14) Caribbean Forum (CARIFORUM) countries have signed and agreed to implement both EPAs:

- Dominican Republic
- Caribbean Community countries:
  - Antigua and Barbuda
  - The Bahamas
  - Barbados
  - Belize
  - Dominica
  - Grenada
  - Guyana
  - Jamaica
  - Saint Lucia
  - St Vincent and the Grenadines
  - St Kitts and Nevis
  - Suriname
  - Trinidad and Tobago

Both agreements follow a similar structure and content regarding data protection provisions and include a chapter (Articles 197–201) dedicated exclusively to provisions regarding the protection of personal data. Under both agreements, the parties both commit to implementing appropriate legal and regulatory regimes and having the administrative capacity to implement them, including independent supervisory authorities, to protect the processing of personal data that is adequate and in line with existing high international standards. Such standards are those included in the following international instruments:

- Guidelines for the regulation of computerised personal data files adopted by the UN General Assembly (Office of the UN High Commissioner for Human Rights 1990) (amended in 1990): These include principles and minimum guarantees that should be provided in national legislations concerning computerised personal data files – for example, the principle of lawfulness and fairness, the principle of security, and trans-border data flow – whenever exchanging countries offer comparable safeguards for the protection of privacy.
- OECD recommendations on the guidelines governing the protection of privacy and trans-border flows of personal data (adopted 1980)

41 Promotion of Access to Information (2000), available at: www.dataguidance.com/sites/default/files/2000-002.pdf

42 Council Decision 2008/805/EC (2008), available at: http://publications.europa.eu/resource/cellar/f5c1c99f-9d19-452b-b0b0-ed690a53dd5f.0006.05/DOC_1

43 Economic Partnership Agreement, Miscellaneous Series No. 18 (2019), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803413/1._CARIFORUM_Command_Paper_Part_One.pdf

44 There is also the EU–LAC Digital Alliance in which some CARICOM members (The Bahamas, Barbados, Jamaica, Suriname, and Trinidad and Tobago) participate alongside other Latin American and Caribbean countries, which includes commitments to: ' an updated legal and regulatory framework that guarantees legal certainty, trust and the protection of the rights of individuals in the digital environment, based on internationally-agreed principles and collaboration with all stakeholders', among other goals (see ECLAC 2022). Articles 197-201

(OECD 2002): These include similar provisions regarding the principles and individual rights concerning data collection and processing (consent, right to access, challenge, purpose and use limitation, etc.) and recommendations to promote cross-border data transfers, including that member countries should endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to trans-border flows of personal data.

The agreements highlight the importance of maintaining effective data protection regimes to not only ensure the rights and interests of consumers are protected, but also to promote trade – that is, to facilitate trans-border flows of personal data and stimulate investor confidence.

Moreover, they specify that the timeline with which parties endeavour to implement the appropriate legal and regulatory regimes should start as soon as possible and no later than seven years after their respective entry into force.

They set out principles to ensure that personal data is collected and processed in a way that is transparent, fair and provides an adequate level of protection for individuals. These include:

- The purpose limitation principle: That data should be processed for a specific purpose.
- The data quality and proportionality principle: Meaning that data should be accurate and, where necessary, kept up to date, as well as being adequate, relevant and not excessive in relation to the purposes for which they are processed.
- The transparency principle: This means individuals should be provided with information on the purpose of collecting and/or processing their data, as well as the identity of the data controller in the third country (where relevant) and other relevant information in so far as is necessary to ensure fairness.
- The security principle: Data controllers need to implement measures ensuring the protection of personal data that are appropriate to the risks presented by the processing, the rights of access, rectification and opposition.
- Restrictions on onward transfers: Further transfers of personal data by the recipient of the original data transfer should be permitted only where the recipient of the onward transfer is also subject to rules providing an adequate level of data protection.
- Sensitive data: where special categories of data are involved (for example, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership), data may not be processed unless domestic law provides additional safeguards.

The agreements specify that enforcement mechanisms should be implemented to ensure a good level of compliance with data protection rules and a high degree of awareness among data controllers of their obligations and data subjects of their rights. Individual data subjects should also be able to enforce their rights rapidly and effectively, and without prohibitive costs. There should be effective and dissuasive sanctions, systems of direct verification of compliance, as well as independent investigations of complaints and appropriate redress mechanisms for injured parties.

They also require the parties to co-operate in matters related to data protection and privacy (for example, assistance in drafting legislation or guidelines, provision of training for key personnel) and to share information, expertise and best practices, with the view to stimulate investor and public confidence.

Outside of the chapter on data protection, in sections specific to certain sectors (for example, financial services, e-commerce, telecommunications), the agreements specify that the sectors in both parties need to ensure the protection of personal data, in particular when transferring personal data.

The HIPCAR project proposed model law

A proposed text for a model law and model policy guidelines to address a regional approach to data protection were developed by the HIPCAR project in 2012. The HIPCAR project was aimed at supporting Caribbean countries to improve their competitiveness by harmonising their approaches to ICT development. It was implemented by the International Telecommunication Union (ITU) in collaboration with the Caribbean Telecommunications Union (CTU), and with the involvement of other organisations in the

Caribbean region, including CARICOM (ITU 2022). The HIPCAR project proposed that the model law and policy guidelines in question – contained in the HIPCAR report on privacy and data protection – provide a framework for countries to consider when developing or adapting national data protection legislation that is consistent with regional and international standards.

The HIPCAR project proposed model law sets out the key principles and requirements for the processing of personal data in the CARICOM region, including:

- Data subjects' rights: Individuals have the right to access their data, request corrections to inaccurate data, and object to the processing of their data for certain purposes.
- Lawful processing: Data may only be processed if there is a legitimate reason for doing so, and the data subject has given their consent where necessary.
- Security measures: Data controllers are required to implement appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure or destruction.
- Cross-border data transfers: Transfers of personal data to countries outside of the CARICOM region are restricted unless the destination country provides an adequate level of data protection or the data subject has given their consent.

The HIPCAR project proposed model law also provides for the establishment of a Data Protection Commission to oversee and enforce the law, with powers to investigate complaints, issue fines, and order the suspension or cessation of data processing activities.

The model law is not yet a binding legal instrument. Rather, it is intended to serve as a template for CARICOM member countries to develop their own data protection laws based on the common principles and requirements outlined in the proposed model law. Some of the countries have already begun the process of developing their own data protection laws based on the model law.

The HIPCAR project proposed model law draws heavily from the EU's legislation, as well as other international data protection frameworks. It seeks to align with international best practices and standards for data protection, while also considering the unique needs and characteristics of the Caribbean region. Like the GDPR, the HIPCAR project proposed model law emphasises the rights of data subjects, establishes principles for the lawful processing of personal data, requires organisations to implement appropriate security measures to protect personal data, and provides for enforcement and sanctions.

However, there are also some differences between the model law and the GDPR, reflecting the particularities of the CARICOM region and its legal traditions. For example, the model law includes provisions on the processing of data for research purposes and public interest that are more specific and detailed than in the GDPR. The model law also allows for greater flexibility in the application of some of its provisions, to take into account the different legal systems and institutional capacities of the CARICOM countries.

Overall, the model law should be more prescriptive regarding rules pertaining to cross-border data transfer and consent standards to avoid heterogeneity in corresponding legal provisions across CARICOM countries. Such heterogeneity could significantly impact digital trade in the region. As a general rule, harmonisation in data protection standards and requirements is most important where they impact cross-border data transfers.

3.3.2 Data privacy and protection laws in individual CSME member countries

Eight CSME member countries have drafted and enacted data protection and privacy laws. These are (Morgan 2022):

- Antigua and Barbuda (2013)
- Barbados (2019)
- Belize (2021)
- Jamaica (2020)
- Saint Lucia (2011)
- St Kitts and Nevis (2018)
- St Vincent and the Grenadines (2003)[45]
- Trinidad and Tobago (2011)[46]

45 Although the Privacy Act 2003 seems to have never been brought into force and its scope is limited to public authorities.

46 Trinidad and Tobago's privacy laws have only been partially brought into force.

Some of the laws drafted after or around the time at which the GDPR was being drafted provide for modern data protection principles and elements relevant to digital market regulation, including consent to processing, direct marketing and rights around automated decision-taking using personal data and/or data portability (for example, Barbados [2019], Jamaica [2020]).

However, 4 of the 13 CSME member countries are still missing relevant data protection laws.[47] Suriname has draft legislation pending enactment, while Guyana had a draft protection bill under public consultation at the time of writing. Guyana's draft bill shares significant similarities with the GDPR and will be discussed in more detail in Section 3.3.3.

ECLAC review of alignment of selected Caribbean data protection laws with the GDPR

A 2020 review of some of the CARICOM data protection laws in terms of their alignment with the GDPR undertaken by the Economic Commission for Latin America and the Caribbean (ECLAC) shows that alignment is partial in most cases (Bleeker 2020).

For each area of the GDPR, the review developed a set of indicators to assess the alignment of each data protection legislation with the GDPR. These indicators were articulated as questions: for example, one of the questions assessing material scope and definitions is 'Does it provide a definition of personal data that is technologically neutral, i.e. does it apply to both automated and non-automated processing (filing systems)?'. Based on these questions, for each area of the GDPR or data sharing best practice, a law was deemed to be:

- fully aligned when a response indicating compliance could be given for the entire set of questions under consideration;
- substantially aligned when a response indicating compliance could be given for all but one or two questions under consideration;
- partially aligned when at least one response indicating compliance was possible for the questions under consideration; or
- not aligned when a response indicating compliance could not be given for any of the questions under consideration (see Table 3.1).

Moreover, the study provides further guidance as to the alignment ratings, specifying that substantial alignment with an area of the GDPR would be in most cases sufficient to achieve essential equivalency or a comparable level of protection to the GDPR.

For some of the jurisdictions with existing data protection laws, those seem outdated in an increasingly digitalised economy. For example, they do not include digital footprints that can lead to data subject identification, such as location data produced by mobile phones, IP addresses, cookie ID and advertising identifiers, within the personal data definition scope of the legislation (for example, Trinidad and Tobago [2011]) Further to that, they seem to exhibit gaps concerning some elements of the GDPR relevant to digital market regulation, such as the right to data portability and/or rules enabling international transfers of personal data. This is discussed in the next section.

3.3.3 Alignment with GDPR elements pertaining to digital markets regulation

This section assesses the state of data protection and privacy legislation and regulation in CARICOM countries in terms of key areas of alignment and gaps with elements of the GDPR pertaining to market regulation, i.e. data subjects' data portability and access rights, safeguards and adequacy assessment regarding international transfers, and data processing rules of consent and grounds of legitimate interest.

Table 3.2 summarises the results of the assessment:

- green indicates that related provisions are included and align with the GDPR;
- amber indicates that related provisions are included but do not align with the GDPR; and
- red indicates that related provisions are not included.

More details per individual available legislation are provided further below. The Guyana draft Data Protection Bill, as an interesting example of legislation that very closely aligns with the GDPR, is discussed first and in more detail relative to all other legislations.

47 Dominica, Grenada, Guyana, Suriname.

Table 3.1 Alignment of selected Caribbean data protection laws with the GDPR

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

Source: Economic Commission for Latin America and the Caribbean (ECLAC) (2020)

Table 3.2 Alignment with key elements of the GDPR pertaining to digital market regulation

Caricom/ CSME member countries	Data processing: consent and grounds of legitimate interest	Right of access	Right to data portability	Conditions and safeguard mechanisms allowing for international data transfers
Antigua and Barbuda	Aligned	Aligned	Not included	Not included
The Bahamas	Included but not fully aligned	Included but not fully aligned	Not included	Included but not fully aligned
Barbados	Aligned	Aligned	Aligned	Aligned
Belize	Aligned	Aligned	Aligned	Aligned
Guyana	Aligned	Aligned	Aligned	Aligned
Jamaica	Aligned	Aligned	Included but not fully aligned	Aligned
Saint Lucia	Aligned	Included but not fully aligned	Not included	Included but not fully aligned
St Kitts and Nevis	Aligned	Included but not fully aligned	Not included	Not included
St Vincent and the Grenadines[49]	Not included	Not included	Not included	Not included
Suriname[48]	Included – alignment not verified	Included – alignment not verified	Included – alignment not verified	Included – alignment not verified
Trinidad and Tobago	Included but not fully aligned	Included but not fully aligned	Not included	Not included

Source: Authors' analysis.

48 The draft Bill in Suriname was not readily available in English and the assessment of the alignment with the GDPR could not be undertaken as a result.
49 The scope of the draft Act seems limited to data held by public authorities.

There are large differences across the relevant (draft) legislations available in the CSME member countries, in terms of their inclusion of key elements of data protection regulation pertaining to digital market regulation. The (draft) legislations in Barbados, Belize and Guyana include all elements and closely align with the GDPR in that regard. Most legislations in other countries (Jamaica, Antigua and Barbuda, Trinidad and Tobago, St Kitts and Nevis, Saint Lucia, and The Bahamas) include elements on consent and grounds of legitimate interest for data processing, as well as the right of access. However, they are often missing the right to data portability, as well as conditions and safeguard mechanisms for international data transfers – although to a lesser extent.

Lack of harmonisation across the various CSME member countries could create some difficulties for cross-border data flows, trade and regional integration of digital markets. It also makes it more costly for businesses handling consumer data across various jurisdictions to be compliant with the different legislations. Regional harmonisation or convergence of national-level privacy regimes is a priority concern in other regional groups such as ASEAN and the Asia–Pacific Economic Cooperation (APEC). ASEAN's approach to achieving regional cohesion around data protection and privacy standards through the development of frameworks, practical guides and fora is discussed in Section 4.3.

Antigua and Barbuda: Data Protection Act, 2013[50]

- Conditions of consent and grounds of legitimate consent to data collection and processing are provided by the Antigua and Barbuda Act, and broadly align with those in the GDPR.
- Right of access to personal data is provided and broadly aligns with that provided in the GDPR.
- Right to data portability is not included.
- Provisions on conditions to allow for international data transfers are not included.

The Bahamas: Data Protection (Privacy of Personal Information) Act, 2003[51]

- Conditions of consent to data collection and processing are not included explicitly in The Bahamas Act. Rather, data collection has to be lawful, fair and not misleading/deceiving to the data subject with regard to the purposes for which data is being collected and used. Grounds of legitimate interest in data collection and processing are broadly provided by the Act.
- Right of access to personal data is provided, although a fee may apply.
- Right to data portability is not included.
- Provisions on conditions to allow for international data transfers are included, but present differences from those in the GDPR. Data could (but not necessarily would) be prohibited to be transferred outside of The Bahamas by the Data Commissioner, if there is a failure to provide protection either by contract or if the receiving country does not provide protection equivalent to that provided under the Act. However, consent (express or implied) by the data subject seems to be sufficient to allow for the data transfer (that is, prior provisions do not apply).

Barbados: Data Protection Act, 2019[52]

- Conditions of consent and grounds of legitimate interest to data collection and processing are provided by the Barbados Act and align closely to those provided in the GDPR.
- Right of access to personal data is provided and related provisions align closely to those in the GDPR.
- Right to data portability is included and related provisions align closely to those in the GDPR.
- Provisions on conditions and mechanisms to allow for international data transfers are included and closely align with those in the GDPR (i.e. adequacy, BCRs, SCCs).

50 Data Protection Act (2013), available at: http://laws.gov.ag/wp-content/uploads/2019/02/a2013-10.pdf

51 Data Protection (Privacy of Personal Information) Act (2003), available at: https://www.lexbahamas.com/Data%20Protection%202003.pdf

52 Data Protection Act (2019), available at: https://gisbarbados.gov.bb/download/data-protection-act-2019/

Belize: Data Protection Act, 2021[53]

- Conditions of consent and grounds of legitimate interest to data collection and processing are provided by the Belize Act and align closely to those provided in the GDPR.
- Right of access to personal data is provided and related provisions align closely to those in the GDPR.
- Right to data portability is included and related provisions align closely to those in the GDPR.
- Provisions on conditions and mechanisms to allow for international data transfers are included and closely align with those in the GDPR (i.e. adequacy, BCRs, SCCs).

Guyana: Draft Data Protection Bill, 2023[54]

The draft Data Protection Bill was published for consultation in April 2023. It shares significant similarities with the GDPR (Morgan 2023):

- Personal data is defined – as in the GDPR – as 'any information relating to an identified or identifiable natural person'. The Bill also includes pseudonymisation and encryption of personal data by organisations ('data controllers') as potential measures to comply with data protection and processing security requirements (55(4)(c), 64(1)(a)).
- Data processing principles (Part II) are fully aligned with those provided in Art. 5 of the GDPR. These provide that personal data must be:
  - processed lawfully, fairly and transparently;
  - collected for specified, explicit and legitimate purposes only;
  - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  - accurate and, where necessary, kept up to date;
  - kept in a form which permits identification of data subjects for no longer than is necessary; and
  - processed in a manner that ensures appropriate security of the personal data.
- Individual data rights (Part III) are almost fully aligned with those provided in Chapter 3 of the GDPR. These include the right of access, the right to rectification, the right to restriction of processing, the right to data portability, the right to object, rights regarding automated individual decision-making, including profiling, etc. The Guyana legislation also includes the 'right to prevent processing likely to cause damage or distress', which provides the right of the data subject to require the data controller to not process (or cease processing) its personal data for a specific purpose or in a specific manner that would cause the data subject or another individual 'substantial damage or distress'. While this is not specifically included in the EU GDPR, it is similar in wording and principle to the UK Data Protection Act 2018, which prohibits processing that is 'likely to cause substantial damage or substantial distress to a data subject'.[55]
- The legislation applies to personal data processing by public and private organisations.
- The principles and mechanisms that govern international data transfers (Part IV) somewhat align with those provided in Chapter 5 of GDPR, but there is one notable difference. The Bill seems to suggest that personal data cannot be transferred to a state or territory outside of Guyana unless both:
  - the state or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data; and
  - appropriate safeguards on condition that the rights of the data subject are enforceable and effective legal remedies are available for data subjects.
- Similar to the GDPR, the adequacy decision is made by the Data Protection Commissioner, which is the regulatory body appointed to

53 Data Protection Act (2021), available at: www.nationalassembly.gov.bz/wp-content/uploads/2021/12/Act-No-45-of-2021-Data-Protection-Act.pdf

54 Guyana Data Protection Bill (2023), available at: www.mola.gov.gy/sites/default/files/DATA%20PROTECTION%20BILL%202023.pdf

55 Data Protection Act (2018), available at: www.legislation.gov.uk/ukpga/2018/12/section/41?view=plain

administer the data protection legislation. The Bill also provides for similar safeguard mechanisms as the GDPR, including binding corporate rules and standard contractual clauses. It also provides for similar derogations to the international transfer adequacy decision and safeguard requirements, including the consent of the data subject to the data transfer and the necessity of the data transfer for the performance of a contract between the data subject and controller.

- The Commissioner may also provide 'technical standards for data protection certification mechanisms and data protection seals and marks', which could help businesses assess with more certainty their compliance with data protection regulations (95). Again, this is in line with the GDPR provision under Art. 42.
- Non-compliance with the regulation can lead to heavy fines, which broadly align with those provided in the GDPR (for example, up to 4 per cent of annual revenue when the offender is a company). The Bill also includes a specific provision for the personal liability of the leadership (or other employee with relevant capacity) of an offending company, if the offence is found to have been committed with the consent or knowledge of the leadership or to be attributable to any neglect from the leadership (100(3)). The GDPR does not include a provision that clearly indicates the extent to which the leadership or employees of the company are also personally liable following a breach of the regulation. However, recent case law, as well as general liability rules of corporate law, suggest that company leadership can also be personally liable for data protection breaches by a company in the EU.[56]

Jamaica: Data Protection Act, 2020[57]

- Conditions of consent and grounds of legitimate interest to data collection and processing are provided by Jamaica's Act and closely align to those provided in the GDPR.
- Right of access to personal data is provided and related provisions align closely to those in the GDPR.
- Right to data portability is not included.
- Provisions on conditions and mechanisms to allow for international data transfers are included and closely align with those in the GDPR (i.e. adequacy, BCRs, SCCs).

Saint Lucia: Data Protection (Amendment)[58] Act, 2011 (2015)[59]

- Conditions of consent and grounds of legitimate interest to data collection and processing are provided and broadly align with the GDPR in Saint Lucia's Data Protection Act.
- Right of access to personal data is provided. However, similar to the Bill in St Kitts and Nevis, there is a prescribed fee applicable to individuals for obtaining a copy of their personal data.
- Right to data portability is not included.
- Provisions on conditions to allow for international data transfers are included. Data can be transferred to countries with comparable safeguards in data protection and with authorisation from the Data Protection Commissioner.

St Kitts and Nevis: Data Protection Bill, 2018[60]

- Conditions of consent and grounds of legitimate interest to data collection and processing are provided by the St Kitts and Nevis Data Protection Bill and broadly align with GDPR.
- Right of access to personal data is provided. Under the 'Access Principle' (see Part II, 13 and Part III, 14), the Bill provides for right of access to personal data that somewhat aligns with GDPR provisions – however, unlike the GDPR,

56 For example, Dresden Higher Regional Court (OLG) ruled that managing directors are their own data protection controllers within the meaning of the GDPR and are therefore also personally liable (ruling of the OLG Dresden of 30.11.2021 [file number 4 U 1158/21]) (see Braken 2022).

57 Data Protection Act (2020), available at: https://japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202020.pdf

58 Data Protection Act (2011), available at: www.dataguidance.com/sites/default/files/act_11_of_2011.pdf

59 Data Protection (Amendment) Act (2015), available at: https://www.dataguidance.com/sites/default/files/act_2_of_2015.pdf

60 Data Protection Act (2018), available at: www.dataguidance.com/sites/default/files/data_protection_act_5_of_2018.pdf

access to personal data may require a fee (Part III, 14). The fee could create an additional barrier to individuals being able to exercise their rights of access.

- Right to data portability is not included.
- Specific provisions regarding international data transfers are not included. Transfers, in general, are included as processing activities and covered as such in the Bill.

St Vincent and the Grenadines

There is a draft online of a 2003 Privacy Act, with scope limited to public authorities,[61] but to our knowledge this never came into force.[62]

Individual organisations on the island have set up their own data protection policies (for example, St Vincent and the Grenadines (SVG) Maritime Association,[63] SVG Environment Fund[64]).

Suriname: Bill for the Privacy Protection Act and Personal Data, 2018[65]

The English translation for this Bill is not readily available online. A search of key translated words and expressions seems to suggest the following:

- Conditions of consent and grounds of legitimate interest to data collection and processing are included.
- Right of access to personal data is included.
- Right to data portability is included.
- Provisions on conditions and mechanisms to allow for international data transfers are included (i.e. adequacy, BCRs, SCCs).

61 Privacy Act (2003), available at: www.theinformationcollective.com/dpl/st-vincent-and-the-grenadines-the-privacy-act

62 St Vincent and the Grenadines Government, Acts 2003, available at: http://assembly.gov.vc/assembly/images/Acts/2003.pdf

63 St Vincent and the Grenadines Maritime Administration, Data Protection Policy, available at: http://www.svg-marad.com/data-protection-policy.asp

64 St Vincent and the Grenadines Environment Fund (2022), Privacy Notice, August, available at: www.svgef.org/privacy-policy/

65 Bill for the Privacy Protection Act and Personal Data (2018), available at: www.dna.sr/media/307641/Wet_Bescherming_Privacy_en_Persoonsgegevens.pdf

Trinidad and Tobago: Data Protection Act, 2011[66]

- Conditions of consent and grounds of legitimate interest to data collection and processing are broadly provided by Trinidad and Tobago's Data Protection Act (DPA), although some provisions regarding conditions of consent are less elaborate than those provided in the GDPR (for example, it does not include withdrawal of consent, demonstration of consent).
- Right of access is limited. The DPA provision that provides individuals with the right to access data is limited to the purposes of challenging the accuracy and completeness of the information (Art. 6.j). Unlike the GDPR, it does not cover the right to access data and information pertaining to the data processing (for example, categories of personal data being processed, recipients, etc.). A comprehensive right to access (as provided in the GDPR) has significant implications for the way businesses in digital markets operate and engage with consumers, in particular, those where individual-level data processing is a key component of their business models (see more in Section 3.2.1).
- Right to data portability is not included. The DPA does not address data portability, which makes sense given that its scope does not specifically include a modern and comprehensive definition of digital data. Data portability is one of the key pro-competitive measures in digital markets, empowering consumers to choose among competing providers by reducing user switching costs and frictions associated with trying new services. However, evidence of its usefulness and effectiveness from a practical perspective is limited (see more in Section 3.2.1).
- Detailed provisions on safeguard mechanisms to allow for international data transfers are not included. The DPA provides that personal information may be transferred outside of Trinidad and Tobago only if the laws in the recipient country provide safeguards for the personal information equivalent to those provided by Trinidad and Tobago law (Art. 6.l). This broadly

66 Act No. 13 of 2011, available at: www.ilo.org/dyn/natlex/docs/ELECTRONIC/88403/101074/F1410860608/TTO88403.pdf

aligns with the GDPR adequacy status approach. However, it does not include detailed provisions on the different safeguard approaches and mechanisms (for example, standard contractual clauses [SCCs], binding corporate rules [BCRs]).

3.4 Gaps and recommendations

This section provides a discussion on the gaps in data protection regulation in CSME countries and policy recommendations to address these gaps.

Challenges associated with full GDPR alignment

CSME countries currently exhibit gaps in data protection regulation relative to the GDPR, which is widely considered best practice in data protection regulation. The GDPR provides a robust and by now embedded framework that prioritises perceived citizen concerns.

However, fully replicating the GDPR in the CSME could be overly complex and costly to both companies and regulatory authorities responsible for enforcing the regulation. Moreover, small jurisdictions like the CSME countries might face risks concerning mutual recognition, whereby adopting a data protection framework modelled after the GDPR might still be insufficient to be recognised and accepted as providing adequate protection by other nations or regional blocs. This lack of mutual recognition could limit the effectiveness of such an approach, particularly in the context of cross-border data flows. Small jurisdictions could also face enforcement challenges because of limited resources. Implementing and enforcing data protection rules requires significant resources, including financial penalties for non-compliance. Smaller countries may struggle to establish and maintain adequate enforcement mechanisms, which could compromise the integrity of their data protection framework.

Bottom-up approach to data protection

Rather than attempting to mirror the GDPR, small countries could explore alternative strategies to enhance their data protection capabilities. These might include:

- building upon existing international norms and standards, such as the Council of Europe's Convention 108 or the Asia–Pacific Economic Cooperation (APEC) Privacy Framework;
- collaborating with other countries, organisations or experts to develop tailored solutions that address unique challenges and circumstances in the CSME; and/or
- leveraging technology and innovation to facilitate compliance, such as using machine learning algorithms to identify and mitigate privacy risks.

CSME member countries could also try to follow a bottom-up approach to data protection regulation that takes local contextual nuances into account. Data protection and privacy requirements vary depending on the specific context and application. For instance, the GDPR focuses on personal data processing within the EU, whereas other regions may have distinct legislation and approaches. Attempting to replicate the GDPR verbatim may not fully address local needs, leading to potential gaps or conflicts.

Regional harmonisation regarding elements of data protection relevant to cross-border data flows

There is significant heterogeneity across the CSME in terms of availability and approach to data protection regulation. Regional heterogeneity, in particular with regard to elements relevant to cross-border data flows, could be problematic. It could reduce cross-border data flows as data protection rules in one country could prohibit data transfers to another in the CSME. This would end up negatively impacting trade and innovation in the regional digital economy.

The CCC could play an important role in advocating for regional harmonisation across the CSME regarding data protection regulation where it has direct competition implications. It could provide guidance in the development of an aligned approach to data protection regulation – in particular with respect to measures to increase contestability of data markets, such as data access and portability.

4. Digital Trade Issues

Key findings

- Data localisation rules aside, all jurisdictions in principle allow cross-border data transfers to take place.
- The EU's GDPR framework represents the most articulated international framework and is likely to be the most relevant for businesses in the CSME. Other relevant international frameworks are the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Additional Protocol to the Council of Europe Convention 108.
- Seeking EC adequacy would require significant effort with uncertain benefits for CSME citizens. Binding corporate rules (BCRs) and standard contractual clauses (SCCs) are options for data transfers, but SCCs can be costly and inflexible. Derogations like explicit consent and contractual necessity are alternatives, which are more suitable for certain industries and types of relationships.
- The CSME can strengthen its international position as a participant in international data markets by harmonising data protection law and practice internally, while advocating for a trade-friendly data protection system globally.

4.1 Background

Rules on international data transfer are the key points of interaction between the large regulatory 'blocs' like the European Union and the US and other countries. The EU's framework (which so far also applies in the UK) represents the most articulated international framework to date.

Sharing data across borders is essential across virtually all segments of developed and developing economies. Data on customers, suppliers and employees are increasingly outsourced to overseas third-party providers (through cloud services) and global value chains are increasingly digitised and spread across the globe. Many countries, including the Caribbean, try to compete to become regional or global hubs in business process outsourcing (BPO), data centres, cloud computing, artificial intelligence or big data analytics.

Data localisation rules aside, all jurisdictions in principle allow cross-border data transfers to take place. However, they do so under conditions that differ between jurisdictions.

Making international data transfers compatible with different data protection frameworks is a global challenge, especially for countries that are 'rule-takers' of the big regulatory blocs. The Asian Business Law Institute (ABLI 2018) summarises the history as follows:

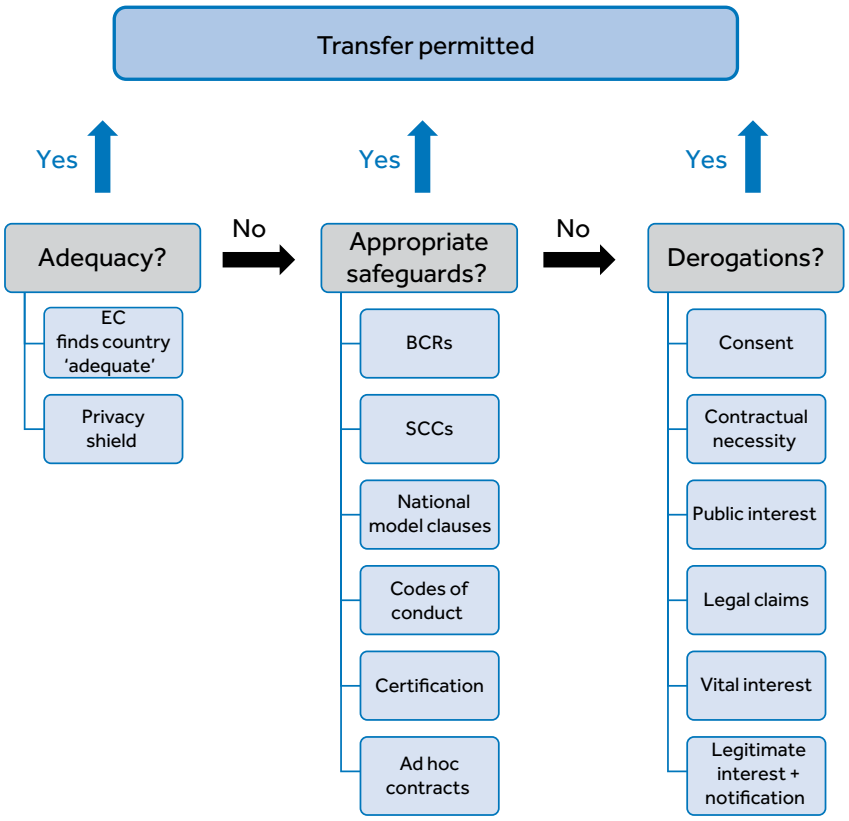
> *Since their early adoption in 1980, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data have articulated this balancing act around a principle of free flow of data and the admission that restrictions may be legitimate, where the country of destination 'does not yet substantially observe' the Guidelines or 'where the re-export of such data would circumvent its domestic privacy legislation'.*

The Guidelines, revised in 2013, have set common standards for OECD member countries to shape their laws and regulations on cross-border data flows, while also insisting on the crucial need to address the global dimension of privacy through improved 'interoperability' of privacy regulations.

The Additional Protocol to the Council of Europe Convention 108 is the only internationally binding data protection instrument to date. The Protocol stipulates that data may only be transferred if the recipient state is able to ensure an 'adequate level of protection', or if 'adequate safeguards, in particular resulting from contractual clauses, are provided by the data exporter in accordance with domestic law'.

With the proliferation of data protection laws worldwide, frictions resulting from adequacy assessments have started to emerge, even in cases where legislation is seemingly aligned. For example, in 2018 the ASEAN Economic Community adopted its Framework for Data Protection to

Figure 4.1 When can personal data be transferred?



Source: Adapted from Alston and Bird (2016).

promote co-operation between members in the implementation of the same Principles of Personal Data Protection in their domestic laws and regulations. However, ABLI (2018) observes:

> *this transposition has not achieved the desired objective of regional consistency. In reality, while frameworks such as the APEC and ASEAN data privacy frameworks have provided 'rough signposts for a common approach to principles-based regulation', 'moving from a plain reading of the text of the newly enacted data protection laws (which in many respects appear similar across the region) to the practicalities of enforcement and compliance, we see increasing divergence as jurisdictions prescribe more and more detailed requirements, often with local nuance.*

4.2 The EU framework for international transfers of personal data

Given the de facto importance of the EU's GDPR as the default framework, this section describes the GDPR framework to international data transfers in more detail.

Under EU law, data may not be transferred outside of the European Economic Area (EEA) unless the member state finds that data is adequately protected. Several legal mechanisms have been developed to allow for data to be transferred internationally, while still maintaining the high level of data protection accorded within EU law. This section highlights these mechanisms. A schematic view of the options that are open to companies wishing to transfer personal data out of Europe is presented in Figure 4.1. Given that no adequacy decision has been made in respect of any of the CSME member countries, the options for data transfers between the EU and the CSME countries have to use either safeguards or derogations.

4.2.1 Adequacy status

The EU's preferred method of enabling international data transfers is through the adequacy framework (sometimes called the 'whitelist'). Article 45(2) of the GDPR empowers the European Commission to decide that a third country provides adequate data protection, and therefore data may be transferred to that country without additional safeguards. At the time of this report, the EC had

recognised that the following countries provide adequate data protection: Andorra, Argentina, Canada,[67] Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom[68] and Uruguay.[69] To our knowledge, none of the CSME countries are currently in the process of obtaining an adequacy decision.

The economically important relationship between the EU and the US is currently covered under the adequacy framework, but has unique characteristics that make it unlikely as a model for other countries. The EC published its new adequacy decision for the EU–US Data Privacy Framework on 10 July 2023. The EU-US Data Privacy Framework replaces the Privacy Shield scheme, which had been invalidated by the EU Court of Justice. The new framework 'introduces new binding safeguards to address all the concerns raised by the European Court of Justice (CJEU), including limiting access to EU data by US intelligence services to what is necessary and proportionate, and establishing a Data Protection Review Court (DPRC)'. (EC 2023)

The EC assesses adequacy based on a broad range of factors, including the relevant data protection legislation, judicial and administrative processes, supervisory authorities etc. The EC's adequacy assessment process 'is complex and prolonged'.[70]This protracted process is evidenced by the small number of countries with adequacy status.[71] Chander and Schwartz (2023) note that the EC has found significantly less than 10 per cent of the world's data protection laws to be adequate and that 'this low number is especially notable in light of the fact that most of the world's data privacy laws follow the European model'.

Current practice by the EC is best exemplified by the EU–Japan adequacy negotiations, which were successfully concluded in January 2019, despite Japan's data protection framework having been described as lax and insufficient only five years earlier (Schwartz 2019).

To achieve this result, Japan undertook a comprehensive process of reform starting with extensive amendments to Japan's Act on the Protection of Personal Information (APPI) in 2015, which contained an expanded definition of sensitive data, greater individual rights, stronger limits on the use of personal data provided to third parties, protection for international transfers of personal data and enhanced enforcement powers for the Japanese data protection authority, the Personal Information Protection Commission (PPC), moving it significantly closer to the GDPR (Ibid). There were further changes following deep engagement between the EC and Japan, including a set of legally binding 'supplementary rules' and commitments by the Government of Japan (Ibid).

The broader background of the change in Japan from weak to EU-strengthened data protection is a strategic move that has complemented Japan's growing economic partnership with the EU. This contrasts with a much more fraught situation with the United States, where consecutive adequacy solutions (Safe Harbor and Privacy Shield) were overturned by the CJEU, despite the more flexible approach the EC adopted towards the US on account of it being the EU's largest trading partner.

The evidence from recent adequacy decisions taken by the EC (Japan and South Korea) suggests that the EC is treating the adequacy assessment process as part of a wider policy strategy to achieve future-proof economic partnerships with third countries.

4.2.2 Appropriate safeguards

If data needs to be transferred to countries without adequacy status, other appropriate safeguards are needed. The two main safeguards under the GDPR are binding corporate rules (BCRs) and standard contractual clauses (SCCs).

Binding corporate rules

BCRs are one of the transfer mechanisms in the EU GDPR (Art. 47), mirrored in the UK GDPR, that is open to any entity in a country not on the whitelist of adequate nations, regardless of the domestic, non-EU law that formally regulates a foreign entity.

67 Commercial organisations only.

68 The United Kingdom was the last country to receive an adequacy decision (in 2021). The UK continues to rely on the EC adequacy decisions for international data transfers under the 'UK GDPR' (the EU GDPR as transcribed into UK law). While the list of adequate partner countries may diverge in the future, this is unlikely given that this would bring the UK regime into conflict with the adequacy framework of the EU, its biggest trading partner.

69 The US–EU Privacy Shield – a voluntary programme for US companies – was also granted adequacy status, but this has since been invalidated (CJEU judgment of 16 July 2020 [Case C-311/18]).

70 Chander and Schwartz (2023). In the case of New Zealand, the process took 17 years, from 1995 to 2012.

71 Which include the UK as an ex-member of the EU, as well as the small dependencies: Jersey, Guernsey, the Isle of Man and the Faroe Islands.

BCRs establish uniform internal rules for transferring personal data across the corporate group and are binding on all relevant entities and personnel in the group.[72] They are essentially codes of conduct that ensure compliance with EU data protection law and adequate protection for data transferred across borders.

Originally, BCRs were only available to data controllers. Since January 2013, BCRs are also available to data processors (BNA 2015). Processor BCRs may be particularly useful for firms like outsourcing providers or cloud computing service providers which transfer large volumes of data but do not act as controllers.

BCRs need to be approved by the European data protection authorities.

Compared with SCCs, BCRs permit organisations to benefit from 'a more integrated, holistic approach' rather than one that must be determined for each transfer of information. In effect, 'BCRs make the entire organisation a kind of "safe haven" in which personal data can be transferred internally without concerns for national borders' (Kuner 2007).

The effectiveness and viability of BCRs is thus not primarily a question of the rules in place: 'the EU has long made clear that adequacy is to be judged by the actual practices of data processing entities' (Schwartz 2019). Consequently, BCRs require a comprehensive privacy programme and compliance infrastructure that includes governance mechanisms, data protection officers, policies and procedures, training and communication, audits and assessments, and in general follows the essential elements of accountability and corporate compliance programmes.

BCRs are currently exclusively used by very large multinational companies (UNCTAD 2016). They are considered only a viable option for data transfers for complex firms with significant transfers from the EU to third countries. The approval process is considered cumbersome and demanding, and the resources required are significant. However, they are also seen as the best model for flexibility in data protection and accountability (Hogan Lovells 2016).

While BCRs are currently only relevant for data transfers to and from the EU and the UK, they are recognised in other jurisdictions and could form a greater part of a future international data transfer landscape (provisions for BCRs exist in Australia, Hong Kong, Japan, New Zealand, Singapore, Thailand and India).

Standard contractual clauses

The second of the two safeguards are standard contractual clauses (SCCs), which establish approved rules for transmitting data that must be signed for each transfer by the sending entities in the EU and the receiving entities in the third country.[73] The EU SCCs were modernised in June 2021.

Initially, three sets of clauses were introduced: two for data controllers[74] and one for data processors.[75] SCCs may not be altered in any way, or they are no longer guaranteed to provide adequate protection. Amended clauses may still be used but can be challenged by the DPA.

SCCs were intended to be quickly implementable. If used verbatim, they would offer a guaranteed legal transfer of data without the need for further safeguards. Hence, no substantial drafting was necessary (Hogan Lovells 2016).

However, the *Schrems II* decision confirmed that while SCCs could be relied upon for personal data transfers to countries without an adequacy decision, an impact assessment of the laws of the third country to confirm whether the data would receive essentially equivalent protection to that provided in the EU would also be necessary (Pinsent Masons 2023). In the case where the assessment of the legal situation in the third country identifies deficiencies relative to the protection provided in the EU, supplementary measures that address these deficiencies and ensure an essentially equivalent level of data projection need to be put in place to allow for the transfer of personal data (for example, pseudonymisation, end-to-end encryption) (European Data Protection Board 2020). This is reflected in the new SCCs that were published by the EC in June 2021. These

72 European Commission, 'Binding Corporate Rules (BCR)', available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

73 The ASEAN Model Contract Clauses and the APEC Cross-Border Privacy Rules (CBPR) system offer analogous frameworks.

74 2001/497/EC and 2004/915/EC.

75 2010/87/EU.

new requirements around the SCCs would likely lead to the SCCs becoming more time and resource intensive.

From a practical perspective, the initial SCCs were found to not be ideal in many cases, as they offered no flexibility. The modernised SCCs are meant to offer more flexibility for complex processing chains, for example, by adopting a modular approach and allowing for more than two parties to be included and make use of the clauses (EC 2021b). They introduce two new sets of SCCs, one for use between controllers and processors and one for the transfer of personal data to third countries, and are meant to provide more legal predictability to EU businesses.

Competition assessment of the terms or provisions of SCCs

Standard contractual clauses (Ibid) establish approved rules for transmitting data that must be signed for each transfer by the sending entities in the EU and the receiving entities in the third country. Like BCRs, SCCs are open to CSME-based firms, but they are generally viewed as being relatively costly and inflexible measures. SCCs do not fit each type of data transfer, must be used without change, and are considered as imposing terms that 'are relatively onerous to meet and can lead to high administrative costs' (Casalini and López González 2019, quoted in Schwartz 2019).

As such, for firms in countries that are not on the 'adequacy' whitelist and are not part of international groups that have BCRs in place, SCCs are one of the few options available for implementing international data transfers involving EU individuals. However, they are not the only ones: explicit consent and contractual necessity are the key derogations (Art. 49 GDPR) that are relevant for commercial enterprises and are likely to be a viable alternative for businesses that enter into direct contractual relationships with EU individuals (B2C). The travel industry, for example, is likely to be able to rely on derogations in many cases. Derogations are less likely to be appropriate for firms selling goods or services without formal contracts and for firms receiving personal data in bulk (B2B).

In general, the availability of SCCs is pro-competitive, as they allow international firms without access to other mechanisms to engage in data transactions with the EU that would otherwise be unlawful. While it is conceivable that firms may use the international data transfer provisions of the GDPR in an anti-competitive way (for example, a firm that is part of an international group of companies could strategically establish a BCR in the group to raise local rivals' costs by forcing them to adopt SCCs to remain competitive), such scenarios are theoretical and depend on the cost differential between BCRs and SCCs, rather than on individual provisions in the EU SCCs.

4.2.3 Derogations

In the absence of adequacy or appropriate safeguards, Article 49(1) of the GDPR sets out six derogations under which data may be transferred internationally. Broadly speaking, data may be transferred if:

- the data subject has given unambiguous consent;
- the transfer is necessary to implement a contract between the data subject and controller;
- the transfer is necessary to implement a contract between the data controller and a third party on behalf of the data subject;
- the transfer is necessary or legally required on the grounds of public interest, or the exercise or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject; or
- the transfer is from a register intended to provide public information and which is open to accessible consultation.

Contractual necessity and consent are often appropriate, for example, in e-commerce and the travel industry.

Unambiguous consent is the most important derogation. However, obtaining unambiguous consent is often a practical challenge, and hence firms tend not to rely on it. Unambiguous consent may, for instance, be impractical for businesses with a large customer base as consent needs to be obtained from all customers. Furthermore, consent must be informed, which is difficult to prove, and data subjects must be able to revoke consent (Osborne Clarke, 04 February 2016).

Contractual necessity refers to cases where the legal basis for a business to undertake the transfer of its EU customers' personal data is the contract that it has with them. For example, with hotel bookings, the transfer of personal data such as name, and the financial and contact details of EU customers

between the hotel booking platform (for example, located in EU) and a local hotel would be necessary to fulfil the provision of the accommodation service.

Derogations are less likely to be appropriate for firms receiving personal data in bulk (B2B).

4.3 ASEAN's approach to regional cohesion around data protection

ASEAN[76] provides CSME with an example of a non-prescriptive regional approach to data protection that aims to promote trade and innovation in the regional digital economy.

The digital economy in Southeast Asia has been growing at a fast pace, with huge potential for further growth: it is the world's fastest growing internet region and its online spending is expected to reach US$200 billion by 2025 (Deloitte 2018). In this context, ASEAN has identified digital technology as key in its 2025 Vision 'ASEAN 2025: Forging Ahead Together' and has been proactive in promoting strong data protection standards in the region, with the view to support trade, the flow of information and innovation across member countries in the digital economy. ASEAN has a distinctive approach to regional co-operation and governance, which protects national sovereignty (that is, non-interference in the domestic matters of fellow countries) and is based on consensus building and informal guiding relationships between respective leaders (UNDP Global Centre for Technology, Innovation, and Sustainable Development 2021). Its approach to achieving regional cohesion around data protection and privacy standards takes the form of frameworks, blueprints, practical guides, declarations and fora. These initiatives are not legally binding and enforceable obligations at the regional level.

As such, the ASEAN Framework on Personal Data Protection, adopted in 2016, provides broad principles for the protection of personal data (for example, consent and purpose, access and correction) that the member countries can endeavour to take into account in their domestic laws and regulations (ASEAN 2016). Following up on that, the ASEAN Framework on Digital Data Governance, endorsed in 2018, similarly guides public and private entities and consumers on how to manage data flows, to strengthen the data ecosystem, and improve the legal and regulatory alignment of data regulations and governance frameworks across the member countries. A stronger data ecosystem and better alignment of policies across the region can promote the growth of trade and the flow of data within and among the ASEAN member countries in the digital economy (Ibid). The Framework set out four initiatives that can be undertaken to support its aims, namely the ASEAN Data Classification/Management Framework, the ASEAN Cross Border Data Flows Mechanism, the ASEAN Digital Innovation Forum, and the ASEAN Data Protection and Privacy Forum.

The ASEAN Data Management Framework provides a common data classification framework, which sets out categories of data, descriptions of what each category entails, as well as security requirements and recommended measures or protections for each category. This provides businesses with practical guidance to identify appropriate controls that they can implement cost-effectively to provide adequate protection of different types of data in the different stages of the data lifecycle (ASEAN 2021a). The ASEAN Cross Border Data Flows Mechanism aims to provide businesses with regulatory certainty on who they may share data with, the types of data that may be shared, and how they may share such data to facilitate data flows between participating ASEAN member countries. It currently mainly comprises the ASEAN model contract clauses (MCCs).

The MCCs are contractual terms and conditions that may be included in the binding legal agreements between parties transferring personal data to each other across borders (ASEAN 2021b). They ensure that the transfer of personal data is done in a manner that complies with the ASEAN member countries' legal and regulatory requirements and aligns with the principles of the ASEAN Framework on Personal Data Protection, as well as – to the extent possible and relevant to the ASEAN context – with global best practices of data protection.[77] At the time of

76 The Association of Southeast Asian Nations (ASEAN) is a political and economic union of ten member countries in Southeast Asia, which includes countries like Singapore, Malaysia, Thailand, Vietnam, Indonesia and the Philippines.

77 These include Fair Information Practice Principles (FIPPs), the 1980 OECD Privacy Guidelines, as well as more recent legal and policy frameworks, such as the APEC Privacy Framework and the EU's General Data Protection Regulation (GDPR).

writing, the ASEAN was also contemplating the development of an ad hoc certification scheme as another component of the Cross-border Data Flow Mechanism.

While the size of ASEAN member countries' economies and digital sectors are much larger than those of CSME countries, both groups need to improve regional cohesion around the development of strong data protection standards. ASEAN has identified increased alignment around strong data protection standards as a key strategy to facilitate cross-border data transfers, increase users' trust in digital services, and to promote trade and innovation in the digital economy. ASEAN has taken a non-prescriptive approach to do so, which CSME countries could draw upon.

4.4 The situation in the CSME

While the CSME is not a major global data hub, it has significant exposure to international data flows and key industries, including financial services, business process outsourcing and tourism, rely on these data flows. Safeguarding these flows is an important policy objective for the CSME.

There are no insurmountable obstacles for the CSME member countries individually or the CSME collectively to achieve adequacy; however, doing so requires a deliberate and holistic long-term strategy by the relevant data protection authorities in the CSME. While small jurisdictions like Jersey, the Isle of Man and Uruguay have received and maintained adequacy status, and countries like Japan have overcome significant obstacles in a short amount of time to achieve adequacy, the value of adequacy needs to be weighed against the alternatives. These include the organic development of data protection laws and practices and the promotion of global rules for data-enabled trade, such as a Global Agreement on Privacy within the WTO (see Chander and Schwartz 2023).

BCRs are a useful instrument for firms with a presence in the CSME that deal with data on EU data subjects. As CSME data protection practices, law and enforcement develop, they become easier for CSME-based firms to implement, but remain costly and will thus be appropriate mostly for international enterprises. Implementing a BCR requires international co-ordination within a corporation throughout its global operations and then formal approval by an EU data protection authority, which can be a lengthy process.

As of June 2023, the European Data Protection Board had registered 49 BCRs,[78] while the UK Information Commissioner's Office had registered 11 (ICO n.d.). Several of the multinationals that have registered BCRs have a presence in the CSME, including professional services firms such as BDO and industrial firms such as the Mercedes Benz Group. As such, BCRs are a useful mechanism for data transfers to and from the CARICOM region. However, their application seems limited and at the time of writing, there were no CSME-headquartered firms with a registered BCR.

4.5 Gaps and recommendations

As the analysis in Section 3.3 shows, the alignment between the CSME data protection laws and the GDPR is incomplete. Individual data rights, as well as the rules on international data transfers, are areas where there are significant gaps. It is therefore unlikely that an adequacy assessment by the EC is currently an option for the CSME as a whole. A detail worth noting is that adequacy can be assessed at the level of 'a third country, a territory or one or more specified sectors within a third country, or an international organisation' (GDPR Art. 45). This means that individual CSME members or territories within the CSME, or specific industries, may pursue adequacy individually. However, apart from the Safe Harbor/Privacy Shield frameworks, which do not offer a promising precedent, there is little experience with non-state adequacy[79] – so this must be considered a highly risky approach.

There is nonetheless merit in aiming for higher standards in data protection and international alignment, even if adequacy is not the goal. For one, it makes the implementation of BCRs easier for companies operating in the CSME.

In general, the focus of CSME authorities should be the organic development of the data protection regime to ensure the protection of CSME citizens.

78 Of these, 35 are controller BCRs and 14 are processor BCRs. See: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en.

79 One limited adequacy finding for a single sector is in place for airline transfers of passenger name records from the EU to the USA.

BCRs and SCCs are open to CSME-based firms, but they are generally viewed as being relatively costly and inflexible measures. SCCs do not fit each type of data transfer, must be used without change, and are considered as imposing terms that 'are relatively onerous to meet and can lead to high administrative costs'. BCRs are not likely to be useful for start-ups and other CSME-based businesses offering services directly to EU citizens.

The other options are explicit consent and contractual necessity as the key derogations (Art. 49 GDPR) that are relevant for commercial enterprises and are likely to be a viable alternative for businesses that enter into direct contractual relationships with EU individuals (B2C) – for example, in e-commerce and the travel industry. However, derogations are less likely to be appropriate for firms receiving personal data in bulk (B2B).

The CSME can strengthen its international position as a participant in international data markets by harmonising data protection law and practice internally (as with the ASEAN experience), while advocating for a trade-friendly data protection system globally.

5. Consumer Protection Issues

Key findings

- Digital markets can give rise to specific types of consumer harm, including data breaches, and manipulation of the choice environment ('dark patterns').
- While there is no firm evidence on the prevalence of digital harms in the CSME member countries, such harms are likely to be present to varying degrees.
- Current consumer protection frameworks are not designed to address complex digital harms. Some CSME countries have established legislation related to consumer protection, data protection, electronic transactions and cybercrime. Others have laws pending.
- Gaps in digital literacy within the CSME could worsen consumer risks. Hence, the CCC, under its functions under Chapter VIII of the Revised Treaty of Chaguaramas (RTC) to support member countries, should investigate the extent of digital consumer harms as a first step in advising consumer protection policy.
- The development of new legislation should consider both its impact on digital innovation and consumer benefits, ensuring it does not hinder helpful products and services.

5.1 Background

Digital technologies are a source of innovation and economic growth that deliver substantial benefits to consumers. At the same time, consumers in digital markets can also face a range of new and amplified risks. These can range from data breaches to excessive prices and discrimination to emotional distress or anxiety. In a digital environment, consumer harms can be amplified and new distinctly digital harms emerge (London Economics 2022).

The best-known risk to consumers in the digital environment is the risk of a data breach. This harms consumers directly, through:

- Identity theft: This is the most serious consequence of a data breach. When a hacker steals personal information, they can use it to open new accounts or make unauthorised purchases.
- Financial loss: If credit card information is stolen, consumers may be liable for any unauthorised charges.
- Damage to reputation: A data breach can damage individuals' reputation and make it difficult to get loans, jobs or housing.
- Stress and anxiety: A data breach can be a very stressful and anxiety-provoking experience.
- Loss of privacy: When personal information is stolen, individuals lose control over who has access to that information, leaving them exposed and vulnerable.

In addition to these direct consequences, data breaches can also have several indirect consequences. For example, they can lead to:

- Increased distrust of businesses and organisations: When consumers lose trust in businesses and organisations, they may be less likely to do business with them. This can have a negative impact on the economy.
- Increased regulatory compliance costs: Businesses and organisations that experience data breaches may face increased regulatory compliance costs. This is because they will need to implement new security measures and procedures to protect their customers' data.
- Increased legal liability: Businesses and organisations that experience data breaches may face increased legal liability. This is because they may be held responsible for the financial losses and other damages that their customers suffer because of the breach.

A particular feature of digital markets is that they provide firms with new tools to shape the consumer experience. For example:

Table 5.1 Categorisation of digital consumer harms

Category	Description
Barriers to effective, informed consumer decision-making	• Distorted consumer choices (dark patterns) • Misinformed consent
Misleading or false content	• Fake reviews • Fraud/scams
Barriers to switching and multi-homing	• Service tying/bundling • Frictions such as sign-up processes, loss of data/lack of portability/interoperability, egress fees
Unfair consumer data practices	• Algorithmic discrimination and targeting • Loss of control over personal data
Exploitative behaviour	• Excessive data collection • Excessive advertising • Excessive prices

Note: Egress fees refer to charges or fees associated with the outbound data transfer or traffic from a network, online platform or cloud service, typically incurred by users when switching from one service provider to another. The categories above focus on harms associated with commercial transactions between consumers and firms. They do not consider some harmful online content and conduct, specifically: illegal and age-inappropriate content; and conduct such as bullying, trolling and harassment.[80]

Source: London Economics (2022).

- It is much easier for businesses operating in the digital environment to manipulate the **choice environment** facing consumers in a way that encourages specific decisions. Choice architecture, including routing, available choices, the mechanics of the user interface and presentation features can all be designed in ways that shape consumers' cognitive and emotional responses. These features can be tailored to specific consumers more easily in digital markets than elsewhere to influence decision-making.
- The large number of choices available across many digital markets means that consumers are often influenced by **ratings and recommendations** from people that are unknown to them. This can be a positive, as it helps consumers make informed decisions. However, it creates a challenge – as these reviews are not always legitimate and are unverified.
- Digital markets are increasingly fast-moving and decisions 'at the click of a button' have an immediate impact. End users have also developed a reduced tolerance for delay, leading to **default behaviour** (a propensity to accept whichever default option is presented to save time and effort) and them being prone to **status quo bias** (a preference for remaining with the existing option, even where this is not the rational choice). This reduces the likelihood of users switching to new/rival firms' services, even where they might offer better value (Department for Business, Energy and Industrial Strategy [BEIS] 2021).

Table 5.1 provides a categorisation of harms that arise to consumers in digital settings.

5.2 International developments

While data breaches are typically sanctioned as part of a data protection regime and can incur very substantial fines,[81] most countries do not

80 For more information on content and conduct harms, see Ofcom (2019).

81 Examples from Europe include:

- Meta (€1.2 billion): In 2022, the Irish DPC fined Meta (formerly Facebook) €1.2 billion for violating the GDPR by transferring the personal data of European users to the United States without adequate safeguards.
- British Airways (€224 million): In 2018, the UK Information Commissioner's Office (ICO) fined British Airways €224 million for a data breach that affected 500,000 customers.
- Under Armour (€100 million): In 2019, the French data protection authority fined Under Armour €100 million for a data breach that affected 150 million customers.

have explicit legislation in place forbidding harmful behavioural manipulation ('dark patterns'). However, most developed countries have general consumer protection laws covering misleading practices. In the EU, this includes regulations like the Unfair Commercial Practices Directive (UCPD), the Digital Services Act (DSA), the Digital Markets Act (DMA) and General Data Protection Regulation (GDPR).

The UCPD provides the most direct legislation against misleading commercial practices in general. While dark patterns are not explicitly in scope of the GDPR and DMA, the two regulations can be used as a tool for regulating certain dark patterns. The UK Competition and Markets Authority (CMA) proposed a 'fairness by design' duty on digital platforms helping users make informed decisions about their personal data. The DMA can also indirectly address dark patterns. It forbids gatekeepers (i.e. large online platforms) from participating in unfair practices that exploit user dependence or undermine their choices through the 'structure, design, function, or mode of operation of a user interface'.

The EU Data Services Act explicitly imposes a ban on dark commercial patterns by digital platforms. By doing so, it will give greater protection to consumers by providing a robust 'transparency and accountability framework for online platforms' throughout the EU.

The Australian Consumer Law (ACL) forbids firms from participating in deceptive conduct in trade or commerce. This includes dark patterns. For instance, in 2019, the Australian Competition and Consumer Commission published a guide on *Online Platforms and the Australian Consumer Law* that detailed the legal conditions for digital platforms regarding consumer protection and explicitly stated that the use of dark patterns served as a violation to this law.

Likewise, the US implemented the DETOUR Act in 2019, which aims to ban large digital platforms from using dark patterns to deceive consumers into surrendering their private data. Recently, US authorities have been clamping down on firms for exploiting dark patterns. For example, in June 2023, the Federal Trade Commission took action against Amazon.com, accusing it of 'tricking' consumers to enrol with Amazon Prime and deliberately introducing frictions if consumers wished to cancel their subscriptions. Here, Amazon has been accused of using dark patterns to manipulate consumer behaviour.

5.3 Situation in the CSME

5.3.1 Evidence of harms

Our research has revealed several significant data breaches in CSME member countries in recent years.

One example is a data breach that affected the Barbados Government's immigration department in 2019. The breach resulted in the personal information of more than 24,000 individuals who had applied for visas to travel to Barbados being exposed, including names, dates of birth, passport numbers and other sensitive data. The government apologised for the breach and took steps to address the issue, including launching an investigation and strengthening its data protection measures.

In 2020, the University of the West Indies (UWI), which has campuses across several CARICOM countries, experienced a data breach that exposed the personal information of more than 4,000 students and staff members. The breach was attributed to a vulnerability in the university's online learning platform, and the university took steps to fix the issue and notify those affected.

Other notable data breaches in the region include a breach that affected the Trinidad and Tobago Government's immigration division in 2018, and a breach that affected a Jamaican telecoms provider in 2017. These incidents highlight the importance of robust data protection measures and cybersecurity practices in the CARICOM region, as in other parts of the world.

In respect of other digital consumer harms, we have not undertaken a comprehensive review of the prevalence of digital harms in the CSME, but all of them are likely present to a greater or lesser degree.

5.3.2 Legislative framework

There are four main areas of legislation in CARICOM countries pertaining to consumer protection in the context of the provision of digital products and services:

- General consumer protection acts: These provide an overarching legal framework to govern consumer interactions and transactions with businesses. They seek

to protect consumers from unfair business practices and ensure that they receive safe, reliable, and quality goods and services.

- Electronic transactions acts: These provide a legal framework for the validity of electronic transactions, and may include provisions that ensure that consumers' interests are protected while conducting electronic transactions (for example, Jamaica's Electronic Transactions Act, Grenada's Electronic Transactions Act).
- Cybercrime/computer misuse acts: These provide a legal framework for crimes committed using computer technology, including data breaches.
- Data protection acts:[82] These provide a legal framework to oversee the use of personal and sensitive data.

Table 5.2 provides an overview of the status of the availability of legislation in each area across the CARICOM and CSME countries:

- green indicates that the legislation exists and is fully in force;
- amber indicates that the legislation has been drafted but is not (fully) in force yet; and
- red indicates that the relevant legislation is missing.

There is some disparity regarding the status of legislation availability across the CARICOM and CSME countries. Some countries, including The Bahamas, Barbados, Antigua and Barbuda, and Jamaica, have existing legislation across the four areas. There are some countries where legislation is mostly available but pending to be finalised and fully enacted, mainly in the area of data protection. These countries include Saint Lucia, St Vincent and the Grenadines, Trinidad and Tobago, Guyana, and St Kitts and Nevis. The Electronic Communications and Transactions Bill and the Consumer Protection Act are pending enactment in Guyana and St Kitts and Nevis, respectively. Some countries are missing legislation in one to multiple areas. Belize is missing legislation in consumer protection, while Grenada is missing legislation in data protection. Suriname is missing both consumer protection and cybercrime legislation, while Dominica is missing legislation in consumer protection, data protection and cybercrime.

General consumer protection legislation provides some foundation to protect consumers against unfair trade practices and terms.

The consumer protection legislation in place in CSME member countries typically offers flexibility to address at least some consumer harms in digital markets. For example, the Antigua and Barbuda Consumer Protection and Safety Act (1987) is explicitly concerned with 'methods of salesmanship employed in dealing with customers' (Art. 2(1)(d)) and can be used to ban practices that have or are likely to have the effect 'of misleading or confusing the consumer' or 'of subjecting consumers to undue pressure to enter consumer transactions; of causing the terms or conditions on which consumers enter into consumer transactions to be so adverse to them as to be onerous' (Art. 16). In principle, this could be applied to prohibit 'dark patterns' used in e-commerce and to restrict excessive data disclosure requirements, for example.

Similarly, the Barbados Consumer Protection Act (2002) contains a prohibition against making 'a representation with respect to an amount that, if paid, would constitute a part of the consideration for the supply of the goods or services' (Art. 17), which could be used against harmful practices like drip-pricing (where consumers have completed a large part of the buying process before they are shown the final price, often in conjunction with scarcity signals – such as, 'x other customers have this item in their basked', 'only x items left').

However, the existing legislation may be too broad and unspecific to address the nuances and complexities of consumer harms that can arise in digital market transactions (for example, personal data processing for automated consumer profiling, digital platform choice architecture), at least without further guidance.

Some electronic transactions legislation includes relevant data protection and privacy provisions, such as restrictions on the disclosure by businesses of private information on individuals (for example, Barbados ETA, Part VI). Nevertheless, these provisions have some limitations: for example, no provisions on anonymisation of data and limited liability of intermediaries.

There is a larger variability in the scope of computer misuse or cybercrime laws across the countries.

82 See Section 3.

Table 5.2 Status of legislation pertaining to consumer protection in digital markets in CARICOM and CSME countries

CARICOM member country	Consumer Protection Legislation	Privacy/ Data Protection Legislation	Electronic Transactions Legislation (ETA)	Cybercrime/ Computer Misuse Legislation
Antigua and Barbuda	Consumer Protection Act, 1987[83]	Data Protection Act, 2013[84]	Electronic Transactions Act, 2013[85] Electronic Transactions (Amendment) Act, 2016[86]	Electronic Crimes Act, 2013[87] and Amendments 2018, 2019, 2020
The Bahamas	Consumer Protection Act, 2006[88]	Data Protection (Privacy of Personal Information) Act, 2003[89]	Electronic Communications and Transactions Act, 2006[90]	Computer Misuse Act, 2006[91]
Barbados	Consumer Protection Act, 2002[92] Consumer Guarantees Act, 2002[93]	Data Protection Act, 2019[94]	Electronic Transactions Act, 2001[95]	Computer Misuse Act, 2005[96]
Belize	No law	Data Protection Act, 2021[97]	Electronic Transactions Act Chapter 229:03, 2020[98]	Cybercrime Act, 2020[99]
Dominica	No law	No law	Electronic Transactions Act, 2013[100] Electronic Funds Transfer Act, 2013[101]	No law
Grenada	Consumer Protection Act, 2018[102]	No law	Electronic Transactions Act, 2013[103]	Electronic Crimes Act, 2013[104]
Guyana	Consumer Affairs Act, 2011[105]	Draft law in consultation stage: Data Protection Bill, 2023[106]	Pending enactment: Electronic Communications and Transactions Bill, 2018[107]	Cybercrime Act, 2018[108]
Jamaica	Consumer Protection Act, 2005[109]	Data Protection Act, 2020[110]	Electronic Transactions Act, 2007[111]	Cybercrimes Act, 2015[112]
Saint Lucia	Consumer Protection Act, 2016[118]	Partially enacted: Data Protection Act, 2011[119]	Electronic Transactions Act, 2020[120]	Computer Misuse Act, 2020[121] Criminal Code Act 9 of 2004
St Kitts and Nevis	Pending enactment: Consumer Protection Act, 2018 In force: Consumer Affairs Act, 2003[113]	Pending enactment: Data Protection Act, 2018[114]	Electronic Transactions Act, 2011[115] Electronic Communications Act, 2021[116]	Electronic Crimes Act, 2009[117]
St Vincent and the Grenadines	Consumer Protection Bill, 2019[122]	Pending enactment: Privacy Ac, 2003[123]	Electronic Transactions Act, 2015[124]	Cybercrime Act, 2016[125]

(*Continued*)

Table 5.2 Status of legislation pertaining to consumer protection in digital markets in CARICOM and CSME countries (*Continued*)

CARICOM member country	Consumer Protection Legislation	Privacy/ Data Protection Legislation	Electronic Transactions Legislation (ETA)	Cybercrime/ Computer Misuse Legislation
Suriname	No law	Pending enactment: Bill for the Privacy Protection Act and Personal Data, 2018[126]	Wet Elektronisch Rechtsverkeer, 2017[127]	No law
Trinidad and Tobago	Consumer Protection and Safety Act, 1985[128]	Partially enacted: Data Protection Act, 2011[129]	Electronic Transactions Act, 2011[130]	Computer Misuse Act, 2000[131]

Source: Authors' analysis.

83 Antigua and Barbuda, Consumer Protection Act, 1987, available at: https://faolex.fao.org/docs/pdf/ant70182.pdf
84 Antigua and Barbuda, Data Protection Act, 2013, available at: http://laws.gov.ag/wp-content/uploads/2019/02/a2013-10.pdf
85 Antigua and Barbuda, Electronic Transactions Act, 2013, available at: http://laws.gov.ag/wp-content/uploads/2019/02/a2013-14.pdf
86 Antigua and Barbuda, Electronic Transactions (Amendment) Act, 2016, available at: http://laws.gov.ag/wp-content/uploads/2019/02/a2016-10.pdf
87 Antigua and Barbuda, Electronic Crimes Act, 2013, available at: http://laws.gov.ag/wp-content/uploads/2019/02/a2013-14.pdf
88 The Bahamas, Consumer Protection Act, 2006
89 The Bahamas, Data Protection (Privacy of Personal Information) Act, 2003
90 The Bahamas, Electronic Communications and Transactions Act, 2006
91 The Bahamas, Computer Misuse Act , 2006
92 Barbados, Consumer Protection Act, 2002, available at: https://faolex.fao.org/docs/pdf/bar81010.pdf
93 Barbados, Consumer Guarantees Act, 2002, available at: https://faolex.fao.org/docs/pdf/bar176423.pdf
94 Barbados, Data Protection Act, 2019, available at: https://gisbarbados.gov.bb/download/data-protection-act-2019/
95 Barbados, Electronic Transactions Act, 2001, available at: http://barbadosparliament-laws.com/en/showdoc/cs/308B
96 Barbados, Computer Misuse Act, 2005, available at: https://cmabarbados.com/Barbados-Computer-Misuse-2005.pdf
97 Belize, Data Protection Act, 2021, available at: www.nationalassembly.gov.bz/wp-content/uploads/2021/12/Act-No-45-of-2021-Data-Protection-Act.pdf
98 Belize, Electronic Transactions Act, Chapter 229:03, 2020, available at: www.agm.gov.bz/uploads/laws/63976fd14681f_Cap_229.03_Electronic_Transactions_Act.pdf
99 Belize, Cybercrime Act, 2020, available at: www.nationalassembly.gov.bz/wp-content/uploads/2020/10/Act-No.-32-of-2020-Cybercrime.pdf
100 Dominica, Electronic Transactions Act, 2013, available at: https://dominica.gov.dm/laws/2013/Electronic%20Transactions%20Act,%202013%20Act%2019%20of%202013.pdf
101 Dominica, Electronic Funds Transfer Act, 2013, available at: https://dominica.gov.dm/laws/2013/Electronic%20Funds%20Transfer%20Act,%202013%20ACT%2017%20of%202013.pdf
102 Grenada, Consumer Protection Act, 2018, available at: www.laws.gov.gd/index.php?option=com_edocman&task=document.viewdoc&id=1278&Itemid=213
103 Grenada, Electronic Transactions Act, 2013, available at: www.laws.gov.gd/index.php?option=com_edocman&task=document.download&id=1095&Itemid=213
104 Grenada, Electronic Crimes Act, 2013, available at: www.laws.gov.gd/index.php?option=com_edocman&task=document.download&id=1097&Itemid=213
105 Guyana, Consumer Affairs Act, 2011, available at: https://fuzearts.gy/clients/CCAC/wp-content/uploads/2018/08/Consumer-Affairs-Act.pdf
106 Guyana, Data Protection Bill, 2023 (draft), available at: www.mola.gov.gy/sites/default/files/DATA%20PROTECTION%20BILL%202023.pdf
107 Guyana, Electronic Communications and Transactions Bill, 2018 (pending enactment), available at: https://ectaguyana.com/Guyana-Electronic-Communications-and-Transactions-Bill-2018.pdf
108 Guyana, Cybercrime Act, 2018, available at: https://officialgazette.gov.gy/images/gazettes-files/Extra_13AUG2018Act16of2018.pdf
109 Jamaica, Consumer Protection Act, 2005, available at: www.miic.gov.jm/sites/default/files/pdfs/Consumer%2520Protection%2520Act.pdf
110 Jamaica, Data Protection Act, 2020, available at: https://japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202020.pdf
111 Jamaica, Electronic Transactions Act, 2007, available at: https://laws.moj.gov.jm/library/statute/the-electronic-transactions-act

112 Jamaica, Cybercrimes Act, 2015, available at: www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf
113 St Kitts and Nevis, Consumer Affairs Act, 2003, available at: https://aglcskn.info/wp-content/documents/Act02and09TOC/Ch-18_38-Consumer-Affairs-Act.pdf
114 St Kitts and Nevis, Data Protection Act, 2018 (pending enactment), available at: https://aglcskn.info/wp-content/documents/Annual-Laws/2018/ACTs/Act-5-of-2018-Data-Protection-Act-2018.pdf
115 St Kitts and Nevis, Electronic Transactions Act, 2011, available at: www.wipo.int/wipolex/en/text/579964
116 St Kitts and Nevis, Electronic Communications Act, 2021, available at: www.ntrc.kn/wp-content/uploads/2021/05/Electronic-Communications-Act-No.-3-of-2021.pdf
117 St Kitts and Nevis, Electronic Crimes Act, 2009, available at: https://aglcskn.info/wp-content/documents/Act17TOC/Ch-04_41-Electronic-Crimes-Act.pdf
118 Saint Lucia, Consumer Protection Act, 2016, available at: https://faolex.fao.org/docs/pdf/stl192160.pdf
119 Saint Lucia, Data Protection Act, 2011 (partially enacted), available at: http://attorneygeneralchambers.com/laws-of-saint-lucia/data-protection-act
120 Saint Lucia, Electronic Transactions Act, 2020, available at: http://attorneygeneralchambers.com/laws-of-saint-lucia/electronic-transaction-act
121 Saint Lucia, Computer Misuse Act, 2020, available at: http://attorneygeneralchambers.com/laws-of-saint-lucia/computer-misuse-act
122 St Vincent and the Grenadines, Consumer Protection Bill, 2019, available at: http://assembly.gov.vc/assembly/images/ActsBillsPolicies/Consumer_Protection_Bill_2019_final_draft.pdf
123 St Vincent and the Grenadines, Privacy Act, 2003 (pending enactment), available at: www.theinformationcollective.com/dpl/st-vincent-and-the-grenadines-the-privacy-act
124 St Vincent and the Grenadines, Electronic Transactions Act, 2015, available at: https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/vc/vc021en.pdf
125 St Vincent and the Grenadines, Cybercrime Act, 2016, available at: http://assembly.gov.vc/assembly/images/ActsBillsPolicies/SVG_Cybercrime_Act_2016.pdf
126 Suriname, Bill for the Privacy Protection Act and Personal Data, 2018 (pending enactment), available at: www.dna.sr/media/307641/Wet_Bescherming_Privacy_en_Persoonsgegevens.pdf
127 Suriname, Wet Elektronisch Rechtsverkeer, 2017, available at: http://www.dna.sr/media/192966/SB_2017___86.pdf
128 Trinidad and Tobago, Consumer Protection and Safety Act, 1985, available at: https://tradeind.gov.tt/wp-content/uploads/2016/02/Consumer-Protection-and-Safety-Act-82.34.pdf
129 Trinidad and Tobago, Data Protection Act, 2011 (partially enacted), available at: https://agla.gov.tt/downloads/laws/22.04.pdf
130 Trinidad and Tobago, Electronic Transactions Act, 2011, available at: https://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/22.05.pdf
131 Trinidad and Tobago, Computer Misuse Act, 2000, available at: https://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/11.17.pdf

For example, The Bahamas' Computer Misuse Act mainly targets unauthorised access to and disclosure of computer material (for example, data and programs). In contrast, Grenada's Electronic Crimes Act has a wider scope and includes provisions on violation of privacy (albeit restricted definition)[132] and harmful content. However, the main aim of these legislations is to criminalise malpractices in the digital space at the individual level through *ex post* action (fines, imprisonment). They do not provide *ex ante* provisions requiring firms to undertake certain actions and procedures to protect consumers against addressable digital harms (such as, breaches of personal data and sensitive data, non-consensual consumer profiling or unsolicited digital marketing). A more detailed assessment of the data protection legislation available in the different CARICOM/CSME countries is provided in section 3.3.

5.3.3 Digital literacy

Digital literacy is a key instrument for ensuring protection against digital consumer harms, alongside a strong legislative framework. This section describes evidence of gaps in digital literacy and inclusion in the CSME, which can exacerbate some of the digital harms to consumers.

Basic digital literacy rates are higher in the CARICOM countries than the global average, but there remain gaps in digital literacy and skills (GSMA 2016). For example, the 2021 National Digital Inclusion Survey of Trinidad and Tobago finds that while 30 per cent of citizens have standard ICT skills, only 4 per cent have advanced ICT skills (TATT 2021). A study assessing the e-commerce readiness of the six member countries of the Organisation of Eastern Caribbean States (OECS)[133] finds that citizen readiness in e-commerce exhibits severe gaps and should be addressed through the completion of digital skills assessments and training initiatives (Commonwealth Secretariat 2021). Moreover, the COVID-19 pandemic has accelerated the shift from in-person to online services and emphasised the digital divides and inequalities in the Caribbean region. For example, the schooling of children from rural areas, disadvantaged backgrounds or children with disabilities was disproportionately impacted during the pandemic due to their limited access to online learning tools and services (Bleeker and Crowder, 2022). Similarly, firms that did not adopt digital payments and technologies were more likely to fail as a result of the pandemic (Acevedo 2021). Digital divides – that is, unequal access to ICTs – and digital literacy gaps are interconnected,[134] both increasing the vulnerability of consumers that are already economically and socially disadvantaged (Alexander et al. 2023). Improving digital literacy is key to promoting and ensuring trust in the use of new and emerging technologies, applications and services among all individuals (TATT 2021).

Some Caribbean governments and organisations have started initiatives to drive digital transformation and address issues of digital divide and literacy at the national/territorial level and the regional level. For example, initiatives at the regional level include the 'Vision and Roadmap for a CARICOM Single ICT Space' (Caribbean Telecommunications Union 2017) and the eLAC2022 (ECLAC 2020), which sets out to promote co-operation in the Latin America and Caribbean region in order to achieve digital objectives.

At the national level, Caribbean countries are in various stages of development and implementation of initiatives aimed at addressing issues of digital divide and literacy. An ECLAC-commissioned study on digital inclusion in the Caribbean finds that while some Caribbean countries have an ICT plan in force, only a few address digital inclusion in their policy framework[135] (Alexander et al. 2023). It finds that digital inclusion efforts remain ad hoc and fragmented, instead of being articulated as part of a broader strategic direction. Similarly, some countries are pushing for improvements in digital literacy. For example, Jamaica launched the five-year 'Digital Skills Training Programme' in 2021, partnering with Microsoft to offer free training in various digital skills areas to more than 150,000 Jamaicans (Angus 2021).

The ECLAC study finds that digital skills in the public sector may be lacking, which can hinder the

132 Provisions on privacy violation mainly target pictures and videos related to the private parts of individuals.

133 The OECS includes Antigua and Barbuda, St Kitts and Nevis, Saint Lucia, St Vincent and the Grenadines, Dominica and Grenada.

134 A digital divide, or limited access to technology and the internet, can hinder digital literacy development. Improved digital literacy, meanwhile, can help overcome some of the barriers created by the digital divide.

135 For example, Jamaica, Trinidad and Tobago, Saint Lucia, and St Vincent and the Grenadines – as identified in the assessment of the ECLAC 2023 Digital Inclusion study.

ability of the government to orchestrate effective digital transformation policies (Alexander et al. 2023). Moreover, when it comes to the provision of e-government services in Caribbean countries, there are significant gaps in citizen awareness and usage of their government's digital service offerings, driven by unfriendly user interfaces, digital divide (that is, lack of connectivity and suitable devices) and lack of trust in personal data usage by the government (PwC in the Caribbean 2022).

5.4 Gaps and recommendations

The gaps in legislation in the CSME identified in Table 5.2, in particular in terms of consumer protection and data protection, should be closed to ensure a consistent level of protection for consumers across the CSME.

Existing consumer protection frameworks in CSME member countries are not designed to protect consumers from modern and complex forms of digital harm. Examples of these harms include algorithmic decision-making processes that lead to discriminatory treatment of consumers or dark patterns that 'distort or impair' the user's ability to make a free choice.

While there is no firm evidence of the prevalence of digital harms in the CSME, they are likely to be present to a greater or lesser degree. Moreover, the risk of digital harm to consumers is potentially exacerbated by the remaining gaps in digital literacy in the CSME member countries.

A useful first step would be for the CCC to investigate the prevalence of digital consumer harms in the CSME, in fulfilment of its mandate to provide support to CSME member countries in promoting consumer welfare.

As a second step, the CCC may issue guidance on the treatment of digital consumer harms under the existing consumer protection legislation to ensure a level playing field for consumers and businesses within the CSME. On this basis, the CCC could support member countries' review of consumer protection legislation to determine whether updates are needed to address specific digital consumer harms.

This would provide policy-makers with a better understanding of how to prioritise the development of new legislative elements to tackle digital harms efficiently. The development of new legislation should also carefully assess the potential impact of that legislation on digital innovation and make sure that it does not impede the development and availability of products and services that are beneficial to consumers.

Providing consumers with information on digital harms (for example, on the CCC website and/or through publicity campaigns) and embedding such information in a wider digital skills strategy are useful auxiliary steps. Businesses in the CSME can implement measures to complement regulatory and legislative initiatives aimed at strengthening consumer protection in digital markets. Such measures include:

- enhancing privacy policies that provide consumers with increased transparency regarding personal data processing;
- adopting relevant industry standards and codes of conduct (if available), which are voluntary instruments to help organisations apply data protection provisions that typically have been tailored to address the specific needs of the sector;
- enhancing security and anti-fraud measures: for example, encryption to encode data in transit or storage, enhanced user authentication, regular audits, fraud detection systems;
- enhancing customer support with more responsive channels to address consumer issues and feedback; and
- supporting the development of consumer awareness and education about digital risks and harms and best practices on how to address those risks and harms.

6. Conclusions

6.1 SWOT analysis

Key insights discussed in this report have been synthesised into a SWOT (strengths, weaknesses, opportunities, threats) analysis of the CSME countries in terms of their personal data protection legislative provisions, as well as their potential for increased regional and global integration in digital markets.

6.1.1 Strengths

The CSME countries exhibit competitive strengths in the global market for digital products and services. A population of native (and in some cases multilingual) speakers in English, French, Spanish, Dutch and Portuguese is one of the key strengths of the region. This makes it easier for Caribbean companies operating in domestic digital markets to scale up their distribution to a wider international consumer base, but also for foreign companies (for example, US and EU firms) to expand their operations in the Caribbean region.

Moreover, in the latter case, the region also offers foreign firms with relatively low cost of operations (for example, 35 to 75 per cent cost arbitrage over tier-2 US cities) (CARICOM 2016), a skilled and service-oriented workforce, as well as competitive ICT infrastructure and services. This has helped grow business processing outsourcing into a key area of success for the region. The Caribbean region has been identified as one of the most attractive locations for large US firms looking to 'near shore' some of their operations (Caribbean Export Development Agency 2019).

The region is also home to a budding local digital start-up scene (Loop 2021). Some examples of successful local firms include MDLink, an online medical consultation platform based in Jamaica that provides services throughout the Caribbean region,[136] and Wipay, an online payment platform based in Trinidad and Tobago.[137]

With the CCC, the CSME has a credible competition authority with sufficient powers to enforce standards for competition and consumer protection with the CSME. Most CSME member countries have relevant data protection and consumer protection laws.

6.1.2 Weaknesses

The majority (9 out of 13) of CSME member countries do not have competition laws. CSME-wide alignment of competition policy for digital markets requires that there are no gaps in the legal framework.

In relation to consumer protection, most CSME member countries have relevant laws that offer flexiblity in dealing with consumer issues in digital markets. However, the lack of relevant guidance and specific provisisons addressing digital consumer harms may be an impediment to effective consumer protection.

In data protection, there is a lack of harmonisation both between CSME member countries and in terms of their alignment with international best practices (that is, with the EU GDPR).

Current gaps in the legislative requirements of safeguard mechanisms in international data transfers could impede the ease with which domestic and foreign businesses will be able to transfer data within and outside countries in the region. This could ultimately have negative effects on the economic activity of the region, across most sectors that involve personal data processing.

Gaps in legislative requirements to provide for the right of access and right to data portability could also have a negative impact on the contestability of digital markets in the region. These rights impact the way businesses in digital markets operate and engage with consumers and could help promote competition in these markets. In particular, the right to data portability can empower consumers to choose among competing providers by reducing user switching costs and frictions associated with trying new services. This could in turn stimulate competition in markets where personal user data is valuable, by making it easier for new entrants to attract users – that is, by reducing barriers of entry associated with data access.

136 MDLink, Homepage, available at: https://themdlink.com/
137 Wipay, Homepage, available at: https://wipaycaribbean.com/

6.1.3 Opportunities

CSME countries should continue with their concerted efforts to drive further regional integration in digital markets and harmonisation in data protection and digital market regulation. An earlier example of such initiatives is the 2012 development of the HIPCAR proposed model law, which enshrines a regional approach to personal data protection.

More recently, CARICOM has unveiled plans to fast-track digital transformation in the region, including through the Girls in ICT Partnership Action Plan and the draft action plan for the CARICOM Digital Skills Task Force (CARICOM 2022). A project looking to assess the ICT sector in each CARICOM member and associate member state was also launched in March 2023 and aims to deliver a regional digital co-operation framework (Nurse 2023).

There are huge gains from an increased alignment in data protection legislation within the region, as well as with international best practices. These include increased cross-border data transfers and trade, in particular in data-intensive markets, within and outside of the region, with large economic areas such as the EU. Data protection legislation can act as a non-tariff barrier (NTB), similar to national quality standards, with a reductive impact on trade. In a 2020 assessment, the International Monetary Fund (IMF) found that the CARICOM region had huge potential for increased trade and welfare gains from a reduction in NTBs and trade costs. That is, in 2018 terms, a 25 per cent reduction in overall NTBs and trade costs within CARICOM and with non-CSME trade partners could lead to trade and welfare gains for all members worth about US$6 billion, or 7.6 per cent of the region's GDP (Ding and Otker 2020).

6.1.4 Threats

The gaps in relevant legislation (competition, data protection, consumer protection) imply that CSME consumers and businesses face some risks that a more comprehensive legal framework could address. Regarding competition, the threat posed by large digital platforms that may impose unfair trading conditions on business partners and overcharge or otherwise exploit (for example, through extraction of personal data) consumers has led to a shift towards *ex ante* regulation in the EU and the UK, and increased regulatory attention in the US. To the extent that these regulatory developments are effective, they open a gap in the protection available to businesses and consumers in the CSME. Similarly, a better understanding of consumer harms that are specific to digital markets has led to some jurisdictions tightening their consumer protection laws and providing research and guidance to improve protection; such moves are currently not replicated in the CSME.

Furthermore, CSME member countries risk losing out, in the long term, on trade with large economic areas such as the EU to other regions because of misalignment in data protection legislation. There is conflicting evidence on whether the GDPR acts as a non-tariff barrier and has a reductive impact on global trade in data-intensive markets. However, there likely is a higher risk of market shutout from the world's largest trading bloc for developing countries that remain unaligned with the GDPR (Mannion 2020). An increasing number of countries are implementing data privacy laws that ensure alignment and compliance with those enacted in large economic areas such as the EU and the US, including CSME countries (for example, Barbados, Belize and Guyana).

6.2 Key policy challenges

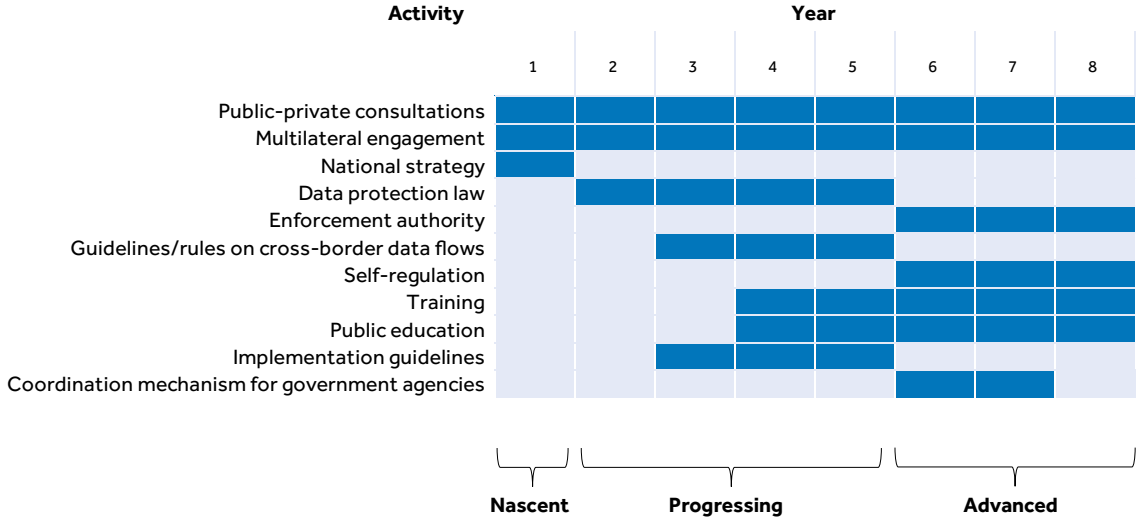
6.2.1 Developing the regional data protection regime

There have been significant developments in the data protection area in the CSME in recent years. However, observers have noted major challenges in this area, namely (Ramsundar 2019):

- lack of a single policy and legislative approach;
- different levels of establishment of key public infrastructure, policies and laws;
- varying levels of public institutional development;
- differing financial and economic policies; and
- lack of political will.

In this light, the CSME countries mostly fall in the 'progressing' category in a schematic of progress to an effective and self-sustaining, mature data protection regime (Figure 6.1).

Figure 6.1 Roadmap of privacy elements – possible stages and timeframe



Source: GSMA. (2018).

Rather than attempting to mirror international data protection laws such as the GDPR, small countries could explore alternative strategies to enhance their data protection capabilities. These might include:

- building upon existing international norms and standards, such as the Council of Europe's Convention 108 or the Asia-Pacific Economic Cooperation (APEC) Privacy Framework;
- collaborating with other countries, organisations or experts to develop tailored solutions that address unique challenges and circumstances; and/or
- leveraging technology and innovation to facilitate compliance, such as using machine learning algorithms to identify and mitigate privacy risks.

To ensure that data protection is aligned with the needs of the citizens of the CSME, the member countries should follow a bottom-up approach to data protection regulation that takes local contextual nuances into account.

At the same time, regional heterogeneity in data protection policy, in particular regarding elements relevant to cross-border data flows, could be problematic. It could reduce cross-border data flows as data protection rules in one country could prohibit data transfers to another in the CSME. This would end up negatively impacting trade and innovation in the regional digital economy.

The CCC could play an important role in advocating for regional harmonisation across the CSME with regard to data protection regulation where it has direct competition implications. It could provide guidance in the development of an aligned approach to data protection regulation with respect to measures to increase contestability of data markets such as data access and portability.

6.2.2 An efficient approach to digital markets regulation

We recommend a fast-follower strategy in terms of competition law enforcement and merger control for digital platforms. A fast-follower strategy involves a smaller player adopting best practices and latest developments from larger players or leaders in the field, and then quickly implementing them to stay competitive. The benefits include the following:

- Efficient use of resources: By following established best practices and guidelines, the CSME authorities can efficiently use their limited resources to address the complex issues arising from digital platform markets.
- Flexibility: A fast-follower strategy allows CSME authorities to adapt quickly to changing market conditions and new developments in technology, which is particularly important in the rapidly evolving digital economy.
- Access to expertise: By leveraging the knowledge and experience of other

jurisdictions, CSME authorities can gain access to expertise and cutting-edge methods and tools that might not be available domestically.

- Enhanced credibility: By demonstrating a commitment to enforcing competition laws and regulating digital platforms consistent with internationally recognised standards, the CSME can enhance its credibility and influence in regional and global economic forums.
- Better positioning for future regulatory co-operation: By closely following the approaches of larger jurisdictions, the CSME can better position itself for future regulatory co-operation and co-ordination, which may become increasingly important as the digital economy continues to grow.

The implementation of this strategy involves:

- creation of the necessary expertise within the CCC;
- ongoing monitoring of relevant international developments; and
- regular review of developments and lessons that are applicable to the CSME.

Participation in international forums and conferences by CCC staff are a minimal requirement for effective implementation of this strategy. A more ambitious strategy would involve co-operation with overseas agencies on digital market topics ranging from regular meetings and knowledge exchange sessions to secondments, personnel exchanges and joint task forces on relevant cases.

References

ABLI (2018), Regulation of cross-border transfers of personal data in Asia. https://abli.asia/abli-projects/convergence-of-data-privacy-laws-and-frameworks-for-cross-border-transfers-of-personal-data-in-asia/

Acevedo (2021), *The Impacts of the COVID-19 Pandemic on Firms in the Caribbean*, Inter-American Development Bank Invest, Washington DC.

Alexander, D, L Døhl Diouf and K Prescod (2023), *Digital inclusion in Caribbean digital transformation frameworks and initiatives: a review*, ECLAC, Santiago.

Alston and Bird (2016), *Transferring data from the EU: Privacy Shield and data transfers under the GDPR*, p 2. https://www.alston.com/files/docs/Roadmap-to-the-GDPR-International-Data-Transfers.pdf

Angus, G (2021), 'Over 150,000 Jamaicans To Benefit From 5-Year Digital Skills Programme', Jamaica Information Service, 31 July, available at: https://jis.gov.jm/over-150000-jamaicans-to-benefit-from-5-year-digital-skills-programme/

Asian Business Law Institute (2018), *Regulation of cross-border transfers of personal data in Asia*, available at: https://abli.asia/abli-publications/regulation-of-cross-border-transfers-of-personal-data-in-asia-softcover/

Association of Southeast Asian Nations (ASEAN) (2016), 'Telecommunications And Information Technology Ministers Meeting (TELMIN). Framework on personal data protection', available at: https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf

ASEAN (2021a), 'ASEAN Data Management Framework. Data governance and protection throughout the data lifecycle', available at: https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf

ASEAN (2021b), 'ASEAN Model Contractual Clauses for Cross Border Data Flows', available at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

Bertuzzi, L (2023), 'EU mulls setting global digital standards with UN Global Digital Compact', Euractiv, 21 March, available at: www.euractiv.com/section/digital/news/eu-mulls-setting-global-digital-standards-with-un-global-digital-compact/?utm_source=piano&utm_medium=email&utm_campaign=30232&pnespid=v_A5GnQZKqQCyv7Pp2q0DsnQ7xXwUJ0rcOW9mbRkrhZmnNqizI4y_rHzY1xCz_RThy30axjj

Bleeker, A (2020), *Creating an enabling environment for e-government and the protection of privacy rights in the Caribbean: a review of data protection legislation for alignment with the General Data Protection Regulation*. Studies and Perspectives series – Economic Commission for Latin America and the Caribbean, ECLAC, Santiago.

Bleeker, A and R Crowder (2022), Selected online learning experiences in the Caribbean during COVID-19, Economic Commission for Latin America and the Caribbean, ECLAC, Santiago.

Bowman, S (2021), 'Breaking Down House Democrats' Forthcoming Competition Bills' *Truth on the Market*, 10 June, available at: https://truthonthemarket.com/2021/06/10/breaking-down-house-democrats-forthcoming-competition-bills/

Braken, A (2022), 'Data protection violations: Managing directors and board members are personally liable'. Certified Senders Alliance, 11 April, available at: https://certified-senders.org/blog/data-protection-violations-managing-directors-and-board-members-are-personally-liable/

Brauer, M and F Erixon (2016), *Competition, Growth and Regulatory Heterogeneity in Europe's Digital Economy*. ECIPE, available at: https://ecipe.org/wp-content/uploads/2016/04/Competition-Growth-and-Regulatory-Heteroge-neity-in-Europe%E2%80%99s-Digital-Economy-final1.pdf

Bundeskartellamt (2016), 'The French Autorité de la Concurrence and the German Bundeskartellamt published a joint paper on data and its implications for Competition Law', available at: www.

bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/10_05_2016_Big%20Data%20Papier.html

Bundeskartellamt (2019), 'Bundeskartellamt prohibits Facebook from combining user data from different sources', available at: www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html?nn=3591568

Bundeskartellamt (2022), 'Compendium of approaches to improving competition in digital markets', available at: www.bundeskartellamt.de/SharedDocs/Publikation/EN/Others/G7_Compendium.pdf?__blob=publicationFile&v=4

Bundeskartellamt (2023), 'Meta (Facebook) introduces new accounts center – an important step in the implementation of the Bundeskartellamt's decision', available at: www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/07_06_Meta_Daten.html;jsessionid=E9D34360D6EAF7217223ACAD6E4EB781.2_cid390?nn=3591568

Bureau of National Affairs (2015), *Why Do We Need Binding Corporate Rules? A Look to the Future*, available at: https://www.huntonak.com/images/content/3/1/v3/3112/Why-Do-We-Need-Binding-Corporate-Rules.pdf

Caribbean Community (CARICOM) (2016), 'Outsource To The Caribbean?', 11 May, available at: https://caricom.org/outsource-to-the-caribbean/

CARICOM (2022), 'ICT Ministers Approve Caricom Secretariat-Led Action Plans To Fast-Track Digital Transformation', 11 February, available at: https://caricom.org/ict-ministers-approve-caricom-secretariat-led-action-plans-to-fast-track-digital-transformation/

CCC (2022), *State of competition enforcement in the CSME* (2019–2021), available at: www.caricomcompetitioncommission.com/images/pdf/report_soc.pdf

Caribbean Export Development Agency (2019), 'The Caribbean Is Best Value Proposition for Outsourcing', 21 February, available at: https://carib-export.com/blog/the-caribbean-is-best-value-proposition-for-outsourcing/

Caribbean Telecommunications Union (2017), *Vision and Roadmap for a CARICOM Single ICT space*, CTU, Trinidad & Tobago.

Chander, A and P Schwartz (2023), 'Privacy and/or Trade', *The University of Chicago Law Review*, Vol. 90 No. 1.

Chen, C, CB Frey and G Presidente (2022), *Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally*, available at: https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf

Commonwealth Secretariat (2021), *Assessment of Digital Trade and E-commerce Readiness and Associated Capacity building Needs in Six Member States of the Organisation of Eastern Caribbean States (OECS)*, Commonwealth Secretariat, London.

Competition Commission South Africa (2020), *Buyer Power Enforcement Guidelines*, available at: www.compcom.co.za/wp-content/uploads/2020/05/Buyer-Power-Guidelines.pdf

Competition Commission South Africa (2022), *Guidelines on small merger notification*, available at: www.compcom.co.za/wp-content/uploads/2022/09/FINAL-GUIDELINES-ON-SMALL-MERGER-NOTIFICATION_.pdf

Competition Policy International (CPI) (2023), 'India Forms Panel To Examine Need For Digital Competition Law', Competition Policy International, 13 February, available at: www.competitionpolicyinternational.com/india-forms-panel-to-examine-need-for-digital-competition-law/

Conselho Administrativo de Defesa Econômica (2021), *Ministério da Justiça e Segurança Pública Conselho Administrativo de Defesa Econômica*, available at: https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/cadernos-do-cade/plataformas-digitais.pdf

Crémer, J, Y-A de Montjoye and H Schweitzer (2018), *Digital policy for the digital era*, available at: https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

CURIA (2016), Judgement of the Court (Fifth Chamber), available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=173680&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=569177

CURIA (2021), 'The General Court Largely Dismisses Google's Action against the Decision

of the Commission Finding That Google Abused Its Dominant Position by Favouring Its Own Comparison Shopping Service over Competing Comparison Shopping Services', available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210197en.pdf

CURIA (2023), 'Judgment of the Court (Grand Chamber)' 4 July, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1652408

Department for Business, Energy and Industrial Strategy (BEIS) (2021), 'Impact Assessment – A new pro-competition regime for digital markets', available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1003915/DMU_Impact_Assessment.pdf

Deloitte (2018), *Data and privacy protection in ASEAN: What does it mean for businesses in the region?*, available at: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf

Digital Competition Expert Panel (2019), *Unlocking digital competition*, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

Ding, D and I Otker (2020), 'Strengthening Caribbean Regional Integration', International Monetary Fund, 4 February, available at: www.imf.org/en/News/Articles/2020/02/04/NA020420-Strengthening-Caribbean-Regional-Integration

DLA Piper (2023), 'Brazil', Data Protection laws of the World, 28 January, available at: www.dlapiperdataprotection.com/index.html?t=law&c=BR#:~:text=The%20LGPD%20is%20Brazil's%20first,enforceable%20on%20August%201%2C%202021.

Eastern Caribbean Telecommunications Authority (ECTEL) (2020), 'Electronic Communications Bill', available at: www.ectel.int/regulatory-framework/electronic-communications-bill/

Economic Commission for Latin America and the Caribbean (ECLAC) (2020), 'Digital Agenda for Latin America and the Caribbean (eLAC2022)', Seventh Ministerial Conference on the Information Society in Latin America and the Caribbean, available at: https://www.cepal.org/en/publications/46440-digital-agenda-latin-america-and-caribbean-elac2022

ECLAC (2022), 'Digital Agenda for Latin America and the Caribbean (eLAC2024) Declaration', Eighth Ministerial Conference on the Information Society in Latin America and the Caribbean Montevideo, available at: https://repositorio.cepal.org/bitstream/handle/11362/48498/S2201147_en.pdf

European Commission (EC) (2020a), 'Impact assessment of the Digital Services Act', available at: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act

EC (2020b), 'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)', available at: https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN

EC (2021a), 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

EC (2021b), 'Standard contractual clauses for international transfers', 4 June, available at: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

EC (2023), 'Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows'. Press release, 10 July, available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3721?s=03 6

EC (n.d.), 'Can individuals ask to have their data transferred to another organisation?', available at: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/can-individuals-ask-have-their-data-transferred-another-organisation_en#references

European Data Protection Board (2020), 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data', November, available at:

https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

European Union (March 2023). European Union contribution to the Global Digital Compact https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_European-Union.pdf.

Goldberg, S., G. Johnson and S Shriver. (2019), Regulating privacy online: The early impact of the GDPR on European web traffic & e-commerce outcomes. https://dx.doi.org/10.2139/ssrn.3421731.

Gonzaga, P (2019), *Algorithms and Collusion*, available at: https://competitioncooperation.eu/wp-content/uploads/2019/01/Day-2-Session-I-Pedro-GONZAGA.pdf

Government of Brazil (2023), 'Brazil asks for more accountability from digital platforms'. Secretaria de Comunicação Social, available at: www.gov.br/secom/en/latest-news/brazil-asks-for-more-accountability-from-digital-platforms

Grentzenberg, V, S Schmechel and J Kranz (2023), "CJEU's landmark decision in Meta vs Bundeskartellamt", DLA PIPER, available at: www.dlapiper.com/en/insights/publications/2023/07/cjeus-landmark-decision-in-meta-vs-bundeskartellamt

GSMA (2016), Digital inclusion in Latin America and the Caribbean, available at: https://www.gsma.com/mobilefordevelopment/resources/digital-inclusion-in-latin-america-and-the-caribbean/

Hausfled (2019), 'Data Exploiting as an abuse of dominance: The German Facebook decision', available at: www.hausfeld.com/en-de/what-we-think/competition-bulletin/data-exploiting-as-an-abuse-of-dominance-the-german-facebook-decision/

Hogan Lovells. (2016, July 22). International Data Transfers: Consider your options. Retrieved January 16, 217, from http://www.hldataprotection.com/2016/07/articles/international-eu-privacy/eu-data-transfers-to-the-u-s-considering-your-options-after-privacy-shield/

Human Rights Watch (2022), 'India: Data Protection Bill Fosters State Surveillance', 22 December, available at: www.hrw.org/news/2022/12/23/india-data-protection-bill-fosters-state-surveillance

Information Commissioner's Office (no date), 'BCRs approved under UK GDPR', available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/guide-to-binding-corporate-rules/bcr-approvals/bcrs-approved-under-uk-gdpr/

International Competition Network Task Force for Abuse of Superior Bargaining Position (2008), Report on Abuse of Superior Bargaining Position, 35. ICN 7th Annual Conference, Kyoto.

International Telecommunication Union (ITU) (2018), *Global ICT Regulatory Outlook 2018*, World Bank, ITU Fig. 1.4, available at: http://handle.itu.int/11.1002/pub/81234575-en

ITU (2022), *Privacy and Data Protection: HIPCAR Model Policy Guidelines & Legislative Texts*, available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/privacy_and_data_protection_model%20policy%20guidelines.pdf

Intersoft Consulting (n.d.), 'GDPR Right of Access', available at: https://gdpr-info.eu/issues/right-of-access/

Ivaldi, M, N Petit and S Unekbas (2023), *Killer Acquisitions: Evidence from EC Merger Cases in Digital Industries*. TSE Working Paper No. 13-1420, available at: http://dx.doi.org/10.2139/ssrn.4407333

Jia, J., G. Z. Jin and L Wagman. (2021). The short-run effects of the General Data Protection Regulation on technology venture investment. Marketing Science 40(4):661–684. https://doi.org/10.1287/mksc.2020.1271

Kerber, W and H Schweitzer (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 8 No. 1, available at: www.jipitec.eu/issues/jipitec-8-1-2017/4531.

Khan, L (2019), 'The Separation of Platforms and Commerce', *Columbia Law Review*, Vol. 119 No. 4, 973–1098, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180174

Kuner, C (2007), *European Data Protection Law: Corporate Compliance and Regulation*, 2nd edition, Oxford University Press, Oxford.

Loop (2021), 5 *Caribbean startups leveraging tech to thrive in a global pandemic*, 21 January,

available at: https://jamaica.loopnews.com/content/5-caribbean-startups-leveraging-tech-thrive-global-pandemic

London Economics (2022), 'Digital consumer issues research', available at: www.gov.uk/government/publications/digital-consumer-issues-research

Lucarini, F (no date), 'How similar is the South African POPIA to the EU GDPR?', *Advisera*, available at: https://advisera.com/articles/how-similar-is-the-south-african-popia-to-the-eu-gdpr

Mannion, C (2020), 'Data Imperialism: The GDPR's Disastrous Impact on Africa's ECommerce Markets', *Vanderbilt Journal of Transnational law*.

Morgan, B (2022), 'Status of Data Privacy Laws in the Caribbean [January 2022]'. *Bartlett D. Morgan*, available at: www.bartlettmorgan.com/2022/01/28/status-of-data-privacy-laws-in-the-caribbean-january-2022/

Morgan, B (2023), 'Guyana publishes draft privacy law for comments', 16 April. *Bartlett D. Morgan*, available at: www.bartlettmorgan.com/2023/04/16/guyana-publishes-draft-privacy-law-for-comments/

Nurse, M (2023), 'Advancing the CARICOM Digital Economy: Assessment of Region's ICT Sector gets underway', *CARICOM Today*, 23 March, available at: https://today.caricom.org/2023/02/27/advancing-the-caricom-digital-economy-assessment-of-regions-ict-sector-gets-underway/

Ofcom (2019), 'Online market failures and harms', available at: www.ofcom.org.uk/__data/assets/pdf_file/0025/174634/online-market-failures-and-harms.pdf

Office of the United Nations High Commissioner for Human Rights (1990), *Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990*, available at: www.refworld.org/pdfid/3ddcafaac.pdf

Organisation for Economic Co-operation and Development (OECD) (2002), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at: www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1686042458&id=id&accname=guest&checksum=C4D1A0A258B8CA77AAB662D3A3CF9E75

OECD (2016), 'Big data: Bringing competition policy to the digital era', available at: www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm

OECD (2019), *Regulatory effectiveness in the era of digitalisation*, available at: www.oecd.org/gov/regulatory-policy/Regulatory-effectiveness-in-the-era-of-digitalisation.pdf

OECD (2020), 'Start-ups, killer acquisitions and merger control', available at: www.oecd.org/competition/start-ups-killer-acquisitions-and-merger-control.htm

OECD (2021), *Data Portability, Interoperability and Digital Platform Competition*, available at: www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf)

Osborne Clarke. (04 February 2016). Can I transfer personal data out of Europe if I have the person's consent? http://www.osborneclarke.com/insights/can-i-transfer-personal-data-out-of-europe-if-i-have-the-persons-consent/

Patel, KN, KT Shinohara, MJ Rosa, JB Harrington, AA Kourinian and H Waltzman (2022), *The American Data Privacy and Protection Act: Is Federal Regulation of AI Finally on the Horizon?*, 21 October, Mayer Brown, available at: www.mayerbrown.com/en/perspectives-events/publications/2022/10/the-american-data-privacy-and-protection-act-is-federal-regulation-of-ai-finally-on-the-horizon

Paul, G, D Sokol and G Baca (2022), 'Key Developments in the United States', *Global Competitive Review*, 25 November, available at: https://globalcompetitionreview.com/guide/digital-markets-guide/second-edition/article/key-developments-in-the-united-states

Pinsent Masons (2023), *International data transfers and Schrems II: GDPR obligations. Pinsent Masons Out-Law Guide*, 4 January, available at: www.pinsentmasons.com/out-law/guides/international-transfers-schrems-ii-gdpr#:~:text=The%20Schrems%20II%20ruling%20confirmed,countries%20without%20an%20adequacy%20decision.

PwC in the Caribbean (2022), *Delivering for citizens: Digital Nation Survey 2022*, available at: https://www.pwc.com/cb/en/services/pdf/digital-nation-report-2022.pdf

Ramsundar, N (2019), 'Are we ready for the digital economy?', Presentation, 14 March, CARICOM Competition Commission.

Schaake, M (2023), 'US regulatory action on the tech sector may come too late — or not at all', *Financial Times*, 8 January, available at: www.ft.com/content/3892776e-ec6f-4551-947f-5aafd01e41b6

Schlesinger, P (2022), 'The neo-regulation of internet platforms in the United Kingdom', *Policy and Internet*, Vol. 14 No. 1, 47–62, available at: https://doi.org/10.1002/poi3.288

Schwartz, P (2019), 'Global data privacy: The EU way', *New York University Law Review*, Vol. 94, 771.

Sidley (2021), 'European General Court Judgment in Google Shopping: Key Takeaways' available at: www.sidley.com/en/insights/newsupdates/2021/11/general-court-judgment-in-google-shopping-key-takeaways

Standing Committee on Finance (2022), *Anti-competitive practices by Big Tech Companies*, Fifty Third Report, available at: https://loksabhadocs.nic.in/lsscommittee/Finance/17_Finance_53.pdf

State of California Department of Justice (2023), California Consumer Privacy Act (CCPA), available at: https://oag.ca.gov/privacy/ccpa

Stigler Committee on Digital Platforms (2019), *Final Report*, available at: www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf

Telecommunications Authority of Trinidad and Tobago (TATT) (2021), *National Digital Inclusion Survey 2021: Accelerating Digital Transformation*, available at: https://cso.gov.tt/wp-content/uploads/2022/06/National-Digital-Inclusion-Survey-DIS-2021-Final-Report.pdf

Tzarevski, A and C Hansen (2022), 'South Africa: The Competition Commission publishes revised Guidelines on Small Merger Notifications', *Global Compliance News*, 2 November, available at: www.globalcompliancenews.com/2022/11/02/https-insightplus-bakermckenzie-com-bm-antitrust-competition_1-south-africa-the-competition-commission-publishes-revised-guidelines-on-small-merger-notifications_10132022/

UNCTAD (2016). Data protection regulations and international data flows: Implications for trade and development. https://unctad.org/publication/data-protection-regulations-and-international-data-flows-implications-trade-and

UNDP Global Centre for Technology, Innovation, and Sustainable Development (2021), *Enabling cross-border data flow: ASEAN and beyond*, available at: www.undp.org/sites/g/files/zskgke326/files/2021-10/enabling-cross-border-data-flow-asean-and-beyond-report.pdf

US Department of Justice (2015), Information: *US v David Topkins*, available at: www.justice.gov/atr/case-document/file/513586/download

US Department of Justice (2023), 'Justice Department Sues Google for Monopolizing Digital Advertising Technologies', available at: www.justice.gov/opa/pr/justice-department-sues-google-monopolizing-digital-advertising-technologies

US House Judiciary Committee (2020), *Investigation of Competition in Digital Markets*, available at: www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf

Commonwealth Secretariat
Marlborough House, Pall Mall
London SW1Y 5HX
United Kingdom

thecommonwealth.org

The Commonwealth

D19698