ALLIANCE FOR ETRADE DEVELOPMENT

TOWARD AN AFRICAN DATA TRANSFER REGIME TO ENABLE MSMES' CROSS-BORDER ECOMMERCE

September 30, 2021

This document is made possible by the generous support of the American People through the United States Agency for International Development (USAID). The contents are the responsibility of Palladium and do not necessarily reflect the views of USAID or the United States Government.

ALLIANCE FOR ETRADE DEVELOPMENT

TOWARD AN AFRICAN DATA TRANSFER REGIME TO ENABLE MSMES' CROSS-BORDER ECOMMERCE

Agreement No:

7200AA19CA00021

Submitted to:

USAID Center for Economics and Market Development

Prepared by:

Kati Suominen and Erica Vambell, Nextrade Group

TABLE OF CONTENTS

ACKNOWLEDGMENTS

This report was produced for the Alliance for eTrade Development, a Global Development Alliance supported by the US Agency for International Development. Suominen is the Alliance's Technical Director. The authors would like to thank Resonance staff for support on selected case studies, and all participants in the African Union Commission-Alliance for eTrade Development Digital Trade Dialogue on September 22, 2021, for their many contributions and insights.

EXECUTIVE SUMMARY

African businesses are increasingly using ecommerce to sell their goods and services and access vendors online, including across borders. In the process, they benefit from access to and the analysis of data on their customers, transactions, competitors, and markets to improve their marketing, offerings, and operations, identify high-potential customers and best-selling product categories, and anticipate demand spikes and competitors' moves.

Players in the ecosystem that support African online sellers—ecommerce marketplaces, social networks, and providers of logistics, financial, payment, and other digital services—also leverage data to improve their customer service and scale their operations. Logistics companies need massive data to optimize routes, consolidate cargo, and improve their operations to save costs for their customers; banks and fintechs need access to client firms' corporate vitals and transactional data to underwrite loans; payment companies need global transactional data sets to be able to predict and preempt payment fraud; and marketplaces and digital service providers need data to support online sellers to adjust prices, identify keywords, orchestrate and optimize fulfillment, aggregate information on their competitors' prices and products, and so on.

Firms' access to data and data analytics capabilities is critical for the development of Africa's ecommerce sector. It is also important for the digital transformation of traditional companies in Africa's construction, healthcare, manufacturing, mining, farming, and multiple other sectors. Companies in these sectors increasingly access, leverage, and process data from their business units, customers, and supply chains to optimize their operations and services, streamline their workflows, and increase their productivity. Data is also increasingly ubiquitous, available, and analyzable: cloud computing has democratized firms' ability to store and gain insights from their data, and even small companies can leverage data today by renting pay-per-use data services from hyperscale cloud providers instead of having to buy expensive hardware and software and hire in-house data analysts.

Firms' use of data has grown in parallel with discussions in Africa and around the world on appropriate data privacy and transfer policies, especially to govern individuals' data. For example, in the past few years, numerous countries, including many in Africa, have created data privacy and transfer laws that oblige companies to ensure that data subjects have consented to the collection and transfer of their data. Much like their counterparts in other parts of the world, African governments are also discussing cross-border data transfer rules in the context of the African Continental Free Trade Agreement (AfCFTA). Six African countries (Benin, Burkina Faso, Cameroon, Côte d'Ivoire, Kenya, and Nigeria) also form part of the World Trade Organization (WTO) Joint Statement Initiative (JSI) on Electronic Commerce, which aims at a plurilateral agreement on ecommerce covering multiple digital economy issues, including cross-border data transfer.

These ongoing national, regional, and multilateral processes are highly consequential. The data regimes that African countries establish today will have far-reaching implications for African firms that engage in ecommerce. They will also affect the productivity and trade of firms in many other sectors and the attainment of a dynamic, trade-creating AfCFTA. The empirical evidence on such demanding data privacy and transfer regimes as the European Union's General Data Protection Regulation (GDPR) suggests that data privacy regimes can entail significant new challenges both for the governments responsible for enforcing them and firms that must implement them, especially when these are micro, small, and medium-sized enterprises (MSMEs). In addition, there is resounding evidence that limiting firms' access to data and the ability to move data across borders comes at a significant economic cost to the imposing country, dampening firms' growth, trade and ecommerce, economic growth and productivity, and inbound investment. There is also evidence, including in Africa, that the global checkerboard of divergent

national data privacy regimes poses particular challenges to small multimarket online sellers and exporters that now have to deal with several, if not dozens, of distinct data privacy regimes when seeking to grow and diversify their exports.

At the same time, many countries and regional groupings—especially ones in the Asia-Pacific and the Americas—are experimenting with regional data transfer regimes that help balance the aspirations for vibrant digital ecosystems, MSME cross-border ecommerce, and data privacy and cybersecurity. These regimes may also be useful in Africa. As African governments and other stakeholders consider regional data transfer rules to promote the AfCFTA, they can learn from these and other experiences.

The purpose of this report is to contribute to the growing discussions on cross-border data transfer policies in Africa and discuss regional data transfer policies that are compatible with the aims of free trade and MSME cross-border ecommerce. In particular, this report (1) explores indicative survey data on 390 African firms and case studies on how African firms are storing, using, and moving data, including across borders; (2) assesses how African governments are regulating data privacy and transfer and how firms perceive the emerging data privacy and transfer rules; and (3) discusses various regional data transfer models that African economies may consider to balance their aspirations for data privacy, cybersecurity, and economic competitiveness. There are seven conclusions:

- African firms already access and use data from individuals, businesses, and their own operations. Exporters and online sellers in particular tend to use data from abroad and send data to foreign markets as part of their daily operations. Cross-border transfer of data is common across different types of firms, including firms that sell in-person services and physical products, and firms that sell digital goods or services. Firms that use data and cloud computing services to store and analyze data report significant productivity gains, cost savings, and innovations in terms of new products and services.

- Compared to their counterparts in other parts of the world, African countries are at relatively early stages in regulating data privacy and transfer. In our mapping of data transfer regimes in 54 African countries, we found that 28 countries have a data privacy and transfer law in place, and at least 7 countries are drafting data privacy laws. Countries that have data transfer rules in place vary in their requirements: some allow data to be transferred when the data subject has consented to the transfer, while many others require the receiving country to have data privacy protection mechanisms that are comparable to or sturdier than those of the sending country. Enforcement of these laws has commenced but is still incipient in most countries.

- African firms have mixed views about their respective countries' data privacy and transfer laws. Overall, micro and small firms in the countries we surveyed (Egypt, Kenya, and South Africa) are still relatively unaware of their countries' data privacy laws and how these might apply to them, whereas midsize and large firms are more informed and already implementing laws. Firms generally feel that their countries' data privacy laws are helping to cement consumers' trust in online transactions and enabling companies themselves to learn to treat consumer data appropriately. However, over a quarter of firms that know about the new laws also view them as costly and/or complicated to implement.

- African firms also appear to be concerned about the implications that the proliferation of data privacy laws in Africa and beyond may have for their ability to sell online to foreign customers. Online sellers that export particularly report that proliferating data privacy rules represent a major obstacle for them to grow their export sales— probably in part because foreign rules can be hard to keep up with and decipher, and in part because multimarket sellers struggle

particularly to deal with the many disparate national data privacy regimes. Our other surveys of African firms suggest that African online sellers are also concerned about the specter of data localization mandates.

- Granted, African governments have also pursued various regional efforts to guide the development of national data privacy laws over the past decade, such as the African Union Convention on Cyber Security and Personal Data Protection (which was completed in 2014 but has yet to take effect), the Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection of 2010, and the South African Development Community (SADC) Model Law on Data Protection of 2013. Although useful, these steps have had a limited impact on national policymaking and only address cross-border data transfer tangentially.

- The current situation points to a two-pronged policy agenda for Africa—one, to ensure that national data privacy laws are more compatible with each other, and two, to enable African firms, particularly online sellers, to use and move data across borders safely and with ease. The policy and technology solutions to consider include the following:

  – Countries in many other regions have wrestled with data policy issues and challenges that are similar to those facing African countries today, and have done so in a similar context, with countries adopting data privacy laws at different speeds and where the national laws that are being adopted differ somewhat or significantly from each other. There exist useful regional data transfer models that balance the objectives of free transfer of data across borders, data privacy, and the ability for countries to maintain their national data privacy laws. Some leading examples include the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system and two free trade agreements with robust digital trade chapters, the 11-country 2018 Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the 2020 United States-Mexico-Canada Agreement (USMCA), which endorsed the CBPR system. Our survey suggests that African companies would be strongly in favor of African governments adopting the kinds of data privacy and transfer rules included in these agreements.

  – Policy is not the only solution for enabling safe, secure cross-border data transfers. Technologies that secure data at rest, in transit, and in use are developing rapidly. Emerging solutions such as encryption and confidential computing can significantly aid African firms that leverage data and transfer data to third parties and across borders—thus preempting onerous regulations and costly enforcement. In the next decade, these and other privacy-preserving technologies are bound to become much more prevalent. Our survey suggests that the majority of African companies are concerned about the security of personal data that they transfer to third parties and are keenly interested in technology solutions to help them safeguard data. In the coming years, African companies could be empowered to adopt and use these emerging technology solutions to maximize the opportunities that data offers for their growth and development, while minimizing the likelihood of data breaches and the misuse of data by third parties.

- There is likely also an important role for technical assistance to accelerate the development and implementation of emerging data privacy and transfer laws in various African countries, and to support the development of a regional framework for data transfer. However, support should be provided to countries with regimes that are compatible with the aims of free trade and MSME cross-border ecommerce.

I. INTRODUCTION

African businesses are increasingly using ecommerce to sell their goods and services and access vendors online, including across borders. In the process, they benefit from access to and the analysis of data on their customers, transactions, competitors, and markets, to improve their marketing, offerings, and operations, identify high-potential customers and bestselling product categories, and anticipate demand spikes and competitors' moves. Players in the ecosystem that support African online sellers—ecommerce marketplaces, social networks, and providers of logistics, financial, payment, and digital services—also leverage data to improve their customer service and scale their operations. Logistics companies need massive data to optimize routes, consolidate cargo, and improve their operations to save costs for their customers; banks and fintechs need access to client firms' corporate vitals and transactional data to underwrite loans; payment companies need global transactional data sets to predict and preempt payment fraud; and marketplaces and digital service providers need data to support online sellers to adjust prices, target keywords, orchestrate and optimize fulfillment, aggregate information on their competitors' prices and products, and so on.

Firms' use of data has grown in parallel with discussions in Africa and around the world about appropriate data privacy and transfer policies, especially to govern individuals' data. Over the past few years, numerous countries, including many in Africa, have created data privacy and transfer laws that oblige companies to ensure, for example, that data subjects have consented to the collection and transfer of their data. Much like their counterparts in other parts of the world, African governments are also discussing cross-border data transfer rules in the context of the African Continental Free Trade Agreement (AfCFTA). Six African countries (Benin, Burkina Faso, Cameroon, Côte d'Ivoire, Kenya, and Nigeria) also form part of the World Trade Organization (WTO) Joint Statement Initiative (JSI) on Electronic Commerce, which aims at a plurilateral agreement on ecommerce covering multiple digital economy issues, including cross-border data transfers.

The data regimes that African countries establish today will have far-reaching implications for African firms that engage in ecommerce. They will also affect the productivity and trade of firms in many other sectors and the attainment of a dynamic, trade-creating AfCFTA. The empirical evidence on such demanding data privacy and transfer regimes as the EU's GDPR suggests that data privacy regimes can entail significant new challenges both for the governments responsible for enforcing them and the firms that must implement them, especially when these are MSMEs. In addition, there is resounding evidence that limiting firms' access to data and ability to move data across borders comes at a significant economic cost to the imposing country itself, dampening firms' growth, trade and ecommerce, economic growth, and productivity, and inbound investment.

At the same time, many countries and regional groupings—especially ones in the Asia-Pacific and the Americas—are experimenting with regional data transfer regimes that help balance the aspirations for vibrant digital ecosystems, MSME cross-border ecommerce, and data privacy and cybersecurity. These regimes may also be useful in Africa. As African governments and other stakeholders consider regional data transfer rules to promote the AfCFTA, they can learn from these and other experiences.

The purpose of this report is to contribute to the growing discussions on cross-border data transfer policies in Africa and discuss regional data transfer policies that are compatible with the aims of continental free trade and MSME cross-border ecommerce. In particular, this report (1) explores indicative survey data on 390 African firms and case studies on how African firms are storing, using, and moving data, including across borders; (2) assesses how African governments are regulating data privacy and transfer and how firms perceive the emerging data privacy and transfer rules; and (3) discusses

various regional data transfer models that African economies may consider to balance their aspirations for data privacy, cybersecurity, and economic competitiveness.

The following section reviews how African companies use data, based on survey data and case study interviews. Section three reviews the evolution of data privacy regimes around the world and the state of play of African countries' adoption and enforcement of data privacy and transfer laws, and African firms' views of these laws. Section four discusses various regional data transfer regimes that have successfully been built in contexts similar to one in which African countries find themselves today—the rapid growth of firms' use of ecommerce and cross-border data, and the multispeed adoption of diverse national data privacy and transfer regimes. Section five concludes.

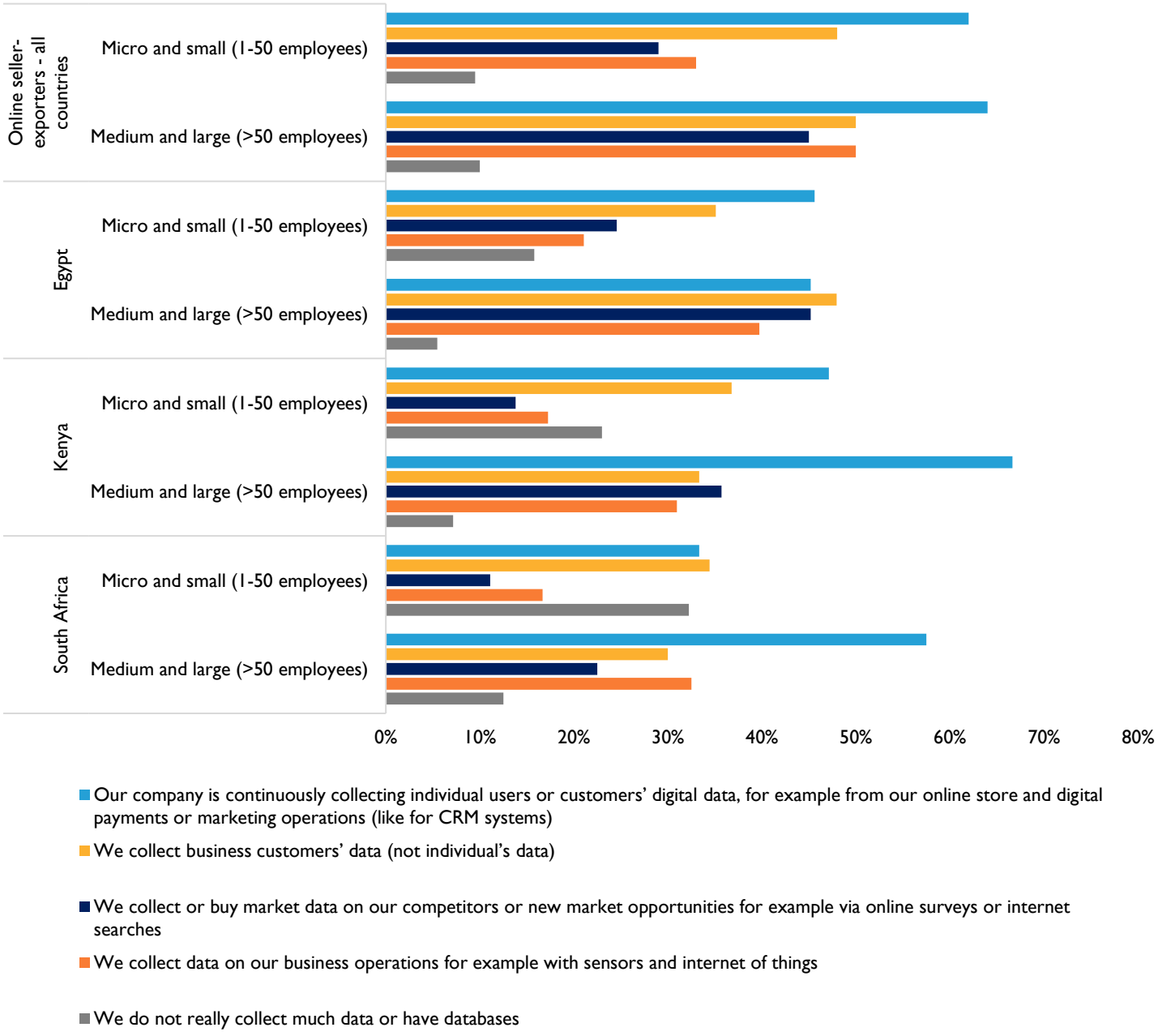
II. HOW DO AFRICAN COMPANIES ACCESS, USE, AND SECURE DATA—AND BENEFIT FROM IT?

The global datasphere is growing exponentially each year. According to estimates, the amount of data created in the next three years alone will be greater than that generated over the past 30.[1] Likewise, there will be three times more data in the next five years than in the past five.

This exponential growth comes from many sources. One is firms' and governments' growing use of devices, sensors, and the Internet of Things (IoT) to access data from factories, cars, planes, machines, highways, cities, and countless other places. Another source of data is consumers' and firms' use of social media, apps, videos, music, and countless online services—and the rise of "born digital" companies such as fintechs, streaming services, and ecommerce marketplaces that access this data to offer and optimize their services.[2] Yet another driver for the growth of the global datasphere is the growing adoption of cloud computing and machine learning capabilities that essentially enable organizations to recycle existing data and extract new insights and value from it. Indeed, the amount of data that is being copied, processed, and analyzed is growing much faster than data that is newly created.[3]

African firms of all sizes also collect, store, use, and move data. Our survey of 390 firms from Egypt, Kenya, and South Africa suggests that nearly half of even MSMEs in these countries continually collect data on individual customers, and a third collect data on business customers (figure 1). Midsize and large firms in some of Africa's largest sectors—agriculture, manufacturing, transportation, and healthcare—tap data from their business operations, leveraging IoT, which can generate significant macroeconomic gains.

Figure 1: African firms' collection of different types of data, by firm size and country



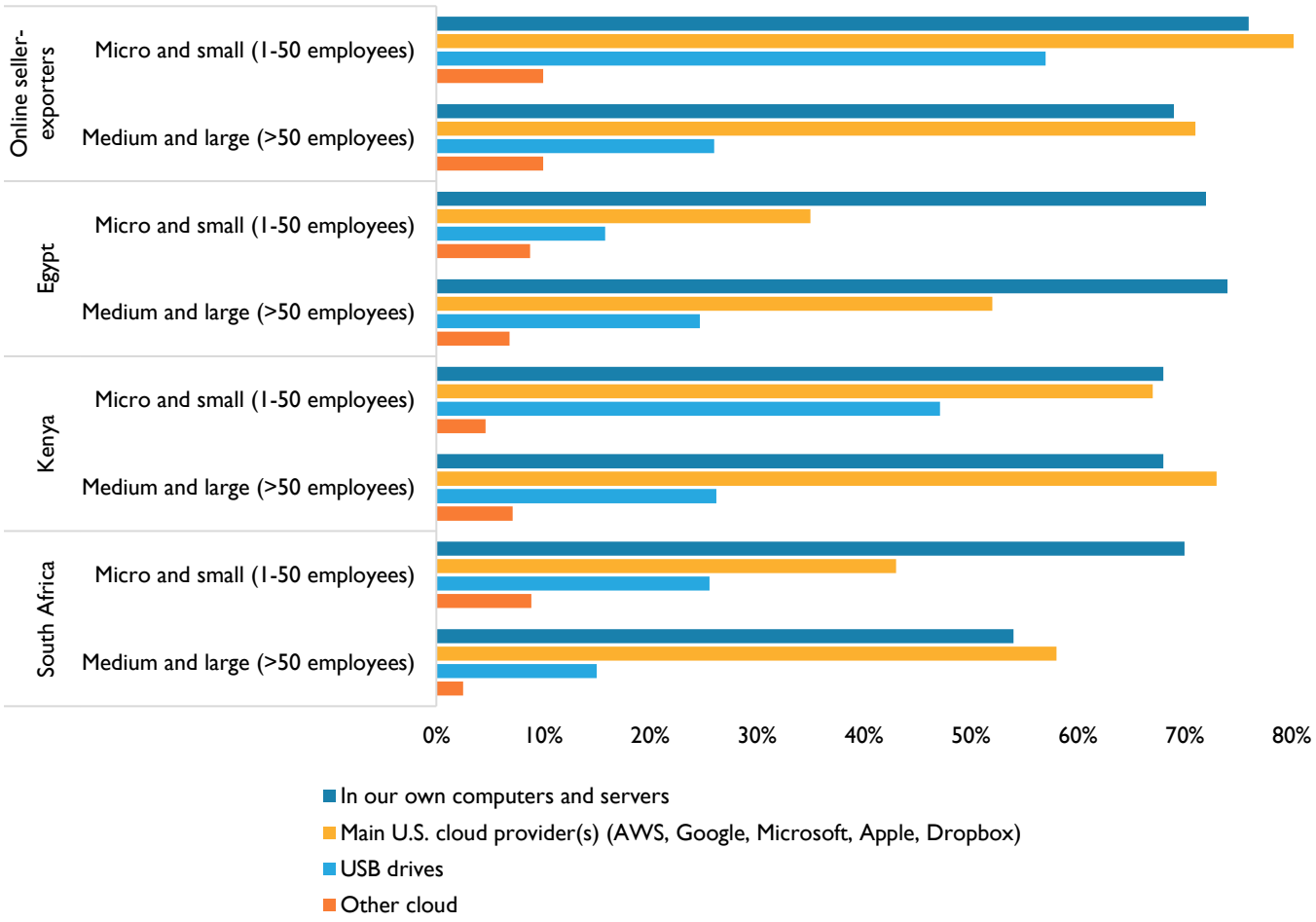
African firms and exporters in particular leverage data and move data across borders (table 1). Firms that sell online and export are particularly data-intensive, suggesting that firms use data to grow their cross-border ecommerce sales. Cross-border data transfers are common across different types of exporters, including firms that sell in-person services and physical products, and firms that sell digital goods or services.

Table 1: Share of firms that transfer data across borders, by type of company and export orientation

			To our foreign affiliates	From our foreign affiliates to us	From online platforms to us	From individuals other countries to us	From foreign companies to us	From foreign governments to us	No data moved across borders
Online seller-exporters	All sectors	Micro and small	38%	33%	52%	19%	38%	5%	14%
	All sectors	Medium and large	50%	6%	62%	38%	45%	19%	2%
Exporters	In-person services	Micro and small	44%	31%	28%	28%	25%	6%	13%
		Medium and large	46%	49%	52%	48%	28%	15%	7%
	Physical products	Micro and small	32%	29%	45%	32%	18%	3%	24%
		Medium and large	48%	54%	48%	46%	29%	13%	10%
	Remote digital services	Micro and small	47%	26%	53%	47%	11%	0%	11%
		Medium and large	48%	50%	50%	54%	27%	17%	6%
	Digital products	Micro and small	28%	17%	59%	38%	14%	10%	14%
		Medium and large	49%	60%	49%	51%	29%	23%	3%
Non-Exporters	In-person services	Micro and small	13%	19%	29%	8%	1%	0%	40%
		Medium and large	15%	20%	15%	0%	0%	0%	55%
	Physical products	Micro and small	6%	8%	31%	16%	6%	0%	50%
		Medium and large	35%	41%	29%	24%	6%	0%	29%
	Remote digital services	Micro and small	18%	21%	33%	9%	6%	0%	36%
		Medium and large	0%	17%	17%	0%	17%	17%	50%
	Digital products	Micro and small	13%	30%	57%	17%	9%	0%	22%
		Medium and large	11%	22%	33%	22%	11%	0%	56%

Most surveyed African firms store this data on their premises in servers and computers; larger firms and online sellers especially tend to use cloud providers for storing data (figure 2). Storing data with hyperscale cloud providers may also imply cross-border transfers to a server located in another jurisdiction.

Figure 2: African firms' data storage, by firm size and country



There is significant case-study evidence on how firms in Africa's ecommerce ecosystem and beyond are benefiting from access to data and cloud capabilities. For example, firms use data to:

- **Scale and accelerate service provision.** Businesses can store, share, secure, process, and analyze data at a much greater scale and speed than was the case in the past, using cloud computing, virtual infrastructures, and machine learning. As one example, Nigerian small business lender OneFi, which also lends to online sellers engaging in ecommerce, leverages data on borrower candidates and utilizes AWS machine learning technology to make lending decisions by quickly analyzing terabytes of data to determine customers' likelihood of repaying a loan. This has tripled OneFi's lending volumes to 1,500 loans a day.[4] Similarly, South African company Simfy Africa, which streams music for mobile subscribers across Africa, turned to cloud computing to store artist and album images, thus scaling its services while cutting costs by 27 percent as compared to a self-managed solution.

- **Improve customer experience and engagement.** African businesses also use data to create new value for their customers and engage their users. For example, Morin-O—a woman-owned decor and gifts company in Lagos, Nigeria, that sells and exports online—has turned to Google

Analytics to better understand its customer base, develop valuable content that speaks to its customers, and analyze data on customer usage of its site to optimize marketing campaigns and product positioning.[5] In South Africa, insurance company Discovery uses data on its customers' physical activity, shopping, eating, and road safety habits to reward customers for healthy living.[6] In Kenya, agtech company SunCulture collects soil sensor and weather data to provide farmers with customized tips through their mobile phones, such as to suggest they irrigate for an extra three minutes on an especially hot day, or change the position of a solar panel to capture more energy.[7]

- **Manage risk and prevent fraud.** Global payment providers that also service African consumers and businesses in their online transactions use massive data to secure online sellers' data and prevent payments fraud. For example, Visa Advanced Authorization risk-scoring considers 500 attributes in one millisecond and covered 127 billion transactions in 2019 alone. By accessing its vast global data set and machine learning capabilities, Visa prevented $25 billion in fraud in 2019.[8] Fraud remains near historic lows, at less than six cents per $100 transacted, despite huge increases in network volume.[9] Again, data is what enables this success: payment providers cannot address risk by looking at a single transaction in a single place; they need to see hundreds of millions of transactions to detect anomalous patterns and predict and preempt fraud.

- **Reduce cost and enhance productivity.** When they build up significant quantities of data, ecommerce companies benefit from cloud applications to manage and analyze this at scale, gain new flexibilities, and save on costs. For example, Nigeria's ecommerce marketplace Konga turned to Google Cloud after struggling to maintain high volumes of concurrent users on the site in a cost-effective manner, thus reducing its monthly cloud infrastructure costs from $85,000 to $30,000.[10] South African travel booking website Travelstart, which is essentially a B2C ecommerce services platform, centralized its online booking operations and data for central Africa and the Middle East on AWS, reducing costs by 43 percent and downtime by 25 percent.[11] In financial services, South Africa's Standard Bank consolidated its national data siloes into a one-stop cloud-based center of excellence to seamlessly support more than 20,000 users across the continent, standardizing analytics across its different operations.[12]

- **Innovate new products and services and propel interoperating ecosystems.** Open APIs are the key connectors that enable software to speak to other software and thus allow ecommerce ecosystems to work. APIs also accelerate innovation: instead of having to construct an entire value chain or negotiate connections one by one, parties can plug into existing APIs and join an ecosystem where they can share data and information with all other parties. One example is payment giant M-Pesa, which has used cloud computing to open APIs for its partner developers. As a consequence, it has onboarded over 15,000 developers into the company's sandbox environment and opened up the M-Pesa ecosystem to 4,500 partners, from startups to large enterprises.[13]

Table 2 summarizes how various African companies use data and what they gain from analyzing it; Case 1 discusses the use of data by Ethiopia's Hibret Bank.

Table 2: Data access and analysis use cases, selected African companies

Company	Country	Service	Challenge	Use case	Impacts
OneFi	Nigeria	Micropersonal loans across Africa	Excessive paperwork and manual processes: to get approval for a loan, a customer had to visit a regional office, fill out a paper form, and wait for employees to physically validate their addresses and identity information.	Launch Paylater app to enable customers to apply for and receive loans online and to fully automate and scale loan processing.	• 1,500 loans disbursed a day instead of 500 a week • Loan authorization times reduced from 2 weeks to 2 minutes • Applicants' ID verified through machine learning rather than physical checks
Konga	Nigeria	Ecommerce marketplace in Nigeria and West Africa	Struggled to maintain high volumes of concurrent users on the site in a cost-effective manner that would enable 180,000 users to connect with over 10,000 vendors.	Scale up quickly to service new traffic and reduce costs when traffic is at a low state.	• Server response times increased between 5% and 400% • Monthly cloud infrastructure costs reduced from $85,000 to $30,000 • IT maintenance and management burden reduced
Morin'O	Nigeria	Online seller of handbags and gifts	Realized early that it needed to learn customers' preferences and cultures and manage a compelling marketing and digital strategy.	Use Google Analytics to understand and segment customer base, develop valuable content that speaks to customers, and analyze data on customer use of site.	• Marketing campaigns and product positioning optimized for key export markets
Cellulant	Nigeria	Digital payments for African companies	Local data centers were incapable of handling payments among mobile subscribers and businesses.	Leverage hyperscale cloud platform to scale service to mobile subscribers and accelerate innovation and experimentation.	• Short feedback cycle • Communication with developers facilitated and accelerated • Regulatory compliance facilitated
Travelstart	South Africa	Travel booking website	Previous cloud provider was unreliable, inefficient, and not ready to help the company scale into new markets.	Use a new cloud provider to expand into new markets, benefiting from cost-efficiency, scalability, depth of portfolio, and especially its flexibility to accommodate different website traffic rates.	• Operational costs reduced by 43% per market • Server downtime cut by 25% • Scale with ease and handle traffic fluctuations
LifeQ	South Africa	Technology that powers wearables such as smart watches and fitness trackers	To attract new business, LifeQ needed data infrastructure that would scale responsively when demand increased, but that was also reliable, secure, and allowed the team to get ideas to market fast.	Use AWS platform to handle millions of users, each of whom generates about 9 gigabytes of data a year, and process data quickly to adhere to service-level agreements.	• LifeQ Cloud implemented in half the time it would have taken for internal infrastructure • Easy and fast to keep up with health industry compliance • Platform can handle fast user growth, millions of users

Standard Bank	South Africa	Financial services	Previously used legacy applications for key business processes, with different countries using different applications. Most analytics use siloed data sources that central IT teams lack insight into, making it difficult to make broad, strategic changes in the data domain.	Establish a center of excellence for Power BI users across the company, enabling users to work with the data needed while providing support and guidance. Microsoft Teams and Power Apps help with collaboration and task automation.	• Significant per-worker productivity gains: a team of merely 11 supports more than 20,000 users across the continent • More standardized applications and analytics are being delivered
SunCulture	Kenya	Agriculture	SunCulture identified access to water as the biggest challenge to farmers in a nation facing food shortages, and where farmers struggle to grow sustainable, profitable crops.	Collect data from sensors on solar-powered pumps and analyze them with Microsoft Azure; make recommendations to farmers by texts, calls, and alerts.	• Farmers provided with water to irrigate up to two acres • Up to 17 hours saved per farmer per week that was previously spent moving water manually • Reduced costs
Safaricom (M-Pesa)	Kenya	Mobile payments	Integrating partners to M-Pesa mobile wallet via APIs was slow due to the arcane process of creating separate network connections and manual requesting that developers perform testing.	Utilize cloud platform to securely expose APIs and improve platform configurability, necessary error handling, and logs.	• APIs developed and deployed from start to finish in just a few hours • M-Pesa ecosystem opened to 4,500+ partners, from startups to large enterprises • API developed and published within a week • 15,000 developers onboarded into company's sandbox environment

Case 1: Data Use Case Study: Hibret Bank

Hibret Bank was established in 1998 as the fifth private bank in operation in Ethiopia. With its headquarters located in the Ethiopian capital of Addis Ababa, the Bank has expanded rapidly throughout the country and now operates over 385 branches and employs over 4,700 employees. All banking branches are connected to the headquarters' data center through a direct connection VPN, or virtual private network, and all transactions are captured through the Oracle FLEXCUBE core banking platform. Types of data that Hibret Bank collects and stores include customer information (e.g., customer identification, credit history, account and balance information), financial transaction information (e.g., withdrawals and deposits, import and export balances), and operations data (e.g., name of the agent who facilitated the transaction, timestamps on transactions, other metadata).

From the raw data, the Oracle FLEXCUBE platform creates dynamic business intelligence reports that enable decision-making based on the data. More than 200 reports are generated for each business unit to capture key metrics and ensure strong health for the business. For example, within the lending business unit there are reports generated for asset quality and repayment schedules, and for retail banking, reports are generated for balance and transaction history. Furthermore, internal auditors use data to protect the system against fraud by setting up internal controls to flag or freeze a suspicious looking account. For example, because most fraud happens on dormant accounts (accounts that have not seen a transaction for over 6 months), the internal auditor will receive an automatically generated notice any time a dormant account becomes active again.

Hibret Bank also captures and uses data when transacting with other institutions. For example, Hibret Bank has a partnership with Ethiopian Airlines to offer ticket sales or a co-branded credit card to customers, both of which require the transfer of data between the two companies. The Bank has also interfaced with Ethio telecom, Ethiopia's government-owned telecommunications provider, for its pre- and post-paid mobile top up offering as well as its recently launched TeleBirr agency banking service. Hibret Bank operates through the SWIFT system when transacting with other financial institutions located outside of Ethiopia.

All of Hibret Bank's data for core banking is housed on the premises of its headquarters in Addis Ababa in a state-of-the-art data center and secured by a closed-circuit video surveillance system and around the clock security staff. Physical data security is considered very important for the business and a similar on-premises data storage system is the norm in Ethiopia's banking sector. Hibret Bank prides itself on being more secure than most as it is the first and only bank in the country that has secured the ISO/IEC 27001 certification for meeting international security standards for information security management.

A major reason for applying for this certification was to signal to customers and governments alike that Hibret Bank takes data security seriously.

Data is housed locally rather than on a remote cloud server for two main reasons. First, internet connectivity is not always consistent in Ethiopia as outages can occur in Addis Ababa and throughout the country, so the Bank's branches connect to the central system through a direct connection VPN, rather than through VPN over the internet, to ensure consistent connection. The Bank is hesitant to move to storing data on a remote cloud server as they have determined that switching to cloud services for data storage would require a 99.9% active internet connection, which is not currently realistic. Second, even though there is no written directive about where to store financial data, Ethiopia's central bank discourages the use of a foreign-owned cloud-based service to store customer data, as it is perceived as creating a dependency on a foreign entity, and therefore strongly encourages the use of local on-premises servers for data storage.

While Ethiopia does not have a general data protection law or data protection authority, digital strategies and protection are mostly managed by the individual sector governing bodies or authorities. In July 2021, Ethiopia's central bank launched its first national digital strategy, marking an acceptance and championing of a

new way of conducting business. The ambitious strategy laid out a four-pronged plan to transform the payment ecosystem by 1) modernizing and expanding the country's digital payments infrastructure, 2) championing the adoption of digital payments, intentionally inclusive of financially excluded segments, 3) building a robust and consistent regulatory and oversight framework, and 4) creating an enabling environment for innovation.

Ethiopia's central bank recently restricted the amount of funds that could be withdrawn daily, currently set at 50,000 Ethiopian Birr or just over $1,000 USD for an individual customer. Hibret Bank's CEO Melaku Kebede, sees the enforcement of this directive as an important measure to lower the risk of a bank run as well as to promote the ease of digital banking in Ethiopia (e.g., not needing to be physically present at a bank to do business). In his view, the current government listens to requests from the private sector related to improving the digital economy. For example, the Governor of Ethiopia's central bank convenes all Ethiopian bank presidents on a regular basis to discuss feedback on policies. Mr. Kebede sees this open line of communication as resulting in strengthened government policies, as well as an opportunity for banks and financial technology companies to learn from one another by discussing their own digital transition.

Looking to the future, Mr. Kebede looks to harness the full value of the data the Bank is collecting, such as to utilize business intelligence for predictive analytics on customer behaviors. With these data analysis tools, the Bank will be able to proactively package and market particular products to customers as they need them. Prior to a shift in data storage on the cloud, Mr. Kebede foresees a period where data will need to be replicated and stored on both local and cloud servers to build confidence in a cloud-based system by both policy makers and consumers alike.

E-Trade Alliance Case Study. Author: Clayton, Emily. Data Use by Hibret Bank. USAID Digital Economy and Market Development Project. September 2021.

III. AFRICAN COUNTRIES' ADOPTION OF DATA PRIVACY AND TRANSFER RULES: STATE OF PLAY AND FIRMS' VIEWS

A. GROWING GLOBAL ATTENTION ON DATA PRIVACY AND TRANSFER, STRICTER LAWS, INCREASING PENALTIES

In response to firms' growing access to and use of data, especially personal information, governments around the world have adopted data privacy and transfer laws that regulate how data is being accessed, managed, and moved. There have been numerous new laws and reforms in the past three years, in particular. For example:

- Perhaps the world's best-known data privacy law is the European Union's GDPR, which took effect in May 2018. The GDPR also addresses the transfer of personal data outside Europe and has extra-territorial reach, applying to any firm that controls or processes Europeans' data. The GDPR forbids the transfer of personal data of European data subjects to countries outside of the European Economic Area (EEA) unless those third countries are deemed by the EU to have "adequate" data protection regulations.

- While there is continued discussion about a federal privacy law, in the United States it is state governments that have led the way in developing data privacy laws. The most rigorous regulation is the California Consumer Privacy Act (CCPA) that came into effect in 2020 and is being assessed and analyzed by many other states.[14] In March 2021, Virginia passed a similar data privacy law. These state laws do not address cross-border transfer, and they exempt small businesses that do not deal intensively in data on the state's residents.[15] The philosophies behind these laws are somewhat different from that behind the GDPR: while the GDPR essentially places a locked door between Europeans and businesses that might want to access their data, the CCPA provides Californians a window into how their data might be used by businesses and gives them control over this.[16]

- Several other advanced countries with established data privacy and transfer laws have recently revised their legislation. For example, the 2020 amendment to Japan's Act on the Protection of Personal Information (APPI) allows data transfer only if the data subject has consented to a transfer, or where overseas recipients are located in countries that have data protection equal to Japan, or where overseas recipients have signed contractual agreements that ensure compliance with data protection standards in Japan.[17] Canada and Singapore also tightened their privacy regimes in 2020, through more rigorous enforcement and greater penalties.[18]

- Several emerging markets, such as Colombia, Malaysia, Mexico, and the Philippines, have also put in place data privacy and transfer regimes over the past decade. Likewise, Argentina, Brazil, Indonesia, Pakistan, and Thailand, among others, passed new data privacy regimes in 2019 and 2020. Some of these are modeled after the GDPR, though typically with greater flexibilities. Brazil's 2020 Lei Geral de Proteção de Dados requires organizations to establish legal bases to process personal data, provide data breach notifications, and adhere to cross-border data transfer restrictions, including obtaining prior specific, informed consent to a transfer from the data subject unless the transfer is to countries or international organizations with an adequate level of personal data protection.[19]

- While most jurisdictions allow data transfer under certain conditions, several countries, including China and Russia, have outright localized data or made it very complicated to move. Under China's latest data privacy and transfer laws, a company seeking to transfer personal data out of China must first undergo a security assessment by the Cyberspace Administration of China (CAC) if the transfer involves a large volume of data, according to the organization's own specifications.[20] However, a company can transfer data if it has a data protection certification issued by a professional organization in line with CAC regulations or if it has an agreement with the foreign recipient requiring it to process the data as specified in the new law. Businesses are barred from providing any data stored in China to foreign law enforcement officials and courts without the Chinese government's approval.[21]

- Likewise, over the past few years, Indonesia, India, Vietnam, Nigeria, and Turkey have introduced laws to localize individuals' data entirely or in a specific sector, such as payments, financial services, or healthcare. In April 2019, the Reserve Bank of India issued one of the most restrictive data localization measures yet, requiring foreign payment companies to store all transaction data involving Indian customers on servers located within India and delete Indian citizens' data on their global servers. Granted, India, Indonesia, and Vietnam have recently relaxed some provisions of their data laws in response to criticism by businesses and trading partners.[22] However, data localization practices have been spreading—according to a recent analysis, 62 countries have imposed 144 data localization practices of some type.[23] The same study identifies China as the most restrictive economy, followed by Indonesia, Russia, and South Africa.

  Governments have justified limiting the cross-border transfer of data on many grounds, including that localization would better enable law enforcement to access data and that it will lead to the creation of new jobs in digital industries and broaden their tax base.[24] However, localization mandates are also often reported to result from lobbying by domestic or foreign companies that already have in-country data processing facilities and call for localization to raise costs for foreign rivals that process data abroad.[25] In some markets, there are concerns that data localization policies are being used to exert censorship and squash dissent.[26]

There is growing research on the impact of these laws on economic outcomes—this is particularly prolific and strong regarding the impacts of the GDPR and data localization mandates:

- Impact analyses of the GDPR suggest that it has created significant implementation costs and challenges to firms and, by limiting firms' access to and use of data, also had significant negative impacts on MSME ecommerce, firms' profit margins and growth, startup investment, and mergers and acquisitions (M&A).

- Research on data localization policies is practically unanimous: data localization mandates cost the imposing country's economy dearly in many ways. Localization mandates increase the cost of world-class digital services for local companies, limit the competitiveness of firms' exports, dampen foreign direct investment and economic growth, undermine data security and cybersecurity, and arrest the competitiveness of firms in data-intensive sectors such as ecommerce, IT and financial services, smart farming, and smart manufacturing.[27] Overall, studies show that data localization mandates have similar negative impacts on local firms as local production mandates or tariffs on intermediate goods: they raise costs for local startups and firms, undermining their competitiveness. Localization also undermines the considerable economic gains from IoT. This research is further explored in case 2.

Case 2: Summary of impacts of the GDPR and data localization policies

In May 2018, the EU began enforcing the GDPR, which essentially made it costlier for companies to access personal data and authenticate people's identities online. Some two-thirds of US businesses spent between $1 million and $10 million to implement the GDPR.[28] Collectively, Fortune 500 companies spent some $7 billion to do so, including hiring lawyers, consultants, and data protection officers.[29] Broader fears about compliance were reflected in dampened M&A activity: in July 2018, a survey of 539 M&A professionals from Europe, Africa, and the Middle East revealed that 55 percent had worked on transactions that did not go through due to concerns about companies' compliance with the GDPR.[30]

Before the GDPR came into effect, there were several forecasts of its impacts on European companies' longer-term revenues, FDI, exports, and other economic outcomes that might result from curtailed access to data. A 2013 forecast expected immediate losses of $66 billion in sales for EU companies.[31] Empirical studies on the GDPR's economic impacts are still limited in number—but in studies that have been conducted, impacts have been especially negative for European MSMEs and startups and include the following aspects:

- **For online businesses, reduced pageviews and ecommerce revenue**. A study of 1,084 diverse online firms suggests that since the GDPR was adopted, companies catering to European consumers experienced a 12 percent reduction in website pageviews (implying 15,043 fewer pageviews per week for the median site), while ecommerce sites saw their online revenue drop by 13.3 percent (or $9,227 per week for the median site). One explanation is reduced interest among users to browse sites, another is user non-consent (where consent requirements discourage users from browsing the site further), and yet another is new limits to firms' ability to market. Non-consent accounts for at least 7 percent of the recorded pageview decline and at least 29 percent of the reduced revenue estimate. The three firms that adopted the stricter consent standards sought by regulators experienced an over 50 percent cut in traffic and a 20 percent increase in bounce rates (where the user leaves after viewing a single page). Another significant negative impact is from the GDPR's impact on email and display ad marketing.

- **Narrower profit margins for European MSMEs than American counterparts.** A study comparing the performance of European and US MSMEs during the first year of GDPR implementation found that European data-intensive MSMEs' profit margins grew 1.7–3.4 percentage points less than those of their US counterparts.[32] Meanwhile, there were no differences among large firms, likely because many large US companies hold Europeans' data and thus had to comply with the GDPR as well.

- **Negative impacts on investment in technology companies**. The GDPR has dampened investments in new and emerging European technology firms versus comparable US counterparts.[33] The GDPR had an especially negative effect on foreign investments, younger ventures, and data-reliant firms, undermining the overall dollar amounts raised across funding deals, the number of deals (by 26 percent), and the dollar amount raised per individual deal (by 34 percent).

- **Changes in advertising revenue.** Different consumer segments responded differently to the GDPR. A study of consumers using travel sites found that consumers that are particularly privacy-conscious—12.5 percent of the sample—moved away from platforms that did not provide rigorous privacy protection.[34] As a result, the remaining consumers became more valuable to advertisers, with the two changes largely offsetting each other.

There have also been numerous simulations and empirical studies on data localization that point to the same conclusion: data localization mandates cost the imposing countries in terms of dampened growth, trade, investment, and more. For example, localization mandates are found to:

- **Undermine exports, FDI, and GDP growth and increase costs to local companies and consumers**. In a simulation, the European think-tank ECIPE found that localization could result in a 1.3 percent drop in EU GDP and an 11 percent drop in EU manufacturing exports to the United States. In general, data localization requirements would lower GDP growth across a diverse range of countries like Brazil, Korea, and India. In another study, CIGI and Gotham House find localization would lower GDP by 0.1 percent in Brazil, 0.6 percent in China, and 0.5 percent in the EU.[35] These results are not surprising—after all, data localization policies are much like local content requirements: they impose a tax on users of data and digital services, such as small businesses and consumers, and thus disincentivize the spread of digital technologies and services. By localizing data, governments curtail companies' and workforces' access to cutting-edge digital services and technologies, and the development of digital skills among their citizens.

- **Undermine data-intense sectors such as ecommerce, IT, and financial services, smart farming, smart manufacturing, and transportation**. In a study of five African countries, data localization was found to particularly increase costs for financial services and undermine productivity growth in manufacturing.[36] In their study, CIGI and Gotham House found that data localization would especially undermine production in sectors including manufacturing, water, communications services, and financial services.[37] Indeed, limits to cross-border data flows are widely found to particularly limit trade in services.[38]

- **Discriminate against foreign providers.** Data localization policies can shield uncompetitive local companies from foreign competitors. As such, they are much like discriminatory trade barriers. One simulation found that the EU's data privacy and residency policies have a discriminatory impact on Korean companies.[39] Another simulation found that while free cross-border data flows enable intense competition among producers, data localization restrictions force a certain clustering of consumers around local firms, and limit consumer choice due to its effect on the price and quality of services.[40] In a survey, the US International Trade Commission identified foreign data localization requirements as a barrier to 52 percent of US small- and medium-sized enterprises in the digital communications sector.[41]

- **Backfire in limiting domestic firms' expansion into new markets.** NASSCOM, a trade association for the Indian information technology and business process outsourcing industry, has raised concerns about other countries' data regulations as possible discriminatory barriers to Indian companies expanding into new markets.[42] Indeed, paradoxically, firms in countries that have promoted data localization and "data sovereignty," such as India and Indonesia, may face the same discriminatory data localization policies their own countries are championing today when they grow and internationalize. In light of these findings, it is hardly surprising that most business leaders and economists oppose data localization. For example, in India, the Centre for Internet and Society finds that 90 percent of Indian think-tanks and associations oppose data localization policies.[43]

- **Conflict with crucial policy objectives.** Data localization requirements increasingly conflict with public policy goals to enable data transfer for development, health, or public safety purposes. For example, data localization rules directly conflict with requirements around anti-money laundering and combating the financing of terrorism (AML/CFT) around international remittances, making it impossible for providers to comply with both regulatory frameworks.[44] Initiatives that seek to share data on a blockchain across public and private sectors across borders—say, health data to respond to the spread of COVID-19—are also increasingly worried about conflict with data privacy and transfer rules.

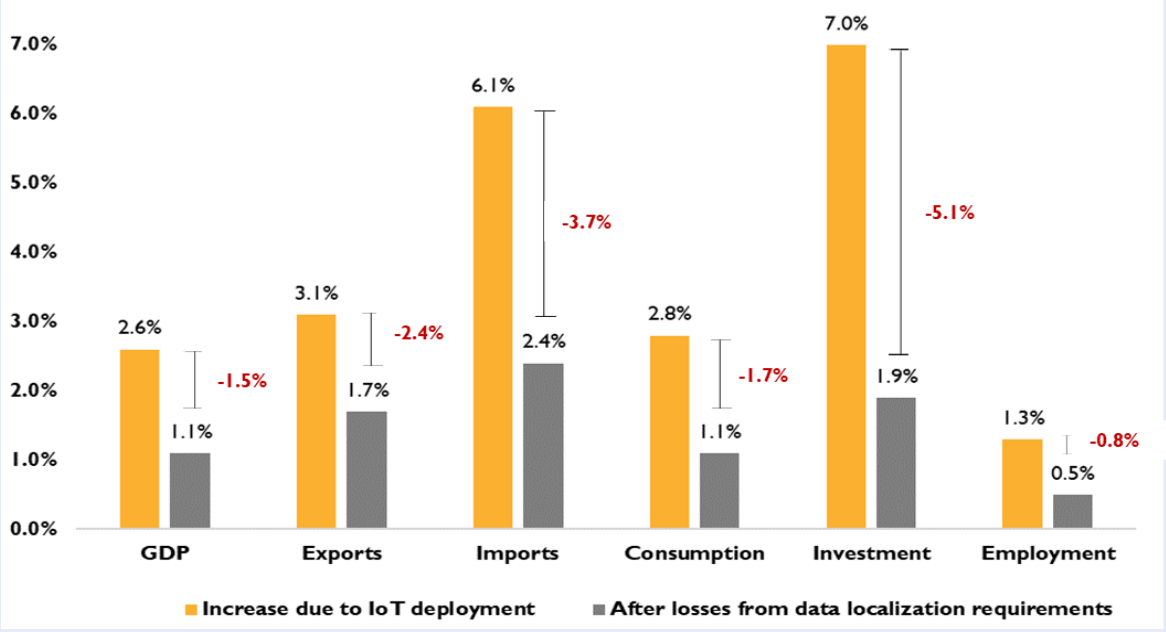
- **Create new cybersecurity vulnerabilities.** Data security has little to do with *where* data is stored but everything to do with *how* data is stored and governed. The negative impacts of data

localization on data security are arguably especially grave if a country lacks the underpinnings to manage and secure data, such as low political risk, excellent IT networks and facilities, strong cybersecurity protection, and so on. Data localization mandates also create data security challenges, as data will now have to be stored and secured locally and anomalous and fraudulent patterns cannot be as easily identified as in global data sets.

- **Undermine gains from 5G, IoT, artificial intelligence (AI), and blockchain.** 5G connections and AI, machine learning, IoT, and blockchain are improving companies' operations across countless industries, from manufacturing to mining. The usefulness of these technologies revolves largely around data. For example, in smart farming, data collected through smart devices, IoT-enabled sensors, and even satellites is transmitted instantaneously and analyzed through sophisticated cloud computing services, to offer farmers real-time capabilities to improve their productivity. Data localization policies raise the costs of such productivity-enhancing services. Countries that limit data flows will also limit data-driven improvements in public services such as medical services or emergency responses.

Indeed, data localization requirements could raise operating costs significantly, as firms have to make internal adjustments based on how to collect, store, process, and transfer data, raising costs. A recent GSMA study found that South Africa's GDP would grow by 2.6 percent and investment by 7 percent due to IoT deployment, but that data localization would undermine these gains, shrinking GDP growth from IoT to 1.1 percent and investment gains to a mere 1.9 percent. Trade, consumption, and employment gains would also shrink (figure 1-1). [45]

Figure 1-1: Contribution of IoT deployment in South Africa[46]



Note: The yellow bars represent increases compared to a baseline where IoT deployment is not expanded; the gray bars show increases after expanded deployment in the presence of data localization policies.

B. EVOLVING DATA PRIVACY AND TRANSFER LAWS IN AFRICA

What, then, is the state of play in data transfer rules in Africa? Compared to their counterparts in other parts of the world, most African countries are at relatively early stages in regulating data privacy and transfer. In our mapping of data transfer regimes in 54 African countries, we found that 26 countries do not yet have a data privacy and transfer regime in place, although a third of them, including Namibia, Rwanda, Mauritania, and Zimbabwe, are working on data privacy laws.

The 28 countries that have adopted data privacy and transfer laws do allow the cross-border transfer of data. However, in most cases, transferring organizations need to adhere to one or some combination of requirements to transfer data, such as to (a) ensure, as with the GDPR, that the country receiving the data has an "adequate" data protection regime; (b) obtain users' (or "data subjects'") consent for the transfer of the data; (c) qualify for an exception, as is the case when the data transfer is necessary for contract execution; and/or (d) notify national authorities of the transfer. Sensitive data can have specific protections. For example, and to simplify somewhat, Uganda requires the firm that transfers data to obtain user consent for the transfer or ensure adequate protection is in place; 17 countries including Botswana, Morocco, and Nigeria require either user consent, adequate protection, or an exception such as transfer for the use of a contract or in the interest of the public; and Burkina Faso, Guinea, Mali, Niger, Egypt, Kenya, Tunisia, and Zambia require adequacy and authorization from the data protection authority (DPA) or a DPA license (table 3 and appendix I).

African countries that require other regions or countries to have "adequate" data protection regimes as a pre-condition for data transfer have diverse lists of which countries these are. For example, Côte d'Ivoire recognizes the member states of ECOWAS as adequate; Chad recognizes those of the Central African Economic and Monetary Community (CEMAC) and the Economic Community of Central African States (CEEAC) members; Lesotho recognizes member states that have transposed the SADC data protection requirements; and Morocco recognizes EEA member states and Canada.[47]

Unlike the GDPR, most of these laws in Africa apply to in-country processing only. However, laws in Benin and Uganda have extra-territorial implications.[48]

Table 3: Data regime types, by country

Regime type	Countries with regime
1. No data protection law in place	Burundi, Cameroon, Central African Republic, Comoros, Congo, Democratic Republic of the Congo, Djibouti, Eritrea, Guinea-Bissau, Liberia, Libya, Malawi, Mozambique, Namibia, Sierra Leone, Somalia, South Sudan, Sudan, Tanzania
2. Draft data protection law	Ethiopia, The Gambia, Mauritania, Rwanda, Seychelles, Swaziland, Zimbabwe
3. Data protection law, no mention of data transfer adequate protection or user consent	Ghana
4. Data protection law, adequate protection not required for transfer if user consent or other exceptions in place	Algeria, Angola, Benin, Botswana, Cabo Verde, Chad, Equatorial Guinea, Gabon, Lesotho, Madagascar, Nigeria, Mauritius, Morocco, São Tomé and Príncipe, Senegal, South Africa, Togo
5. Data protection law, adequate protection or user consent required for transfer, no other exceptions listed	Uganda
6. Data protection law, adequate protection required for transfer, authority should be notified/approve of transfer	Burkina Faso, Guinea, Côte d'Ivoire, Mali, Niger
7. Data protection law, adequate protection required, special circumstances met, consent, authority should be notified/approve of transfer	Egypt, Kenya, Tunisia, Zambia

Following a global trend, African countries have set out to adopt more complex and demanding data transfer regimes in the past few years (figure 3). The content of data transfer laws in Africa mirrors global trends: in the eTrade Alliance's policy mapping with 40 non-African countries, the vast majority of countries have a data transfer law in place and most require the receiving country to have "adequate" data protections in place, and/or for the data subject to consent to the data transfer (figure 4).

Figure 3: African countries' data transfer regimes and timeline for adoption, by type

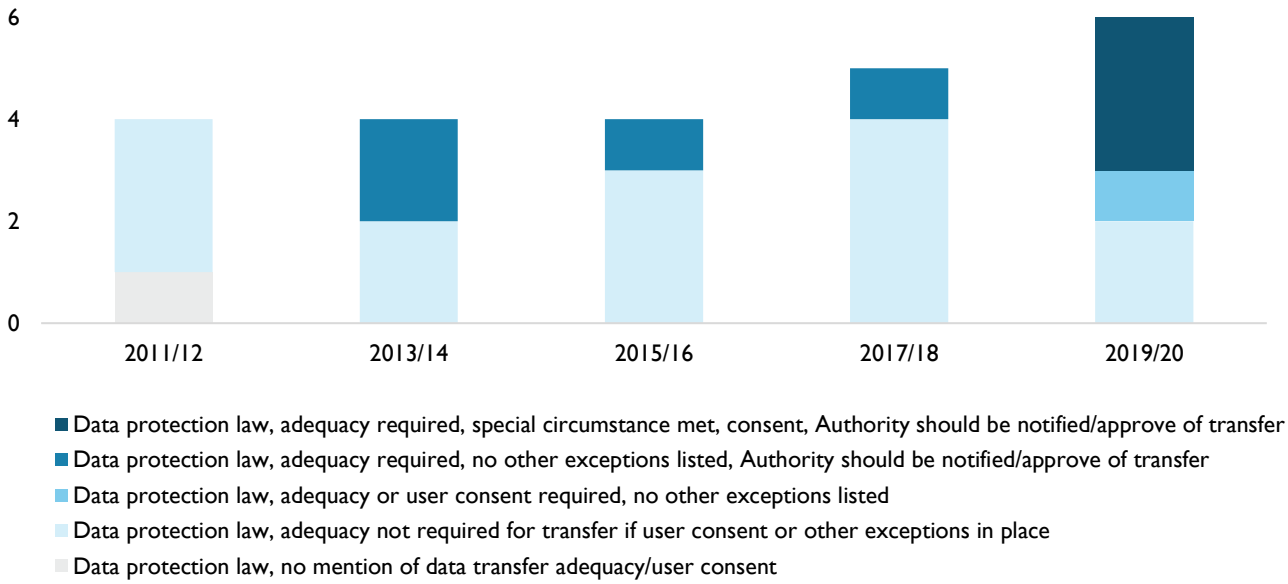
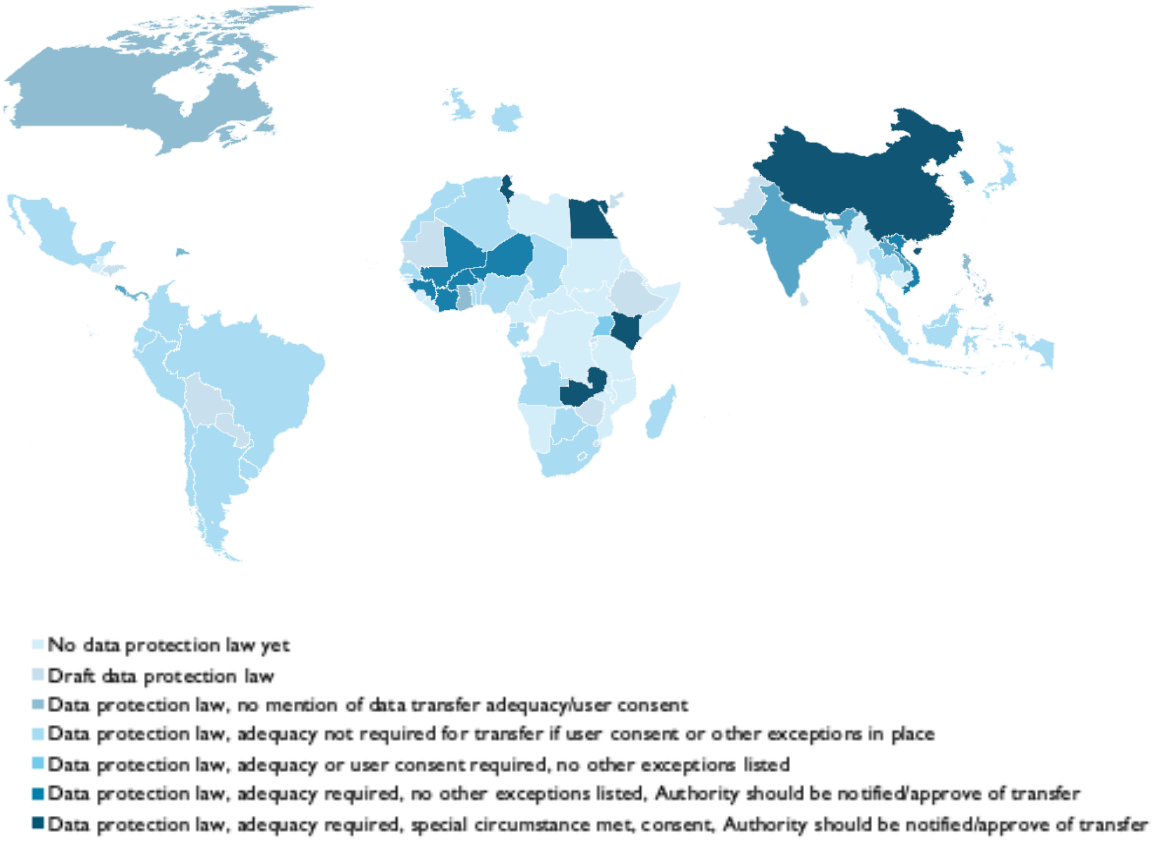


Figure 4: 94 countries' data transfer regimes, by type (mapping focused mostly on emerging markets and developing countries)



C. ENFORCEMENT OF DATA PRIVACY LAWS IN AFRICA

African governments have made inroads into enforcing their data laws; the DPAs of Benin, Ghana, Mali, Mauritius, Morocco, Senegal, and Tunisia have reportedly been especially active. [49] Some examples of implementation and enforcement processes include the following:

- **Morocco**'s data protection law was passed in 2009. The DPA Commission nationale de contrôle de la protection des données (CNPD) has issued activity reports for the years 2010–2013, 2014, 2015, and 2016. In 2019, there were 1,675 notifications (declarations and authorizations) and 575 complaints; the number of complaints rose to 429 between January 1, 2020, and June 8, 2020.[50] It is not clear whether CNDP has made enforcement actions.

- **Ghana**'s Data Protection Act was passed in 2012. In 2017, the Data Protection Commission issued the first public notice of noncompliance of data controllers with a list of companies that perform the function of a data controller but had not registered with the commission, advising the companies to register immediately to avoid prosecution.[51] It is not clear whether these notices resulted in enforcement action. In October 2020, the Data Protection Commission launched a new Registration and Compliance Software (RegSys) to streamline the registration and renewal process and improve the user experience for data controllers and processors.[52] Data controllers were given a six-month period to register and pay the current year's fees only. If a data controller failed to do so, the company would be subject to enforcement action, including payment of all arrears going back to 2012, where applicable.[53]

- **Benin** passed Law No. 2009-09 Dealing with the Protection of Personally Identifiable Information in 2009 and established the DPA (APDP) in 2011.[54] After the EU's GDPR went into effect in 2018, Benin promulgated the Digital Code, the Fifth Book of which specifically supplements the 2009 law with several GDPR principles. The APDP has published activity reports since 2011.[55] The reports include information on authorizations and declarations and complaints received.[56] It is not clear whether APDP has taken enforcement actions.

- **Kenya**'s Data Protection Act entered into force on November 25, 2019. A year after, in November 2020, the first data commissioner was appointed and the Office of the Data Commissioner commenced operations, launching a website, a contact form, and an email address, acquiring a postal address, and setting up social media accounts.[57] The office launched public stakeholder consultations and in April 2021 issued its Draft Guidelines for Compliance and Enforcement, Registration of Data Controllers and Data Processors, and Data Protection.[58] The guidelines were then open to public participation before further review by the office and subsequent planned enforcement later in 2021.

- **Nigeria**'s Data Protection Regulation (NDPR) was issued in January 2019. The National Information Technology Development Agency (NITDA) released the implementation framework for the regulation and appointed Data Protection Compliance Organizations (DPCOs), which are entities licensed by NITDA for training, auditing, consulting, and rendering services aiming to ensure compliance with this regulation.[59] DPCOs can be professional consultants, IT service providers, or law or auditing firms.[60] The NDPR requires organizations that process the personal data of more than 1,000 data subjects in six months to submit an initial audit report with NITDA, and organizations that process data of more than 2,000 data subjects in 12 months must submit an audit report annually.[61] In its first year in force, organizations had until October 2019 to submit an initial audit. In December 2019, NITDA issued noncompliance notices to 100 companies that had failed to submit an initial audit or

request an extension.[62] In 2021, NITDA extended the deadline for filing the 2020/21 audit report from March 15th to June 30th, 2021.[63]

- **Egypt**'s government issued Data Protection Regulation in July 2020; the law entered into force three months later in October 2020, with a one-year grace period for compliance.[64] During the grace period, data controllers and processors had to obtain a license or permit from the regulatory authority to process personal data. The license carries a maximum fee of 2,000,000 Egyptian pounds (approximately $125,000).[65] There is little further data on implementation or penalties to date.

- In **Uganda**, the Ministry of ICT and National Guidance released the Draft Data Protection and Privacy Regulations 2020 for public comment in September 2020.[66] These address registration, security breach notifications, and DPO requirements. The law creates a Data Protection Office within the National Information Technology Authority.

- In **South Africa**, enforcement of the data privacy law began on July 1, 2021.

Better analysis is still needed regarding the enforcement of the new data privacy laws and their economic impacts. The experience from the GDPR, a regime that has been increasingly widely studied, suggests that enforcement is challenging and costly for governments and that the regime has also had negative impacts on business activity and online sellers (case 3).

Case 3: Three years after entering into force, the GDPR is challenging for EU governments to enforce

Today, the majority of Europeans know about the GDPR and their data subject rights, but do not necessarily always know how to act on these.[67] When data subjects do make requests, businesses have struggled to keep up—in one survey, only 30 percent of organizations could respond to data requests within a month.[68] Businesses also err on the side of caution, flooding government agencies: in 2018, the UK's Information Commissioner's Office (ICO) disclosed that of the 500 weekly calls it received from companies reporting data breaches, one-third did not meet its reporting threshold.[69] During the GDPR's first nine months in force, authorities from 31 countries received 206,326 cases—94,622 complaints, 64,684 breach notifications, and 47,020 unspecified other cases—or an average of 740 cases per month per country.

What about enforcement? European DPAs—typically national entities such as ICO in the United Kingdom, Agencia Española de Protección de Datos (AEPD) in Spain, and Commission nationale de l'informatique et des libertés (CNIL) in France—are empowered to fine companies up to 4 percent of their annual revenue if they violate regulations pertinent to data collection, processing, and use. In the first two years of implementation of the GDPR, there were 261 enforcement actions, most of them implying small fines for privacy violations. The main large fines have included Google's €50 million fine (for not seeking consent), H&M's €35.3 million fine (for secretly monitoring employees), TIM's €27.8 million fine for aggressive marketing and unsolicited communications, and British Airways' €22 million fine (for data breach violations).[70] Altogether, GDPR fines are estimated to have totaled $332.4 million in 2018–2020.[71]

These headline cases notwithstanding, according to industry sources and the EU's own assessment, DPAs have had only limited capabilities to enforce regulations. The GDPR required that European governments provide adequate human and financial resources for enforcing it—but in 2020, 14 DPAs receive less than €5 million annually, and 21 national DPAs had only 10 or fewer specialist tech investigation staff (7 DPAs have 2 tech specialists or less).

EU's own GDPR review noted these challenges, highlighting the "stark difference between Member States" in DPA budgets and also discussing challenges in building a "truly common data protection culture" and handling cross-border cases.[72] Germany stood out with a budget of more than €80 million and 100 specialists (with federal and Länder resources combined).[73] Meanwhile, Ireland, the hub of tech companies that has the most complaints, reduced its enforcement budget even as complaints have grown. This has led to calls for the secretariat of the European Data Protection Board to establish an investigative tech unit to support national DPAs, another budget allocation.[74]

D. IMPACTS OF DATA PRIVACY AND TRANSFER RULES IN AFRICA: EARLY VIEWS FROM FIRMS

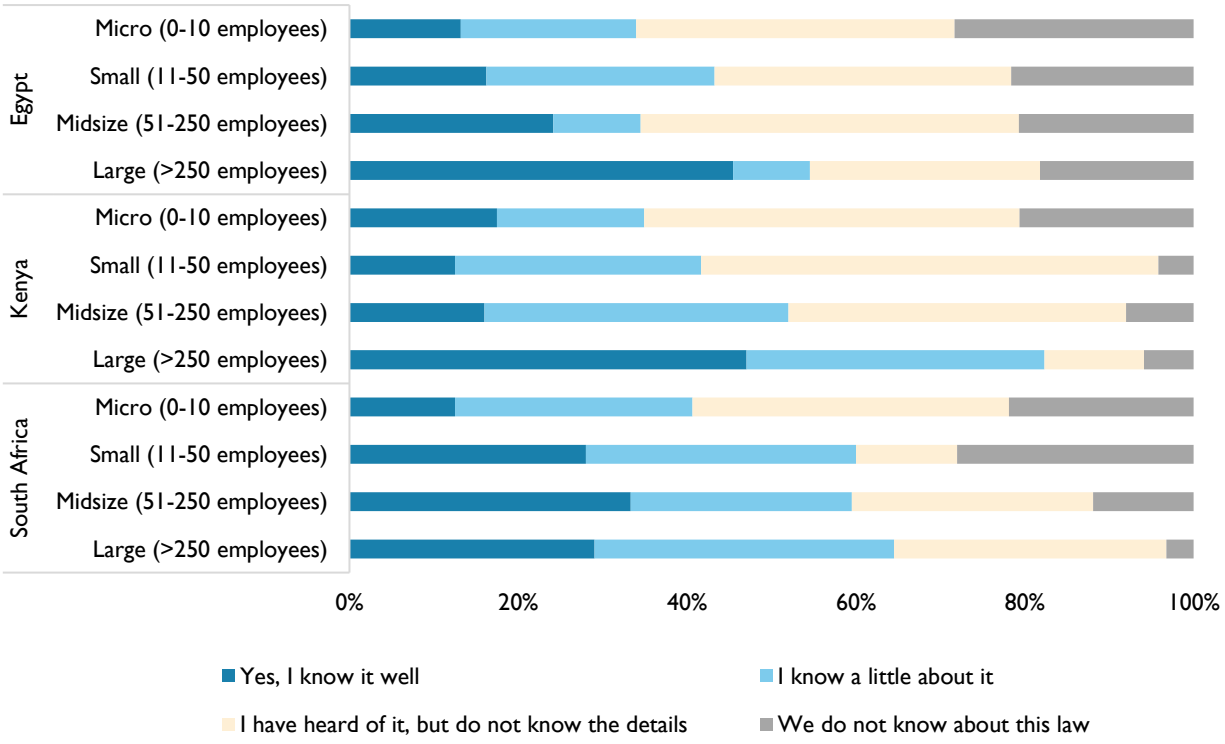
What then has been African firms' experience with the emerging data laws? Our survey data suggests several outcomes:

- About one-half of MSMEs are still quite unaware of their countries' data privacy laws and how these might apply to them; midsize and large firms are more informed and already implementing laws (figure 5; case 4).

- Firms of all sizes that know about their countries' laws have mostly learned about them from social media and the news. In Kenya, firms have also learned about laws from business associations (figure 6). Indeed, Kenyan firms are especially well-informed from many sources; in our survey, no firms from Kenya indicated difficulties in finding information about Kenya's privacy law.

- Companies find that their countries' data privacy laws have been positive in terms of providing greater clarity around how to use data and helping promote consumer confidence in online transactions. In Kenya and Egypt, large firms (which are better aware of these countries' data privacy laws) especially find that the law has helped build consumers' trust in online transactions (figures 7 and 8). Granted, a substantial set of firms (24 percent of large firms in Egypt and 33 percent of large firms in Kenya) find that implementation has been costly. So far, the negative effects of data laws on firms' cross-border data and sales have been muted.

Figure 5: African firms' knowledge of data privacy and transfer regulations in their countries, by country and firm size



Case 4: MSME online sellers learning about data privacy and transfer rules

Ruhi Suttarwala is Founder and CEO of Emmerce Ltd., a Kenya-based technology and marketing firm that offers digital solutions for African companies seeking to enhance their online visibility and performance, including website and mobile app development, integration of ecommerce platforms, and digital marketing services. The company's clients range from home business start-ups to medium-sized firms—selling products as diverse as home furniture and appliances to toys and sporting goods—many of which currently operate in or are seeking to expand to other African countries.

While Kenya and other East African nations require firms collecting "sensitive data" to register with and obtain special permissions from a government entity, Ms. Suttarwala notes that most of the customer data collected by her clients—typically name, email, address, and phone number, with payment details generally collected and stored by a third-party provider such as PayPal —does not in her company's interpretation fall into the category of "sensitive data." Her firm also employs third-party email marketing service providers to ensure that its clients offer appropriate unsubscribe options in all email communications.

Most of Emmerce's clients believe that so far, general terms and conditions included on their websites are usually sufficient to address any legal issues, that regulators are unlikely to introduce more restrictive policies in the near future, and that risk to their business is low given limited enforcement of data privacy laws.

However, Ms. Suttarwala recognizes that many digital policies and regulations are still in process across the continent, with various gray areas yet to be fully defined, e.g., whether birth date is considered "sensitive data." Emmerce is also cognizant of ever-changing policies on data privacy by private online platforms such as

Google and Facebook—some of which are generated in response to data policies and regulations elsewhere in the world. For example, Emmerce was forced to reconfigure various clients' online apps in response to a smartphone update, which mandated that developers ask users for their permission to track them across apps and websites owned by other companies.

Of greater concern to most of Emmerce's clients than data privacy is cybersecurity, which is as significant a threat in Africa and other developing and emerging markets as it is elsewhere in the world. There are also concerns about online fraud. While many of Emmerce's clients offer online sales, most orders are fulfilled as cash on delivery (COD) rather than more efficient electronic payments, as customers are reluctant to provide financial details for digital transactions.

Figure 6: African firms' sources of information about their countries' data privacy laws, by country and firm size

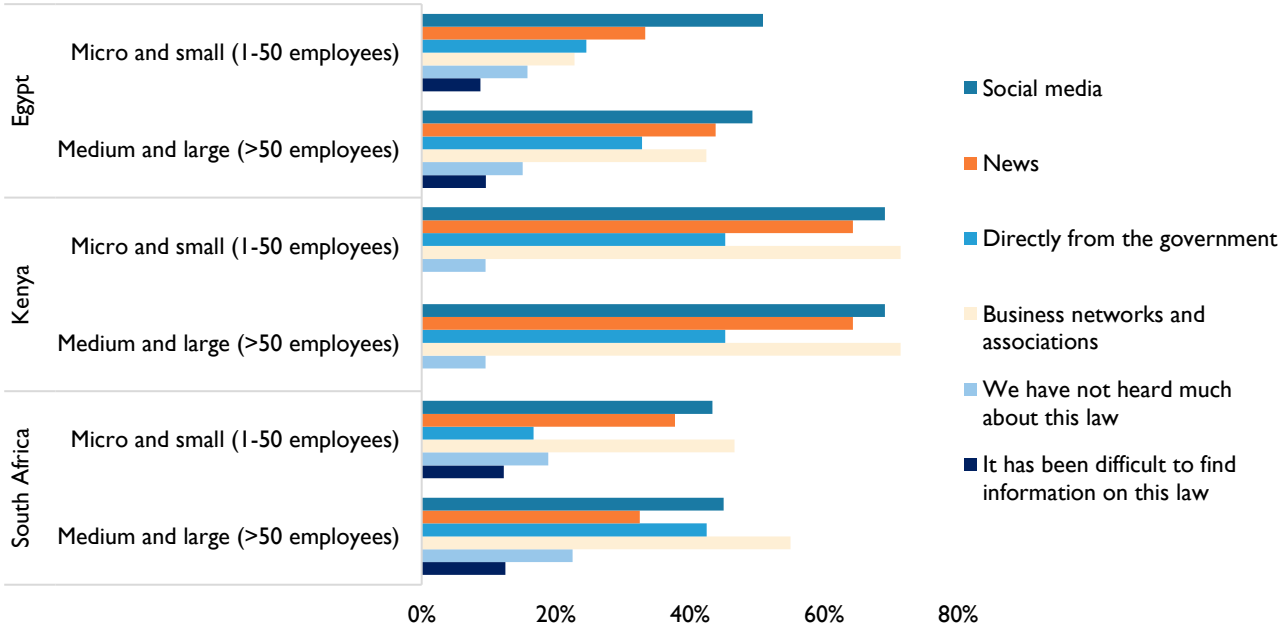
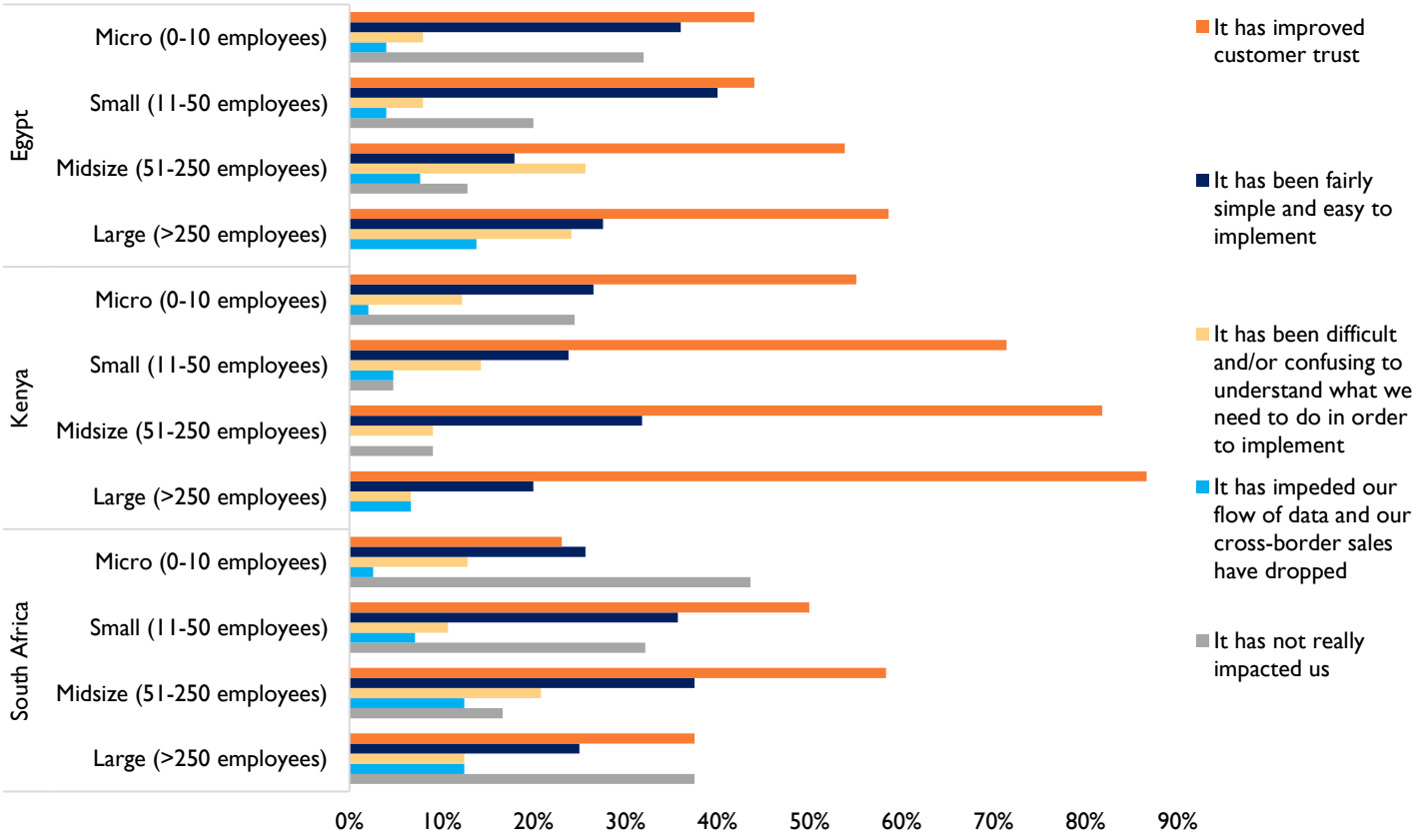


Figure 7: African firms' general impressions of data privacy and transfer regulations in their countries (how aware firms are of data privacy laws in their country)

Figure 8: African firms' perception of how data privacy and transfer regulations in their countries have impacted their businesses to date



Our survey data however also suggest new challenges are emerging, especially for firms that move data across borders:

- African firms appear hungry for clear rules to protect data that is being transferred: more than half of African firms take data protection seriously and are concerned about the end uses of data when transferring data to a third party (figure 9). This is especially true of marketplace sellers that move data across borders.

- At the same time, companies struggle to keep up with the proliferation of data privacy regimes in Africa and around the world: 54 percent of online seller-exporters and over 40 percent of non-exporters cite foreign data privacy laws as a deterrent to growing their cross-border ecommerce (figure 10). Foreign data privacy regimes are one of the two greatest challenges for both small and large exporters and non-exporters alike, alongside the similarly proliferating national regulations on online consumer protection.

- The checkerboard of divergent national digital regulations—differences across national data privacy regimes and digital regulations in general—is a growing challenge to current and aspiring multimarket exporters: 48 percent of micro and small online seller-exporters and 40 percent of midsize and large online seller-exporters feel that differences in national digital regulatory regimes limit their potential to export online.

Figure 9: Percentage of African firms expressing concerns about how third-party recipients of data use this ("Are you concerned about how a recipient of the data you transfer uses it?")

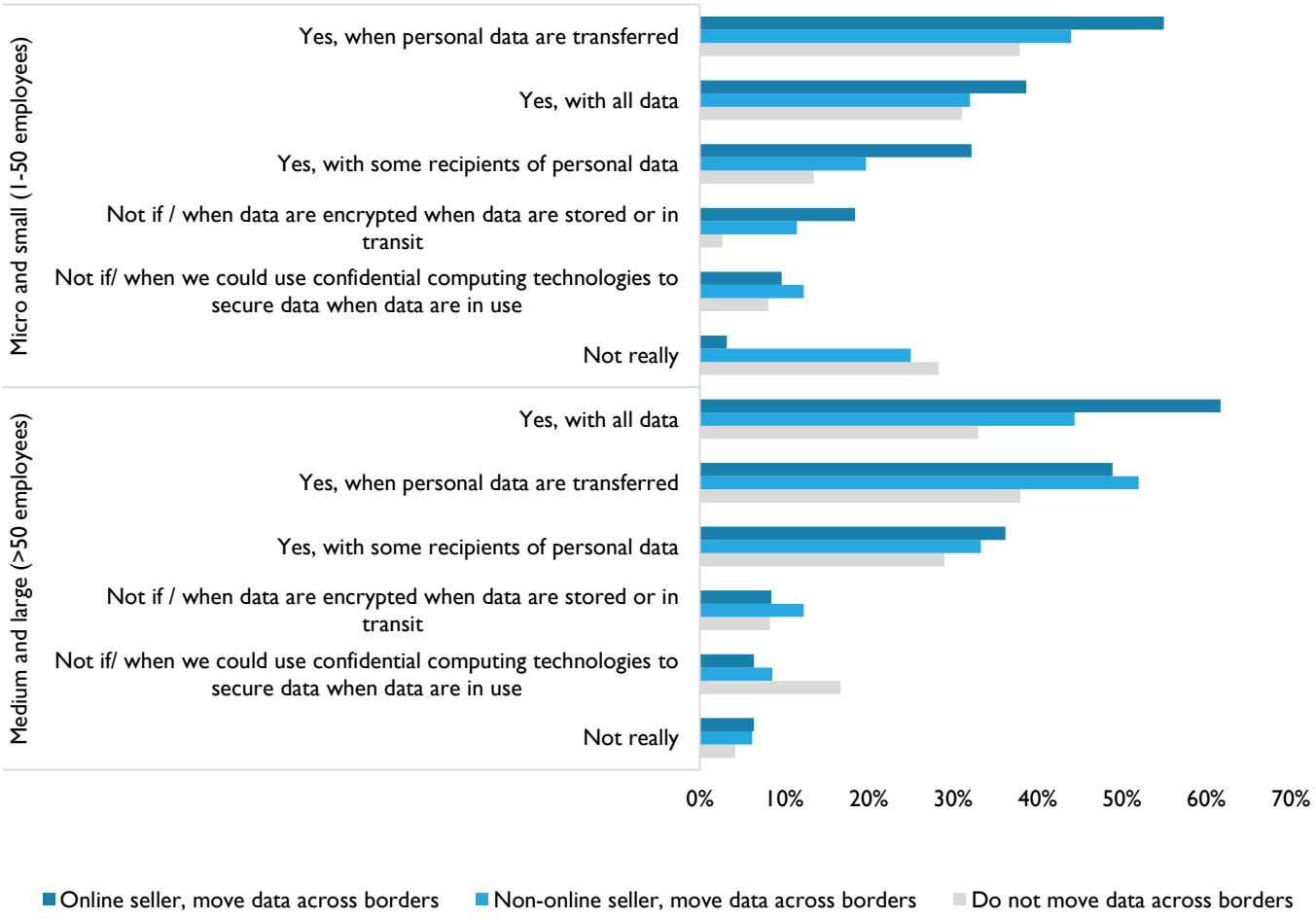
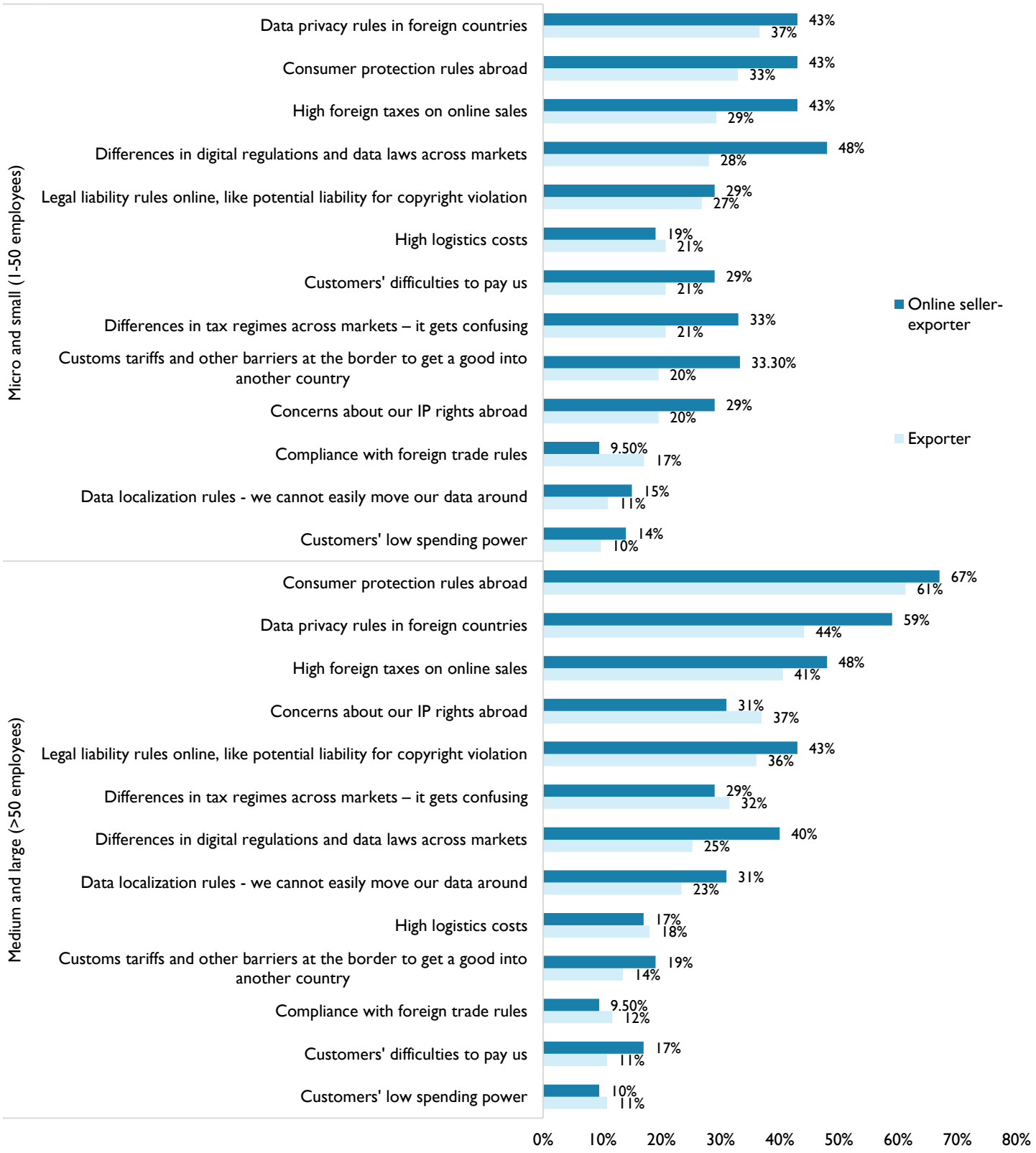


Figure 10: African firms' main perceived challenges in exporting products or services online, by size, export status, and type of seller



Granted, over the past decade, African governments have sought to preempt a setting with diverse national data privacy laws by pursuing various regional efforts to guide the development of national data privacy laws both at the continental level and through regional economic communities. There are two regional binding data protection instruments, the African Union Convention on Cyber Security and Personal Data and the ECOWAS Supplementary Act on Personal Data Protection:

- The **African Union Convention on Cyber Security and Personal Data Protection (AU Convention) of 2014** establishes continental rules for electronic transactions, personal data protection, and cybercrime.[75] The AU Convention is however not in effect, as it requires 15 members to ratify it, and only eight have done so to date (Angola, Ghana, Guinea, Mauritius, Mozambique, Namibia, Rwanda, and Senegal).[76] Some 14 further member states have signed it.[77]

- In 2018, the AU Commission and Internet Society developed **guidelines for implementing the principles of the AU Convention**. These endorse consistency among national data privacy laws in Africa, for example in such areas as the establishment of DPAs, enforcement measures, and determinations of such protection for cross-border transfers, and also recommend the establishment of an Africa-wide personal data protection committee.[78]

- The **ECOWAS Supplementary Act on Personal Data Protection of 2010** is a model law that aims to provide member states with direction for their national data protection laws.[79] It also establishes rules for governing special categories of data like genetic data and health research, criminal data, and biometric data, and data processed for public interest reasons. The act has been signed by 13 countries.

There are further nonbinding guidelines for regional data privacy laws in Africa, including:

- The **South African Development Community (SADC) Model Law on Data Protection** of 2013, which echoes the ECOWAS Supplementary Act and the AU Convention and seeks to build compatibilities among member states' data protection regimes. It includes principles for data processing, such as accuracy, storage limitations, lawfulness and fairness, purpose limitation, and accountability.[80]

- The **East African Community (EAC) Framework for Cyberlaws** of 2008, which addresses thematic issues like electronic transactions and signatures, cybercrime, data protection, data privacy, and consumer protection. Of the five member states, Kenya and Uganda now have data protection laws.

- The **Economic Community of Central African States (ECCAS) and the Communauté économique et monétaire de l'Afrique centrale (CEMAC)** also have data protection guidelines. ECCAS has 11 members while CEMAC has 6, which also belong to ECCAS. In 2013, ECCAS adopted model laws similar to the SADC model law; CEMAC also adopted these as draft directives.

Table 4 lists these instruments and member states. These are useful steps forward and likely served as guidance for governments that are fashioning data privacy laws. However, they have been more focused on domestic issues rather than addressing cross-border data transfers and have only helped converge national data privacy regimes to a limited extent.

Table 4: Regional data privacy and transfer models in Africa: Contents and member countries

Instrument	Contents	Binding or voluntary	Member countries	Countries that have ratified and/or applied
African Union Convention on Cyber Security and Personal Data of 2014	Establishes rules for electronic transactions, personal data protection, promoting cybersecurity, and combating cybercrime	Binding (but not in effect; requires 15 countries to ratify it)	55 AU member states	8 ratified: Angola, Ghana, Guinea, Mauritius, Mozambique, Namibia, Rwanda, and Senegal
ECOWAS Supplementary Act on Personal Data Protection of 2010	Establishes data protection rules including for special categories of data like genetic data and health research, criminal data, biometric data, and data processed for reasons of public interest	Binding	Member states: Benin, Burkina Faso, Cabo Verde, Cote d'Ivoire, The Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo	13 signatories: Benin, Burkina Faso, Cabo Verde, Cote d'Ivoire, The Gambia, Ghana, Guinea-Bissau, Liberia, Mali, Nigeria, Senegal, Sierra Leone, and Togo
South African Development Community (SADC) Model Law on Data Protection of 2013	Establishes principles for data processing, such as accuracy, storage limitations, lawfulness and fairness, purpose limitation and accountability, and cross-border flows	Voluntary	Member states: Angola, Botswana, Comoros, Democratic Republic of the Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania, Zambia, and Zimbabwe	All member states
EAC Framework for Cyberlaws of 2008	Series of recommendations to member states to reform laws on electronic transactions, electronic signatures, cybercrime, data protection and privacy, and consumer protection	Voluntary	Member states: Burundi, Kenya, Rwanda, South Sudan, Tanzania, and Uganda	All member states; however only Kenya and Uganda have data protection laws
ECCAS Model Laws/Communauté économique et monétaire de l'Afrique centrale (CEMAC) Draft Directives	Recommendations on data protection, electronic communications, and cybercrime. Similar to SADC model law, with added elements of its own on genetic data processing	Voluntary	ECCAS: Angola, Burundi, Cameroon, Central African Republic, Chad, Democratic Republic of the Congo, Equatorial Guinea, Gabon, Republic of the Congo, and São Tomé and Príncipe CEMAC: Gabon, Cameroon, the Central African Republic, Chad, the Republic of the Congo, and Equatorial Guinea	All member states

IV. TOWARD A REGIONAL DATA PRIVACY AND TRANSFER MODEL IN AFCFTA: WHAT ARE THE OPTIONS?

The above analysis has shown that many African countries have relatively new data privacy and transfer laws, and about half have no law in place. Countries are moving at different speeds to regulate data privacy. The existing regimes tend to fall into five groups, some of which require only the user's consent to transfer data, while others demand that the company making the transfer secure the data subject's consent, ensure the recipient country has an "adequate" data privacy regime, and notify a government agency about the transfer.

In turn, our survey data and anecdotal evidence suggest African firms that seek to engage in ecommerce use data intensively and are working to deal with the changing regulatory regimes. There are five main findings:

- African firms already access and use data from individuals, businesses, and their own operations, and exporters and online sellers particularly tend to import and export data as part of their daily operations. The boom in ecommerce in the continent will likely only amplify these flows.

However, most small firms are still quite unaware of their countries' new data privacy laws and how these laws impact them or their data transfer practices. Firms that do know about their respective countries' data privacy laws tend to view these laws as helping them understand how to treat consumers' data and generally promoting consumer trust in online transactions. However, a quarter of firms also see the new laws as costly to implement.

- African firms do not take data privacy lightly. Most firms are concerned about consumers' data privacy and about how third parties to whom data is being transferred may use this data.

- Firms that aspire to export are concerned about their ability to decipher and comply with foreign data privacy and other digital regulations, such as consumer protection laws.

- Online sellers struggle to deal with digital regulations, particularly the many disparate national data privacy regimes, when seeking to diversify their export markets—just as small exporters have struggled for decades to meet differing national product standards across potential export markets.

This diagnostic points to a two-pronged policy agenda for Africa—one, to ensure that national data privacy laws are in place and more compatible with each other, and two, to enable African firms and especially online sellers to use and move data across borders safely and with ease. Specifically, African governments can:

- Champion clear, high-quality data privacy regimes in various African countries and engage in awareness-building around them for MSMEs.

- Promote regulatory convergence to ensure that aspiring exporters only have to deal with relatively similar sets of rules when selling to and operating across many countries. Likewise,

digital regulations need to be more compatible to accommodate firms' interest in using ecommerce to service customers across multiple markets.

- Enable businesses to transfer, store, and process data with providers and locations that enable them to save costs and optimize their customer services and operations.

- Empower African companies, through policy and technology, to take greater control of and be accountable for their data management and transfer practices and strengthen their regulatory compliance.

A great many countries and regional groupings, especially ones in the Asia-Pacific and the Americas, have faced very similar circumstances to those that Africa is experiencing today—that is, a context in which countries are adopting data privacy laws at different speeds and the national laws that are being adopted differ somewhat or significantly from each other. As a result, these groupings have experimented with regional data transfer regimes that may also be useful in Africa and that help MSMEs comply with diverse data privacy laws across markets while enabling cross-border data transfers. As African governments and other stakeholders consider regional data transfer rules to support African MSMEs to engage in cross-border ecommerce, they can learn from these and other experiences. We turn to these next.

A. EMERGING REGIONAL DATA TRANSFER MODELS

There exist useful regional data transfer models that balance the objectives of the free transfer of data across borders, data privacy, and the ability for countries to maintain their national data privacy laws, that may also be helpful for African countries seeking to design a regional data transfer regime. Some leading examples include:

- The **APEC CBPR system**, a government-backed data privacy certification that private companies join voluntarily to demonstrate compliance with international data privacy protection mechanisms. Several members of the APEC forum follow the APEC CBPR. The 2020 USMCA recognizes the CBPR as a valid baseline for regulating data transfers in North America (case 4). Japan also refers to the CBPR in its data privacy legislation. Unlike the EU's GDPR, the CBPR does not replace or change a country's domestic data privacy laws and regulations, nor does it determine whether a country's privacy protections are "adequate." The CBPR is recognized by nine economies—Australia, Canada, Taiwan, Japan, Mexico, Philippines, South Korea, Singapore, and the United States (table 5). So far, four of the nine member countries have designated accountability agents, which are the third-party certification bodies required to certify a company as CBPR-compliant.

Table 5: CBPR system member countries

Member countries and accountability agents, if appointed	Countries with reported interest in joining CBPR
• Japan (JIPDEC) • South Korea (Korea Internet and Security Agency) • Singapore (Infocomm Media Development Authority) • United States (TRUSTe, Schellman & Company, NCC Group, HITRUST, BBB National Programs) • Australia • Canada • Taiwan • Mexico • The Philippines	• Brazil • Chile • China • Malaysia • Vietnam

- The 11-country **Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) of 2018** prohibits parties from localizing computing facilities (such as servers) in their countries; requires parties to allow the cross-border transfer of data and personal information; and calls on parties to adopt or maintain laws to protect ecommerce users' personal information. Many of these provisions have been "exported" to further trade agreements among CPTPP members and third countries, such as Chile's FTAs with Uruguay, Argentina, and Brazil. They are also echoed (even without enforcement) in the **Regional Comprehensive Economic Partnership (RCEP)** among 15 Asia-Pacific nations and the 2020 **Digital Economic Partnership Agreement** between Singapore, New Zealand, and Chile.

- The **United States–Mexico–Canada Agreement (USMCA)** of 2020 is a free trade agreement with a digital trade chapter that requires parties to allow the cross-border transfer of data of personal information and also recognizes the validity of the APEC CBPR system as the baseline data transfer mechanism. USMCA also requires member countries to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade." In other words, while USMCA calls on countries to allow data transfers in North America, it allows each member to maintain and adopt new privacy laws and encourages robust data privacy (case 5). Furthermore, the agreement calls on members to make their different privacy regimes interoperable and mutually compatible.

- The **Korea–United States FTA (KORUS)** of 2014 contained a pioneering ecommerce chapter that called for parties to "endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[81] The updated 2019 version cements these provisions further.

- The **United States–Japan Digital Trade Agreement** went into effect on January 1, 2020, and echoes the data transfer provisions in the USMCA.

- **ASEAN Model Clauses**. In January 2021, the Association of Southeast Asian Nations (ASEAN) approved "model contractual clauses" for cross-border data flows. Known as the **ASEAN Model Clauses**, these are voluntary and aim to get businesses in the ASEAN region

to adopt key data protection obligations and reduce compliance costs. They apply to controller-to-controller transfers and controller-to-processor transfers and are described in guides that are easy to understand.[82] Each ASEAN country's national regulators are to promote the Model Clauses and the ASEAN Data Management Framework (DMF) of January 2021, which supports the region's firms' compliance with data privacy laws.[83] For example, the DPA for Singapore encourages organizations in the country to use the DMF and the ASEAN Model Clauses to meet the requirements for international transfer under Singapore's Personal Data Protection Act.

- The **Digital Economic Partnership Agreement (DEPA)** of 2020 between Singapore, New Zealand, and Chile also echoes the CPTPP provisions but goes further in calling for parties to work on interoperable digital identities, electronic invoicing, electronic payments, and cooperation in such areas as AI governance and digital inclusion.

- The **Singapore–Australia Digital Economy Agreement (SADEA)** of 2020 bolsters the existing digital trade provisions of the 2017 Singapore–Australia Free Trade Agreement that calls for parties to allow cross-border data flows and adopt or maintain a legal framework to protect the privacy of users in ecommerce.[84] The SADEA echoes DEPA in that it includes forward-looking digital rules, including seven memoranda of understanding (MOUs) to operationalize "modules" on AI, data innovation, digital identities, personal information protection, e-invoicing, trade facilitation, and e-certification of agricultural commodities.

- The **Southern Common Market (Mercosur)**, consisting of Argentina, Brazil, Paraguay, and Uruguay, issued an ecommerce agreement in April 2021 whereby member countries committed to allowing cross-border transfers of data required for commercial activities, protecting the personal data of ecommerce users, applying adequate levels of protection to personal data received from another member state, and promoting self-regulation in the private sector.[85] The members also banned any duties on electronic transmissions.

- **The Regional Comprehensive Economic Partnership (RCEP)** was signed in 2021 among Australia, Brunei, Cambodia, China, Indonesia, Japan, Korea, Laos, Malaysia, Myanmar, New Zealand, the Philippines, Singapore, Thailand, and Vietnam. It has similar data transfer rules as the CPTPP but its ecommerce chapter is not subject to the agreement's dispute settlement clause, rendering it nonbinding and toothless. The chapter also has clauses that enable parties to opt out at will and for example to localize data or bar data transfers for a party to attain a "legitimate public policy objective, provided that the measure is not discriminatory."[86]

Table 6 summarizes the many regimes that have promoted data transfers or the protection of data privacy.

There are also useful bilateral policy innovations:

- The **United States–United Kingdom executive agreement** under the US Clarifying Lawful Overseas Use of Data (CLOUD) Act balances businesses' needs to transfer data across borders with law enforcement requests for data on overseas servers in criminal cases.[87] In 2018, the United States and the UK passed the executive agreement under the CLOUD Act, empowering each country's law enforcement agencies to approach cloud service providers in the other country and access data associated with criminal cases from them. To access the data, the requesting government must demonstrate probable cause, proof of a serious crime, and evidence that the information being sought relates directly to that crime.[88] Under the act, digital service providers may refuse to disclose data if doing so conflicts with their country's laws.

These types of arrangements may offer a useful means to regulate governments' access to data in another country in an organized and legal fashion.[89]

Case 5: Balancing privacy and data transfer in cross-border business—Mexico, Canada, and the United States in the USMCA and the APEC CBPR[90]

Many countries are in the process of reforming their data privacy laws to address internet users' privacy concerns, and many are also joining free trade agreements with increasingly robust digital trade and ecommerce chapters that discuss data privacy and data transfer across borders. What are the implications of these agreements for national data privacy laws?

The relationship between the 2019 USMCA and Mexico's 2010 Data Privacy Law is one example. The latter is one of the most advanced and frequently enforced privacy laws in Latin America. It obliges data owners to provide detailed information in their privacy notice regarding the data transfers that the data subject, or "owner," is willing to make, including personal information about the data subject, name of the data processor, the purpose of the transfer, and type and category of activity sector of the processor. The same terms that apply to the data owner also apply to the third party receiving the transferred data.

The law stipulates that international data transfers can be performed without the consent of the data subject when the transfer is allowed by a law or treaty signed by the Mexican government.[91] The USMCA is one such treaty. Its digital trade chapter states, "no Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person."[92] Parties to the USMCA can adopt or maintain a measure that is "inconsistent" with that principle, though, if "necessary to achieve a legitimate public policy objective," provided such a measure does not present "unjustifiable discrimination or a disguised restriction on trade." The USMCA also explicitly bars data localization, stating that "no Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."

Legal experts interpret the USMCA to be liberalizing in that it permits cross-border data transfer and clarifies potential exceptions countries can make to cross-border data transfer rules under the CPTPP agreement that both Mexico and Canada are members of (the United States withdrew before its signing).[93]

However, USMCA also cements the principle of data privacy. It requires member countries to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade." In other words, while USMCA calls on countries to allow data transfers in North America and promote interoperability of their data privacy regimes, it allows each member to maintain and adopt new privacy laws. Furthermore, the agreement calls on members to make their different privacy regimes interoperable and mutually compatible.

Notably, the USMCA formally recognizes the validity of the APEC CBPR system as the baseline data transfer mechanism, stating that "the Parties recognize that the APEC Cross-Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information."[94]

CBPR is a government-backed data privacy certification that private companies voluntarily join to demonstrate compliance with international data privacy protections.[95] Businesses and organizations that opt into the CBPR system must submit their privacy practices and policies for evaluation by an APEC-recognized "Accountability Agent" such as TRUSTe in the United States. Upon certification, the practices and policies become binding for that organization and enforceable by a privacy enforcement authority (such as the US Federal Trade Commission).

Unlike the EU's GDPR, which applies across EU countries, the CBPR does not displace or change a country's domestic laws and regulations, nor does it determine whether a country's privacy protections are "adequate." The CBPR is recognized by Canada, Mexico, the United States, Japan, South Korea, Australia, Taiwan, the Philippines, and Singapore.[96] Japan recognized the CBPR as a valid data transfer regime in its 2017 data privacy law. Thus, CBPR-compliant US companies transferring data from Japan do not need the protection decisions from the Japanese government they would otherwise need under Japanese law.

Developed by all 21 APEC economies and endorsed by APEC Leaders in 2011, an APEC economy must demonstrate that it can enforce compliance with the CBPR system's requirements before joining.

There are still some question marks. Some legal experts argue that the USMCA provision citing the CBPR means that America's eventual federal privacy law would recognize the CBPR to be consistent with the USMCA.[97] Others argue that CBPR participation does not and cannot displace local law if and when local law is more demanding.[98]

However, in the view of many observers, the USMCA has generally been successful in creating a flexible approach to data privacy and transfer that accommodates local needs and existing national legislation, such as that of Mexico, within a global framework.[99] It also provides a clear signal to the private sector that the United States, Mexico, and Canada are committed to creating a unified cross-border data transfer regime.

Table 6: Data transfer provisions in various regional groupings and trade agreements in the Asia-Pacific and the Americas

Agreements or instrument	Contents related to data transfer	Other key commitments to members related to digital trade	Binding or voluntary	Member countries
APEC Cross-Border Privacy Rules (CBPR) system (2011)	Free cross-border transfer of personal data among companies that have been CBPR-certified, specifically a recognized system to protect the data that is transferred across borders. Participating businesses like Apple, Box, HP, IBM, Lynda.com, Merck, Rimini Street, Workday, and Intasect to develop and implement data privacy policies consistent with the APEC Privacy Framework. These policies and practices must be deemed compliant with the minimum program requirements of the APEC CBPR system by an accountability agent (the only US-based accountability agent is TRUSTe) and be enforceable by law.	• Provide governments and organizations with a ready-built, internationally recognized framework to ensure adequate protection of personal information while enabling the secure flow of data	Voluntary	Australia Canada Japan Mexico Philippines South Korea Singapore Taiwan United States
Comprehensive and Progressive Agreement for Trans-Pacific Partnership (2018)	Parties are to allow the cross-border transfer of information, including personal information, by electronic means. Financial services data is exempted. Parties can adopt measures inconsistent with this rule to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.	• Put data privacy protections in place • Cooperation on consumer protection in ecommerce activities • Framework to prevent unsolicited commercial electronic messages • Promote cooperation on cybersecurity • Ban localization of computing facilities • Ban duties on electronic transmissions • Nondiscriminatory treatment of digital goods	Binding	Australia Brunei-Darussalam Canada Chile Japan Malaysia Mexico Peru New Zealand Singapore Vietnam
United States-Mexico-Canada Agreement (2020)	Parties are to allow the cross-border transfer of information, including personal information, by electronic means. Financial services data is exempted. Parties can adopt measures inconsistent with this rule to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.[100] Member States are to promote data privacy and can retain data privacy laws. APEC CBPR-consistent cross-border data transfers.	• Put data privacy protections in place • Cooperation on consumer protection in ecommerce activities • Framework to prevent unsolicited commercial electronic messages • Promote cooperation on cybersecurity • Ban localization of computing facilities • Ban duties on electronic transmissions • Promote safe harbor laws for internet intermediaries • Nondiscriminatory treatment of digital goods	Binding	Canada Mexico United States

Korea–United States FTA (KORUS) (updated 2019)	Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.	• Cooperation on consumer protection in ecommerce activities • Ban duties on electronic transmissions • Nondiscriminatory treatment of digital goods	Binding	Korea United States
United States–Japan Digital Trade Agreement (2019)	Parties are to allow the cross-border transfer of information, including personal information, by electronic means. Financial services data is exempted. Parties can adopt measures inconsistent with this rule to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.	• Put data privacy protections in place • Cooperation on consumer protection in ecommerce activities • Framework to prevent unsolicited commercial electronic messages • Promote cooperation on cybersecurity • Ban localization of computing facilities • Ban duties on electronic transmissions • Promote safe harbor laws for internet intermediaries • Nondiscriminatory treatment of digital goods	Binding	Japan United States
Digital Economic Partnership Agreement (2020)	Parties are to allow the cross-border transfer of information, including personal information, by electronic means. Financial services data is exempted. Parties can adopt measures that are inconsistent with this rule to achieve a legitimate public policy objective, provided that the measure (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.	• Put data privacy protections in place • Cooperation on consumer protection in ecommerce activities • Framework to prevent unsolicited commercial electronic messages • Promote cooperation on cybersecurity • Ban localization of computing facilities • Ban duties on electronic transmissions • Cooperation on interoperable digital identities, electronic invoicing, electronic payments, and in such areas as AI governance and digital inclusion	Binding	Singapore Chile New Zealand
Singapore–Australia Free Trade Agreement (SAFTA) (2017) and Singapore–Australia Digital Economy Agreement (SADEA) (2020)	Parties are to allow the cross-border transfer of information by electronic means, including personal information. Parties can adopt measures that are inconsistent with this rule to achieve a legitimate public policy objective, provided that the measure (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.	• Put data privacy protections in place • Cooperation on consumer protection in ecommerce activities • Framework to prevent unsolicited commercial electronic messages • Promote cooperation on cybersecurity • Ban localization of computing facilities • Ban duties on electronic transmissions • Nondiscriminatory treatment of digital goods • In 2020, MOUs on: AI, data innovation, digital identities, personal information protection, e-invoicing, trade facilitation, and e-certification of agricultural commodities	Binding	Singapore Australia

Regional Comprehensive Economic Partnership (RCEP) (2020)	Parties are to allow the cross-border transfer of information by electronic means, including personal information Financial services data is exempted. Parties can adopt measures inconsistent with this rule to achieve a legitimate public policy objective, provided that the measure (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective. However, members can exempt themselves at will from the ban on data localization to protect their "essential security interests."	• Put data privacy protections in place • Cooperation on consumer protection in ecommerce activities • Framework to prevent unsolicited commercial electronic messages • Promote cooperation on cybersecurity • Ban localization of computing facilities • Ban duties on electronic transmissions	Agreement is binding, but ecommerce chapter is carved out and not subject to dispute settlement, rendering it nonbinding	Brunei Darussalam Cambodia Indonesia Laos Malaysia Myanmar Philippines Singapore Thailand Vietnam Australia China Japan Korea New Zealand
ASEAN approved "model contractual clauses" (2021)	Free cross-border transfer of personal data, with templates setting out responsibilities, required personal data protections, and related obligations of the parties.	• Establish contractual terms and conditions that may be included in the binding legal agreements between parties transferring personal data to each other across borders	Voluntary	Singapore Brunei Cambodia Indonesia Lao Malaysia Myanmar Philippines Thailand Vietnam
Southern Common Market (Mercosur) Ecommerce Agreement (2021)	Parties are to allow the cross-border transfer of information by electronic means, including personal information. Parties can adopt measures inconsistent with this rule to achieve a legitimate public policy objective, provided that the measure (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.	• Put data privacy protections in place • Cooperation on consumer protection in ecommerce activities • Framework to prevent unsolicited commercial electronic messages • Promote cooperation on cybersecurity • Ban localization of computing facilities • Ban duties on electronic transmissions	Binding	Argentina Brazil Paraguay Uruguay

B. AFRICAN FIRMS' VIEWS OF LEADING REGIONAL DATA TRANSFER REGIMES IN THE ASIA-PACIFIC AND THE AMERICAS

Our survey suggests that African companies would be strongly in favor of the kind of data privacy and transfer rules included in CPTPP and USMCA also being adopted in Africa: both exporters and non-exporters look favorably on provisions that require signatories to adopt laws that bolster consumers' data privacy, encourage them to use technologies to safeguard data, allow data transfers across borders and allow firms to store data where it is most convenient (figures 11 and 12), describing these as "very" or "somewhat" beneficial.

Figure 11: African firms' views of selected ecommerce-related provisions in the CPTPP and USMCA, by type of seller

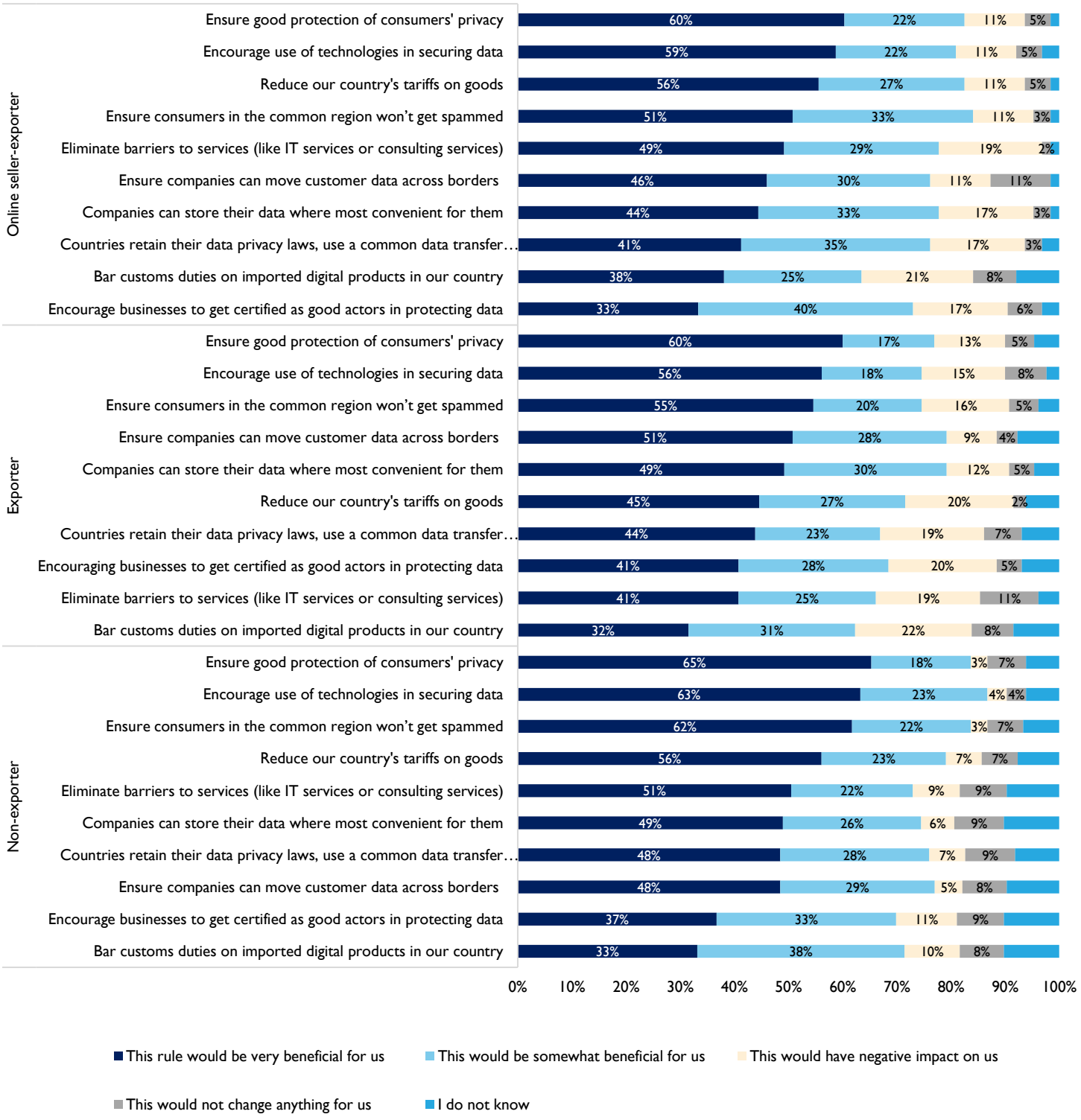
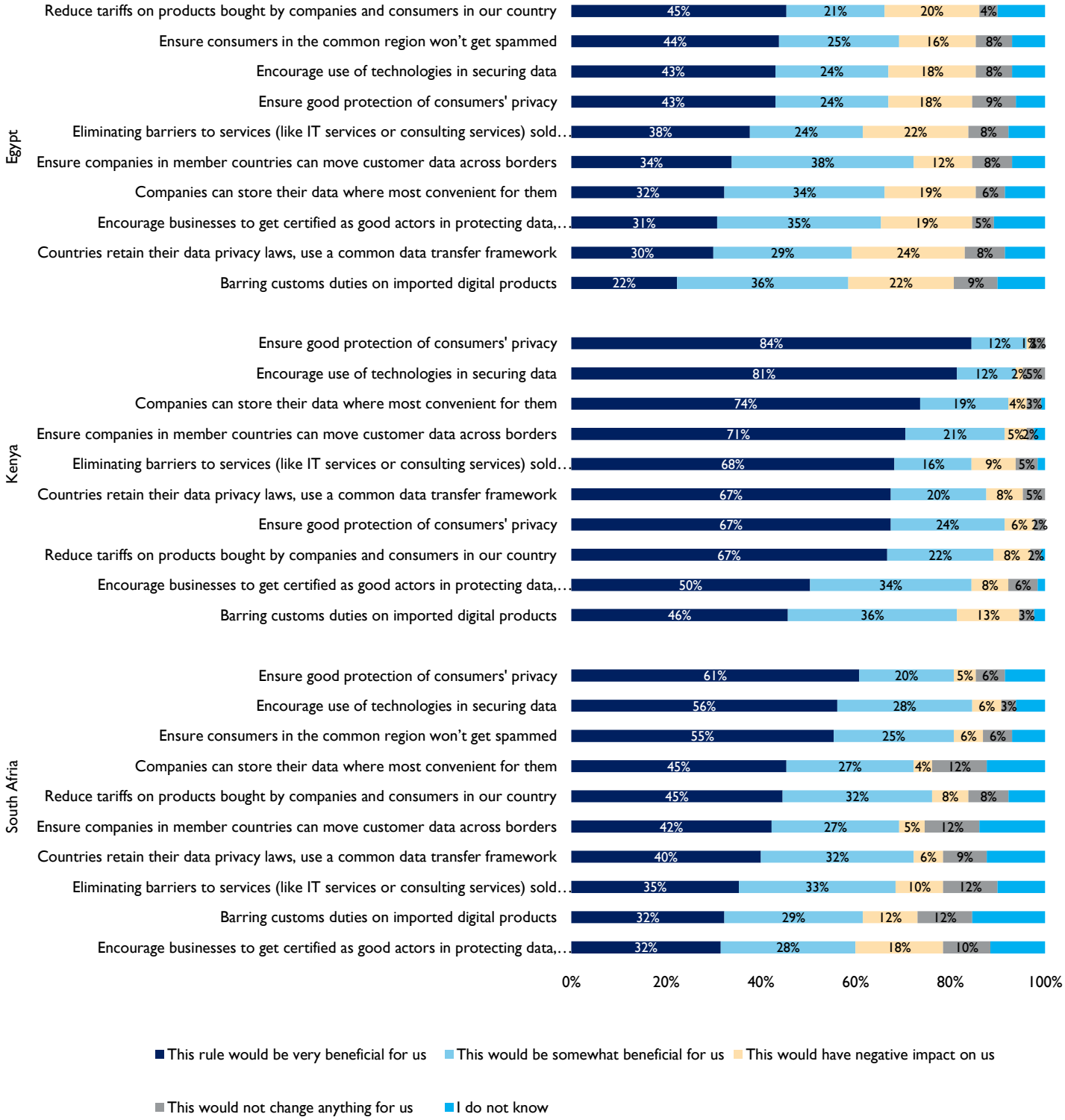


Figure 12: African firms' views of selected ecommerce-related provisions in the CPTPP and USMCA, by country



C. EMERGING PRIVACY-ENHANCING TECHNOLOGY SOLUTIONS FOR DATA AT REST, IN TRANSIT, AND IN USE

Policy is not the only solution for enabling secure and safe cross-border data transfers. Technologies that secure data at rest, in transit, and in use are developing rapidly—and our survey has suggested that the majority of African companies are concerned about the security of personal data they transfer to third parties and are keenly interested in technology solutions to help them safeguard this. Emerging solutions such as encryption and confidential computing can significantly aid African firms that leverage data and transfer data to third parties and across borders, thus preempting onerous regulations and costly enforcement. These solutions include:

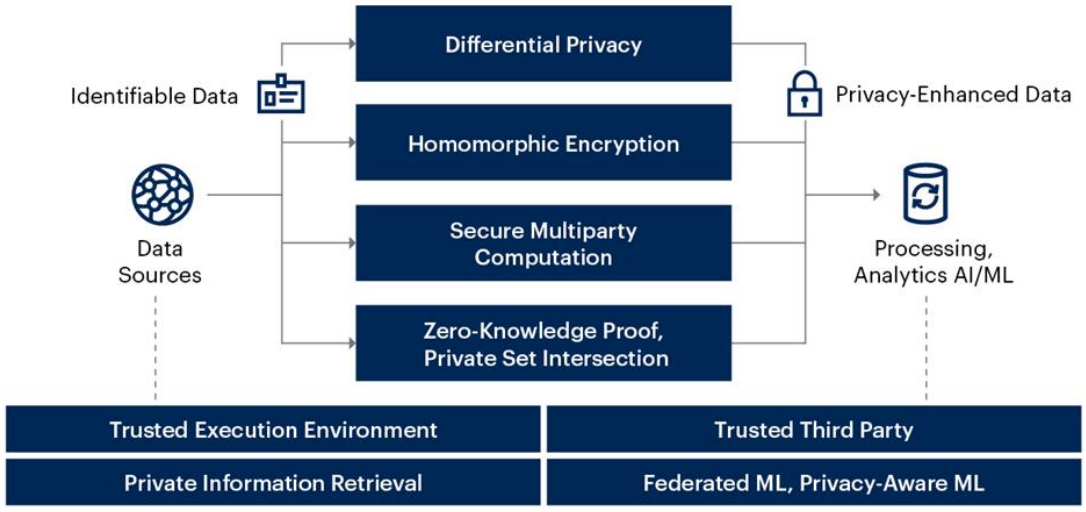
- **Encryption techniques that protect data that is *at rest or in transit*.** Encryption protects the confidentiality of data that is stored on computer systems and transmitted using the internet or other computer networks. Encryption algorithms are essential for the security of IT systems and communications and produce ciphertext that can be viewed in the original form if decrypted with the correct key.[101]

- **Confidential computing that helps protect privacy while data is *in use*** by isolating sensitive data during processing in a protected central processing unit (CPU) "enclave."[102] This helps solve the thorny problem that while data is typically encrypted at rest and in transit, it is exposed when in use within an organization or by a third party.[103] Some forecasts suggest that by 2025, half of large organizations will seek to adopt privacy-enhancing computation for processing data in multiparty data analytics.[104] Confidential computing could enable cloud computing applications, whereby two companies could combine data sets without accessing each other's data.[105] For example, retailers and credit card companies could verify transaction data for fraud without exposing user data. The early adopters of confidential computing in the United States have been the financial services, health, research, and government sectors.[106]

- **Two further solutions protect data in use: homomorphic encryption (HE)**, which enables permits users to perform computations on its encrypted data without first decrypting it, and **trusted platform module (TPM**), a security device that holds computer-generated keys for encryption and preempts hacking to capture passwords, encryption keys, and other information.[107]

Figure 13 summarizes the various privacy-enhancing technologies and use cases. African regulators need to account for the upcoming significant innovation in privacy technologies—which can possibly obviate onerous regulations that could cost businesses and governments enormous resources to implement. When fashioning data transfer policies, African governments could also support firms in piloting, adopting, and using these emerging technology solutions to maximize the opportunities that data could bring for their growth and development, while minimizing the likelihood of data breaches and misuse by third parties.

Figure 13: Privacy-Enhancing Computation Techniques



Source: Gartner.

V. CONCLUSIONS

African firms across sectors use data to improve their customer service, innovate new services, and mitigate fraud. Access to data and scalable storage and analytics solutions will bolster the region's ecommerce and digital ecosystems, accelerate the digital transformation of traditional industries and improve their productivity, and promote data privacy and security. Today, African MSMEs and startups setting out to grow their cross-border sales have ready access to globally available open APIs, software-as-a-service solutions, cloud computing services, global marketplaces, and global payment networks. These technologies enable them to leapfrog the 20th century's paper-based processes and monolithic IT systems to build innovative, vibrant digital ecosystems and attract investment.

This paper has shown that African firms, especially African online sellers, demand policies and technologies to safeguard their users and customers' data privacy and to import and export data to support their operations. There are two main ways in which countries could meet this demand:

- Countries in many other regions have wrestled with similar data governance issues and challenges to those facing African countries today. They have also done so in similar contexts where countries are adopting data privacy laws at different speeds and the national laws that are being adopted differ somewhat or significantly from each other. There exist useful regional data transfer models that balance the objectives of free data transfer across borders, data privacy, and the ability for countries to maintain their national data privacy laws. Some leading examples include the APEC CBPR system and two free trade agreements with robust, high-quality digital trade chapters, the CPTPP and the USMCA. The data transfer and privacy protection policies included in these agreements are fully consistent with the aspirations of a vibrant, trade-creating AfCFTA and the promotion of MSME ecommerce. According to our survey, both are also strongly favored by African firms.

- Policy is not the only solution for enabling secure and safe cross-border data transfers. Emerging technology solutions such as encryption and confidential computing can significantly aid African firms that leverage data and transfer data to third parties and across borders, thus preempting onerous regulation and costly enforcement. In the next decade, these and other privacy-preserving technologies are bound to become much more prevalent; their use among African firms needs to be promoted.

There is likely also an important role for technical assistance to accelerate the development and implementation of emerging data privacy and transfer laws in various African countries, and to support the development of a regional framework for data transfer. However, support should be provided for countries with policy frameworks that are compatible with the aims of free trade and MSME cross-border ecommerce.

Appendix I: Data Privacy and Transfer Laws in Africa

Country	Year	Data transfer is allowed explicitly due to regulation/law or implicitly because of lack of law	Data transfer is limited with jurisdictions with laws that are weaker or not branded "adequate"	Data transfer requires user consent
Algeria	2018	Article 44 of Law No 18-07 on data protection states that the data controller may only transfer personal data to a foreign country with the authorization of the national authority, and only if that country ensures a sufficient level of protection of privacy and fundamental rights and freedoms of individuals concerning the processing of data. The level of protection provided by a State is assessed by the national authority.	Yes, receiving country should have sufficient protections in place. If not, the data controller must obtain express consent from data subjects, or another exception needs to apply.	Not required if the receiving country has adequate protection in place. However, if such protection is not in place, then transfers are justified by consent or a list of other exceptions such as to safeguard the life of that person, protect the public interest, or the performance of a contract.
Angola	2011	Under Law No. 22/11 on the Protection of Personal Data, data transfer is allowed to countries with adequate protection, but the DPA must be notified of the transfer.	Yes, if the transfer is to a country without adequate data protection, the DPA must authorize and approve the transfer.	Not required if the receiving country has adequate protection in place. However, if such protection is not in place, then written user consent is sufficient for the DPA to authorize the transfer. Other reasons include if the transfer is necessary because of a treaty, for humanitarian assistance, necessary for the execution of a contract, to protect the public interest, or to protect data subjects' vital interests.
Benin	2017	Article 391 of Book V of the 2017 Digital Code of the Republic of Benin: Protection of Personal Data states that before any transfer of personal data to a third country or international organization, the controller must obtain authorization from the authority.	Yes, the country to which data is being transferred should have adequate protection (Article 391).	Not required if the receiving country has adequate protection in place. However, if such protection is not in place, then express user consent is sufficient to authorize the transfer. Other reasons for authorizing transfers include the transfer being necessary to conclude a contract, to protect the public interest, or to protect data subjects' vital interests (Article 392).
Botswana	2018	Under Article 48 of the Data Protection Act 2018, data transfer to another country is generally prohibited. However, "the Minister may, by Order published in the Gazette, designate the transfer of personal data to any country listed in such Order."	Yes. The transfer of personal data from Botswana to another country will be prohibited except if designated adequate by the minister through an order published in the Government Gazette. Cross-border transfers of personal data require prior authorization to be granted by the commissioner. If this is not in place, there are certain exceptions where a transfer can take place.	Not required if the receiving country has adequate protection. However, transfers are justified by consent as well as certain exceptions such as where the transfer is: necessary for the performance of a contract, for a legal claim, to protect the data subject's vital interests, or made from a register that is intended to provide the public with information and is open to public inspection (Article 49).

Burkina Faso	2004	Law No. 010-2004 on data protection states that the data protection agency allows international data transfers by legal or contractual means: the legal process necessitates the host country to provide adequate protection; the contractual process, in case of the absence of data protection legislation, requires two companies to abide by a contract for personal data transfer in accordance with the protection legislation. The agency also recognizes the binding corporate rules of the Association francophone des autorités de protection des données personnelles (AFAPDP) as an alternative to the contractual process.	Yes, receiving country should have adequate protection, or parties should have a contractual agreement, or through the AFAPDP's binding corporate rules.	Not found in the law (Article 24).
Burundi		No data protection law in place as of 2021.	N/A	N/A
Cabo Verde	2001	Data can be transferred to countries deemed as having adequate privacy measures in place, and the authority will need to be notified or the data controller will have to obtain authorization from the authority.	Yes, data transfer is limited if receiving country is not deemed adequate, or the authority has to authorize the transfer.	According to Article 20 of the Law, the cross-border transfer of personal data requires the express consent of the data subject. However, the Law provides that the consent is not required in a number of circumstances, such as: where the transfer is necessary for the execution of a contract, to protect an important public interest or for the defense of a potential legal claim, to protect the vital interests of the data subject, and where the data was lawfully collected from publicly available sources.
Cameroon		No data protection law in place as of 2021.	N/A	N/A
Central African Republic		No data protection law in place as of 2021.	N/A	N/A
Chad	2015	Data can be transferred to countries that are members of CEMAC or CEEAC. If the country is not a member, then it should ensure adequate protection. If neither of these circumstances exists, data subject consent or other exceptions may allow the transfer.	Yes, if the country is not a member of CEMAC or CEEAC, it needs to have adequate protection.	Not required if the country is a member of CEMAC or CEEAC or has adequate protection. Otherwise, consent alone can justify the transfer, as well as exceptions such as to protect data subject, public interest, or fulfill a contract.
Comoros		No data protection law in place as of 2021.	N/A	N/A
Congo, Republic of the		No data protection law in place as of 2021.	N/A	N/A
Congo, Democratic Republic of the		No data protection law in place as of 2021.	N/A	N/A

Côte d'Ivoire	2013	Article 26 of the Law 2013-450 on the Protection of Personal Data states that data can be transferred to a third country if a higher or equivalent level of protection is provided, and that before any transfer the data processor must first obtain permission from the protection body.	Yes, the receiving country should have higher or equivalent privacy protections.	N/A: the law does not mention user consent in data transfer.
Djibouti		No data protection law in place as of 2021.	N/A	N/A
Egypt	**2020**	The Law on the Protection of Personal Data of 2020 stipulates that it is prohibited to carry out transfers, storage, or sharing of personal data to a foreign country unless there is a level of protection no less than what is required by this law. A license or permit from the DPA for protecting personal data must also be obtained. However, data may be transferred in the absence of this if the data subject consents and an exception exists.	Yes, the other country must have adequate standards in place, otherwise the conditions of data subject consent and an exception must be met.	Not required, if adequate measures are in place in the receiving country and the data controller has received a license or authorization from the DPCO. Otherwise, consent is required.
Equatorial Guinea	2016	Under Article 27 of the Data Protection Law, personal data can only be transferred to countries that offer adequate protection, unless such transfers are made pursuant to an authorization from the DPA, the data subject has consented, or another exception exists.	Yes, either the authority must authorize the transfer, the data subject must consent, or another exception must be met.	Not required if adequate safeguards are in place or the transfer is needed to fulfill a contract or international treaty or for the public interest, for example.
Eritrea		No data protection law in place as of 2021.	N/A	N/A
Eswatini		Draft Data Protection Bill Part VIII establishes that data should be transferred to an SADC member state that has transposed the data transfer requirements. Otherwise, there needs to be extra authorization, consent, or the transfer should be necessary to fulfill a contract, public interest, etc.	In the draft law, yes, it should be an SADC member country who has transposed requirements or has such protections in place. Otherwise, consent or special circumstances are required.	In the draft law, not required if the country is an SADC member state or adequate measures are in place.
Ethiopia		Draft Data Protection Proclamation discusses data transfer; however, it has not been passed into law.	N/A	N/A
Gabon	2011	Under Article 94 of Law No. 001/2011 on the Protection of Personal Data, data transfers to another country are prohibited unless the other country ensures an adequate level of privacy protection.	Yes, receiving country should have adequate data protection in place, with a few exceptions.	Not required if the receiving country has such protection standards in place, However, if the country does not have adequate protection, then express user consent is sufficient to allow the transfer. Other exceptions to such protection include if the transfer is necessary to save a person's life, safeguard the public interest, be used in a court of law, or perform a contract (Article 95).
The Gambia		Section 9 of the Draft Data Protection and Privacy Policy Strategy of 2019 specifies that the cross-border transfer of personal data may only take place when the appropriate protection is guaranteed.	In the draft law, such protection must exist in receiving country for data transfer.	N/A
Ghana	2012	Ghana's Data Protection Law from 2012 does not mention data transfer.	N/A	N/A

Guinea	2016	Article 28 of the Law on Cybersecurity and Data Protection states that the person responsible for processing personal data may only be authorized to transfer data to a third country if the receiving state ensures a higher or equivalent level of protection. Before any effective transfer of personal data to this third country, the data controller must first obtain the authorization of the Personal Data Protection Authority. Any transfer of personal data to a third country is subject to strict and regular control by this Authority with regard to their purpose.	Yes, limited to countries that are deemed adequate by the Personal Data Protection Authority.	Unclear: the law does not mention user consent in data transfer.
Guinea-Bissau		No data protection law in place as of 2021.	N/A	N/A
Kenya	2019	In November 2019, Kenya passed the Data Protection Act, 2019 which complies with EU legal standards. Article 48 states that in order to transfer data to another country, the data processor shall ensure adequate standards are met in the receiving country and provide proof to the data commissioner, and the transfer should be necessary for a listed reason such as the performance of a contract, a matter of public interest, or to protect data subjects' vital interests.	The transfer of personal data outside Kenya is highly regulated under the Act. Prior to any transfer, the data controller or data processor must provide proof to the data commissioner regarding the appropriate safeguards for the security and protection of personal data, including for jurisdictions with similar data protection laws.	Yes, for sensitive personal data, consent is required for transfer out of Kenya. In addition to obtaining consent, the transfer must be to a country with adequate safeguards, and necessary for: the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures taken at the data subject's request; for the conclusion or performance of a contract; for any matter of public interest; for a legal claim; to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights, and freedoms of the data subjects (Article 48, 49).
Lesotho	2011	The Data Protection Act of 2011 states that to transfer data, either the recipient should have similar protection provisions and safeguards in place, or the data subject must consent to transfer, the transfer must be necessary for a contract, or the transfer must benefit the data subject.	Yes, receiving country should have adequate measures in place, otherwise the data subject's consent is needed, or the transfer must be necessary for a contract or be in the data subject's best interest.	Not required if adequate measures are in place or the transfer is necessary for a contract or is in the data subject's best interests.
Liberia		No data protection law in place as of 2021.	N/A	N/A
Libya		No data protection law in place as of 2021.	N/A	N/A

Madagascar	2014	Article 20 of Madagascar's Law No 2014-038 on the Protection of Personal Data states that the data controller may only transfer personal data to a foreign country if the receiving country has legislation that ensures a level of protection for individuals similar to that provided by this law.	In the absence of a similar level of protection, the Commission malagasy sur l'informatique et des libertés (CMIL) may authorize the transfer of personal data when the data controller offers sufficient guarantees with regard to the protection of privacy and the fundamental rights and freedoms of individuals; these guarantees may come from contractual clauses or the adoption of internal rules. There are also other exceptions where data can be transferred (Article 20).	Not required if the receiving country has such protection standards in place or the data controller can ensure appropriate safeguards, However, if these conditions are not met, then express user consent is sufficient to allow transfer as long as they have been informed of the lack of similar levels of protection. Other exceptions to such protection include: to safeguard the public interest, if necessary, for use in a court of law, to perform a contract, or to protect data subjects' vital interests (Article 20).
Malawi		No data privacy laws have been passed as of 2021, though the government is working on a draft.	N/A	N/A
Mali	2013	Article 11 of Law No 2013-015 on the Protection of Personal Data states that in order to transfer data abroad, the data controller must ensure the receiving state has sufficient levels of protection due to internal legislation or international commitments. Alternatively, the authority in charge of protecting personal data can authorize the transfer if the receiving state guarantees an adequate level of protection, particularly through contractual clauses or internal rules.	Yes, receiving country should have adequate protections in place through laws, international commitments, contractual clauses, or internal rules.	Law does not mention consent in terms of data transfer.
Mauritania		As of 2021, draft data protection law had not yet commenced. Section 2 states that the third country should have adequate measures in place, otherwise the data controller will need authorization from the DPA, the data subject should consent, or another exception must be in place.	Draft law—yes.	Draft law—not required unless such protection is not in place or other exception is not in place.
Mauritius	2017	Article 36 of Data Protection Act No. 20/2017 states that data can be transferred to another country where the data controller has provided the commissioner with proof of appropriate safeguards, the data subject has given explicit consent, or the transfer is necessary under a list of exceptions.	Yes, the data controller should provide the commissioner with proof that appropriate safeguards are in place in the other country, otherwise another exception must be met.	Not required if the data controller has provided the commissioner proof that adequate protection is in place in the other country, otherwise, explicit consent can authorize a transfer after notice has been given of a lack of appropriate safeguards. Other circumstances that can authorize a transfer include when the transfer is necessary for a contract, in the reason of public interest, to protect a data subject's vital interests, or for a legal claim.

Morocco	2009	Pursuant to Chapter V of the Moroccan Data Protection Act Law No. 09-08/2009, offshore data transfer is permitted as long as the laws of the importing state provide adequate protection. If not, the data owner may expressly consent to the transfer, or an exception can authorize the transfer.	Prior authorization from the National Commission is required before any transfer of personal data to a foreign state. Further, the person in charge of the processing operation can transfer personal data to a foreign state only if said state ensures adequate protection for the privacy and fundamental rights and freedoms of individuals regarding the processing to which this data is or might be subject, under the applicable legal framework, unless the data subject has expressly consented to the transfer or the conditions for an exception are met.	Not required if the receiving country has adequate protections in place, or a special circumstance is met, such as compliance with a legal obligation; the execution of a contract; protection of the vital interests of the relevant data subject, if that person is physically or legally unable to give their consent; performance of a task of public interest or related to the exercise of public authority; fulfillment of the legitimate interests pursued by the data controller or by the recipient, when not outweighed by the interests or fundamental rights and freedoms of the relevant data subject.
Mozambique		No data protection law in place as of 2021.	N/A	N/A
Namibia		Namibia has been working on a draft data protection bill, but it has not been passed as of 2021.	N/A	N/A
Niger	2017	Transfer of a data subject's personal data to a third country is allowed if the country guarantees individuals a sufficient level of protection in terms of privacy and fundamental rights and liberties. Prior to any transfer of personal data to a third country, the data controller must inform the HAPDP.	Yes, the receiving country should guarantee adequate protection.	N/A
Nigeria	2019	The Nigeria Data Protection Regulation 2019 is modeled on the GDPR. For data to be transferred to a foreign country, the NITDA or Honorable Attorney General of the Federation (HAGF) should ensure the foreign country has adequate data protection standards in place. However, in the absence of any decision on such protection from the foreign country, data can be transferred under certain circumstances.	Yes, the receiving country must either be branded adequate, or the data subject must consent to transfer after being informed of possible risks due to lack of such protection, or the transfer must meet an exception.	Not required if the receiving country has adequate protection in place, or a special circumstance is met, such as transfer being necessary for the performance of a contract, for important reasons of public interest, for a legal claim, or if the transfer is necessary to protect the vital interests of the data subject or other people, or where the data subject is physically or legally incapable of giving consent.
Rwanda		In October 2020, Rwanda's cabinet passed the Data Protection Bill, however, it has not been implemented yet. It is similar to Mauritius's legislation—the data controller should get authorization to transfer after providing proof of appropriate safeguards to the authority, or the data subject must give explicit consent if appropriate safeguards are absent, or in the case of other exceptions, such as a contract, public interest, or data subjects' vital interests (Article 54).	Under the draft law, yes.	Under the draft law, user consent is required if appropriate safeguards are not in place and the user must be notified of the possible risks this entails.
São Tomé and Príncipe	2015	Under Chapter V of the Data Protection Law, the transfer should take place only to countries with adequate protection. If no such protection is in place, user consent or another special circumstance can allow the transfer.	Yes, the other country should have such protection in place, otherwise, user consent is needed, or exceptions can apply.	Not required if such protection is in place, otherwise, user consent can authorize transfer, or another exception like the performance of a contract, or being in the public interest.

Senegal	2008	Under Law No. 2008-12 of January 25, 2008, on the Protection of Personal Data, data transfer should occur only to a third country that ensures an adequate level of protection, and the data controller must first inform the commissioner before transferring data. If this protection is not in place, there are alternative options for authorization, such as user consent and certain exceptions (Article 49, 50).	Yes, the receiving country should have adequate protection, otherwise, user consent or certain circumstances would be necessary.	Not required if there are adequate safeguards in place and the commissioner has authorized it. But, if this is not the case, the data controller may transfer personal data to a third country that does not meet such protection requirements if the transfer is one-off, not massive, and the person to whom the data relates has expressly consented to its transfer; or if the transfer is necessary for any of the following purposes: to protect the subject's life, to protect the public interest, to comply with a legal claim, or for the performance of a contract (Article 50).
Seychelles		Data protection bill from 2003, but still not in force as of 2021.	N/A	N/A
Sierra Leone		No data protection law in place as of 2021.	N/A	N/A
Somalia		No data protection law in place as of 2021.	N/A	N/A
South Africa	2013	The main data protection legislation in South Africa is the Protection of Personal Information Act No. 4 of 2013. Transfers of personal data abroad must be to countries deemed adequate and are prohibited unless the data subject consents to the transfer, the transfer of data is necessary for the conclusion or performance of a contract, or when the transfer is for the benefit of the data subject.	Yes, the foreign country must have similar adequate measures in place.	Yes, with exceptions. It is not necessary to obtain consent if the transfer is for the benefit of the data subject, and it is not reasonably practicable to obtain the data subject's consent to the transfer or, if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.
South Sudan		No data protection law in place as of 2021.	N/A	N/A
Sudan		No data protection law in place as of 2021.	N/A	N/A
Tanzania		No data protection law in place as of 2021.	N/A	N/A

Togo	2019	Under Law No. 14/2019 on the protection of personal data, the data controller may only transfer data to a third country if that country ensures adequate protection of privacy, and the controller must first inform the DPA for authorization before transferring data. However, if there is no such protection, there are some exceptions where data can still be transferred (Article 28-31).	Yes, the data controller should ensure adequate safeguards and obtain approval from the authority. However, in absence of this, there are a few exceptions.	Not required if the authority had approved the transfer and there are adequate safeguards in place, otherwise, data can be transferred if the transfer is one-off, not massive, and the data subject has expressly consented to the transfer. Transfers would also be allowed for one of the following reasons: to safeguard the life of the person, protect the public interest, comply with a legal claim, execute a contract (Article 29).
Tunisia	2004	In every case, the authorization of The National Authority for Protection of Personal Data is required before the transfer of personal data.	Yes, receiving country should have adequate measures in place.	Consent is required when the data is necessary for public authorities' missions, for public security or national defense, for criminal prosecutions, or for carrying out missions in accordance with the laws and regulations in force. However, if a data subject denies a transfer, the authority can overrule this when the transfer is necessary for the protection of the data subject's life, scientific or historic research, or the performance of a contract.
Uganda	2019	The Data Protection and Privacy Act 2019 states that for personal data to be processed outside of Uganda, the other country must have adequate protective measures in place, or the data subject must consent.	Yes, adequate measures must be in place or the user will have to provide consent.	Yes, consent is necessary if adequate measures are not in place.
Zambia	2020	According to the Data Protection Law of 2020, data should be stored in Zambia, though the minister may make exceptions. User consent and certain other exceptions also apply.	Yes, the Minister considers whether the level of protection is adequate before allowing the transfer.	Not required, but it can be used to authorize the transfer.
Zimbabwe		Draft cybersecurity and data protection bill with similar provisions to those of other countries: data can be transferred to another country with such protection in place, or if the user consents, or there is an exception.	In the draft law, yes.	In the draft law, if no such protection is in place or no other exception exists then consent allows the transfer.

Agreement Officer's Representative:
Devi Ramkissoon, USAID
USAID, Center for Economics & Market Development
dramkissoon@usaid.gov
+1 (347) 866–6298

Project Director:
Brett Johnson, Palladium
Brett.Johnson@thePalladiumgroup.com
+1 (202) 777–0960

Technical Director:
Kati Suominen, Nextrade Group
Kati@nextradegroupllc.com
+1 (202) 294–8871

www.allianceforetradedevelopment.org

References

[1] "IDC's Global DataSphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data," IDC, May 8, 2020, https://www.idc.com/getdoc.jsp?containerId=prUS46286020.
[2] "Africa Startups," Crunchbase, Build Query: Organizations, accessed June 2021, https://www.crunchbase.com/search/organizations/field/hubs/org_num/africa-startups.
[3] Oliver Peckham, "Global DataSphere to Hit 59 Zettabytes in 2020 Alone, IDC Projects," Datanami, May 19, 2020, https://www.datanami.com/2020/05/19/global-datasphere-to-hit-59-zettabytes-in-2020-alone-idc-projects/
[4] "Onefi Case Study," Amazon Web Services, accessed November 2020, https://aws.amazon.com/solutions/case-studies/onefi/?did=cr_card&trk=cr_card.
[5] Kati Suominen, "Roadmap for Empowering Women-Led Firms in Ecommerce and the Digital Economy," Alliance for eTrade Development and US Agency for International Development (forthcoming in 2021).
[6] "How Vitality Works," Discovery, accessed June 2021, https://www.discovery.co.za/vitality/how-vitality-works
[7] "Kenyan Agri-Tech Startup Meets the Needs of Farmers Through Precision Agriculture," Microsoft Customer Stories, August 21, 2020, https://customers.microsoft.com/en-us/story/836844-sunculture-energy-azure-en-kenya
[8] "Visa Prevents Approximately $25 Billion in Fraud Using Artificial Intelligence," Visa Press Release, June 17, 2019, https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.16421.html.
[9] "VisaNet: The Technology Behind Visa," Visa, 2013, https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/visa-net-booklet.pdf.
[10] "Konga: Cutting Cloud Infrastructure Costs by Two-Thirds," Google Cloud Customers, accessed June 2021, https://cloud.google.com/customers/konga.
[11] "AWS Case Study: Travelstart," Amazon Web Services, accessed March 2019, https://aws.amazon.com/solutions/case-studies/travelstart/.
[12] "South African Bank Increases Agility and Productivity with Power BI and Azure," Microsoft Customer Stories, July 18, 2020, https://customers.microsoft.com/en-us/story/831695-standard-bank-banking-capital-markets-power-bi.
[13] Calestor Kizito Magero, "Safaricom: Harnessing the Power of APIs to Transform Lives in Africa," Google Cloud Blog, June 18, 2019, https://cloud.google.com/blog/products/api-management/safaricom-harnessing-the-power-of-apis-to-transform-lives-in-africa.
[14] 2020 Consumer Data Privacy Legislation, National Conference of State Legislatures, January 17, 2021, https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx.
[15] The CCPA applies to businesses that: (1) do business in the State of California; (2) collect California State resident personal information; and (3) have annual gross revenue of over $25 million; buy, receive, sell or share the personal information of 50,000 or more California residents, households or devices for commercial purposes each year; or derive 50 percent or more of annual revenue from selling consumer personal information. Virginia's law applies to entities that control or process personal data of at least 100,000 Virginia residents or derive over 50 percent of gross revenue from the sale of personal data (though the statute is unclear as to whether the revenue threshold applies to Virginia residents only) and control or process personal data of at least 25,000 Virginia residents.
[16] "CCPA vs the GDPR | Compliance with Cookiebot CMP," Cookiebot, accessed June 2021, https://www.cookiebot.com/en/ccpa-vs-gdpr/.
[17] Andrada Coos, "Data Protection in Japan: All You Need to Know about APPI," Endpoint Protector Blog, February 1, 2019, https://www.endpointprotector.com/blog/data-protection-in-japan-appi/.
[18] Esther Franks, Farhana Sharmeen, and Gen Huong Tan, "Extensive Changes to Singapore's Data Protection Regime Take Effect," JD Supra, February 16, 2021, https://www.jdsupra.com/legalnews/extensive-changes-to-singapore-s-data-5171045/.
[19] "Brazil," DLA Piper Data Protection Laws of the World, last modified January 28, 2021, https://www.dlapiperdataprotection.com/index.html?t=transfer&c=BR#:~:text=The%20Brazilian%20General%20Data%20Protection,Data%20Protection%20Act%20.
[20] Arjun Kharpal, "China's Tech Crackdown Has a New Battleground—Data," CNBC, July 5, 2021, https://www.cnbc.com/2021/07/05/china-tech-crackdown-focuses-on-data-after-didi-probe-.html; Jenny Sheng, Chunbin Xu, and Esther Tao, "China Adopts New Data Security Law," JD Supra, July 12, 2021, https://www.jdsupra.com/legalnews/china-adopts-new-data-security-law-8416153/.

[21] Jenny Sheng, Chunbin Xu, and Esther Tao, "China Adopts New Data Security Law," JD Supra, July 12, 2021, https://www.jdsupra.com/legalnews/china-adopts-new-data-security-law-8416153/.
[22] Arindrajit Basu, "The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam," The Diplomat, January 10, 2020, https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/.
[23] Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology & Innovation Foundation, July 19, 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost
[24] The Alliance for eTrade Development, which is funded by USAID, developed a similar taxonomy in 2018 and mapped 40 countries' adoption of different types of data privacy and transfer rules: Kati Suominen, *Expanding Developing Country Small Businesses' Use of Online Platforms for Trade* (Washington, DC: USAID, 2018), https://pdf.usaid.gov/pdf_docs/PA00TM8V.pdf.
[25] Arindrajit Basu, "The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam," The Diplomat, January 10, 2020, https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/; Tanwen Dawn-Hiscox, "Indonesia's Data Center Industry Protests Data Localization Reform," Data Center Dynamics, November 9, 2018, https://www.datacenterdynamics.com/en/news/indonesias-data-center-industry-protests-data-localization-reform/.
[26] Claudia Biancotti, "India's Ill-Advised Pursuit of Data Localization," Peter Institute for International Economics, December 9, 2019, https://www.piie.com/blogs/realtime-economic-issues-watch/indias-ill-advised-pursuit-data-localization.
[27] See, for example, Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization," CIGI and Chatham House, Paper Series 30, May 2016, https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf.
[28] Michael Nadeau, "General Data Protection Regulation (GDPR) Requirements, Deadlines and Facts," CSO Online, February 16, 2018, https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirementsdeadlines-and-facts.html.
[29] Oliver Smith, "The GDPR Racket: Who's Making Money From This $9bn Business Shakedown," Forbes, May 2, 2018, https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#38765ac234a2.
[30] "GDPR Burdens Hinder M&A Transactions in the EMEA Region, According to Merrill Corporation Survey," Merrill Corporation, press release, November 13, 2018, https://www.merrillcorp.com/us/en/company/news/press-releases/gdpr-burdens-hinder-m-a-transactions-in-the-emea-region.html.
[31] Deloitte, "Economic Impact Assessment of the European General Data Protection Regulation: Final Report," Deloitte, December 16, 2013, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-european-data-protection-tmt.pdf.
[32] Heli Koski and Nelli Valmari, "Short-Term Impacts of the GDPR on Firm Performance," ETLA, Working Paper 77, February 25, 2020, http://pub.etla.fi/ETLA-Working-Papers-77.pdf
[33] Jian Jia, Ginger Zhe Jin, and Liad Wagman, "The Short-Run Effects of the GDPR on Technology Venture Investment," NBER Working Paper 25248, November 2018, https://www.nber.org/papers/w25248
[34] Samuel, Goldberg, Garrett Johnson, and Scott Shriver, "Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic and E-Commerce Outcomes," Economics of Digitization Summer Institute Meeting, July 17, 2019, https://dx.doi.org/10.2139/ssrn.3421731.
[35] Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization," Centre for International Governance Innovation and Chatham House Paper Series 30, May 2016, https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf.
[36] Mona Farid Badran and Rizwan Tufail, "Economic Impact of Data Localization in 5 Selected African Countries, an Empirical Study," Working Paper, March 2019, https://pic.strathmore.edu/wp-content/uploads/2019/03/PIC_RANITP_Economic_Impact_of_Data_Localization_in_5_selected_African_Countries.pdf; Kyu Yub Lee, Moonhee Cho, Jungu Kang, and Minji Kang, "Welfare Effects of the EU the GDPR and Data Localization Measures," World Economy Brief 9(7), April 3, 2019, https://think-asia.org/bitstream/handle/11540/9995/WEB19-07.pdf?sequence=1.
[37] Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization," Centre for International Governance Innovation and Chatham House Paper Series 30, May 2016, https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf.

[38] Martina F. Ferracane, Janez Kren, and Erik van der Marel, "The Cost of Data Protectionism," Vox, October 25, 2018, https://voxeu.org/article/cost-data-protectionism
[39] Kyu Yub Lee, Moonhee Cho, Jungu Kang, and Minji Kang, "Welfare Effects of the EU the GDPR and Data Localization Measures," World Economy Brief 9(7), April 3, 2019, https://think-asia.org/bitstream/handle/11540/9995/WEB19-07.pdf?sequence=1.
[40] V. Sridhar, Sai Rakshith Potluri, and Shrisha Rao, "Effects of Data Localization on Digital Trade: An Agent-Based Modeling Approach," Telecommunications Policy 44, no. 9 (October 2020), https://doi.org/10.1016/j.telpol.2020.102022.
[41] "Digital Trade in the US and Global Economies, Part 2," United States International Trade Commission, August 2014, https://www.usitc.gov/publications/332/pub4485.pdf.
[42] Kalika Likhi, "India's Data Localization Efforts Could Do More Harm Than Good," Atlantic Council Blog, February 1, 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/india-s-data-localization-efforts-could-do-more-harm-than-good/.
[43] Arindrajit Basu, Elonnai Hickok, and Aditya Singh Chawla, "The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India," The Centre for Internet and Society, India, March 19, 2019, https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf
[44] Claire Scharwatt, "The Impact of Data Localisation Requirements on the Growth of Mobile Money-Enabled Remittances," GSMA, March 2019, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation.pdf.
[45] Hosuk Lee-Makiyama, Badri Narayanan, and Simon Lacey, "Cross-Border Data Flows: The Impact of Data Localisation on IoT," GSMA, January 2021, https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf.
[46] Hosuk Lee-Makiyama, Badri Narayanan, and Simon Lacey, "Cross-Border Data Flows: The Impact of Data Localisation on IoT," GSMA, January 2021, https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf.
[47] Cynthia J. Rich, "Out of Africa (and the Near East): Privacy Rules Come at Rapid Pace," Morrison Forrester Client Alert, January 11, 2021, https://www.mofo.com/resources/insights/210111-africa-near-east-privacy-rules.html.
[48] Cynthia J. Rich, "Out of Africa (and the Near East): Privacy Rules Come at Rapid Pace," Morrison Forrester Client Alert, January 11, 2021, https://www.mofo.com/resources/insights/210111-africa-near-east-privacy-rules.html.
[49] Cynthia J. Rich, "Out of Africa (and the Near East): Privacy Rules Come at Rapid Pace," Morrison Forrester Client Alert, January 11, 2021, https://www.mofo.com/resources/insights/210111-africa-near-east-privacy-rules.html.
[50] Christophe Fichet, "Morocco—Data Protection Overview," OneTrust DataGuidance, February 2021, https://www.dataguidance.com/notes/morocco-data-protection-overview.
[51] "Ghana's DPC Lists Companies Failing to Register Under Data Protection Act, 2012," iapp, June 30, 2017.
[52] "New Interactive Registry for Data Controllers Launched," GhanaWeb, October 9, 2020, https://www.ghanaweb.com/GhanaHomePage/business/New-interactive-registry-for-data-controllers-launched-1081219.
[53] "The Data Protection Commission Launches New Registration and Compliance Software and Announces Amnesty," Ministry of Communications and Digitalisation, Republic of Ghana, accessed July 14, 2021, https://www.moc.gov.gh/data-protection-commission-launches-new-registration-and-compliance-software-and-announces-amnesty
[54] Tanya Gaye, "Benin—Data Protection Overview," OneTrust DataGuidance, June 2021, https://www.dataguidance.com/notes/benin-data-protection-overview.
[55] Tanya Gaye, "Benin—Data Protection Overview," OneTrust DataGuidance, June 2021, https://www.dataguidance.com/notes/benin-data-protection-overview.
[56] "Rapport annuel d'activités 2018," Autorité de Protection des Données à Caractère Personnel, République du Bénin, 2018, https://apdp.bj/wp-content/uploads/2019/10/rapport-annuel-dactivit%C3%A9s-APDP-2018.pdf
[57] "Recent Developments on Data Privacy and Protection in Kenya," JDSupra, March 16, 2021, https://www.jdsupra.com/legalnews/recent-developments-on-data-privacy-and-1051513/#:~:text=The%20ODPC%20has%20been%20set,appointed%20on%2016%20November%202020.

[58] "Legal Alert: Kenyan Data Commissioner Issues New Draft Data Protection (General) Regulations, 2021," TripleOKLaw Advocates, accessed July 15, 2021, https://tripleoklaw.com/kenyan-draft-data-protection-general-regulations/.
[59] "Nigeria: One Year of the Data Protection Regulation," OneTrust Data Guidance, February 2020, https://www.dataguidance.com/opinion/nigeria-one-year-data-protection-regulation.
[60] "Data Protection Compliance Organisation," National Information Technology Development Agency of Nigeria, August 23, 2019, https://nitda.gov.ng/data-protection/.
[61] "Nigeria Data Protection Regulation 2019," National Information Technology Development Agency of Nigeria, https://ndpr.nitda.gov.ng/Content/Doc/NigeriaDataProtectionRegulation.pdf.
[62] "NITDA to Issue Notices of Data Protection Non-Compliance to 100 Firms," CommunicationsWeek, December 13, 2019, https://www.nigeriacommunicationsweek.com.ng/nitda-issues-100-firms-data-protection-non-compliance-notice/.
[63] "NITDA Extends Deadline for Filing of 2020/21 Data Audit Report," Jackson, Etti & Edu, March 24, 2021, https://jee.africa/nitda-extends-deadline-for-filing-of-2020-21-data-audit-report/.
[64] "Egypt's Data Protection Law Enters into Force," Clyde&Co, October 19, 2020, https://www.clydeco.com/en/insights/2020/10/egypt-s-data-protection-law-enters-into-force.
[65] "Egypt's Data Protection Law Enters into Force," Clyde&Co, October 19, 2020, https://www.clydeco.com/en/insights/2020/10/egypt-s-data-protection-law-enters-into-force.
[66] "Uganda's Draft Data Protection and Privacy Regulations," Collaboration on International ICT Policy for East and Southern Africa (CIPESA), September 2020, https://cipesa.org/?wpfb_dl=420.
[67] In 2020, 69% of the population above the age of 16 in the EU had heard about the GDPR, and 71% of people heard about their national data protection authority, according to the EU Fundamental Rights Agency.
[68] Deloitte, "A New Era for Privacy: GDPR Six Months On," 2018, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf.
[69] Information Commissioner's Office, "ICO Deputy Commissioner (Operations) James Dipple-Johnstone—Speech to the CBI Cyber Security: Business Insight Conference," ICO, September 12, 2018, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/cbi-cyber-security-business-insight-conference/.
[70] Josephine Wolff and Nicole Atallah. 2021. "Early GDPR Penalties: Analysis of Implementation and Fines through May 2020," *Journal of Information Policy* 11: 63–103, https://www.jstor.org/stable/10.5325/jinfopoli.11.2021.0063.
[71] See, for example, Ross McKean, Ewa Kurowska-Tober, and Heidi Waem, "DLA Piper GDPR Fines and Data Breach Survey: January 2021," DLA Piper, January 19, 2021, https://www.dlapiper.com/en/uk/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/.
[72] Dan Cooper, Kristof Van Quathem, Nicholas Shepherd, and Anna Oberschelp de Meneses, "European Commission Publishes 2-Year Report on the Implementation of the GDPR," Inside Privacy Blog, Covington, June 25, 2020, https://www.insideprivacy.com/eu-data-protection/european-commission-publishes-2-year-report-on-implementation-of-the-gdpr/.
[73] Brave, "Europe's Governments are Failing the GDPR: Brave's 2020 Report on the Enforcement Capacity of Data Protection Authorities," 2020, https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf.
[74] Brave, "Europe's Governments are Failing the GDPR: Brave's 2020 Report on the Enforcement Capacity of Data Protection Authorities," 2020, https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf.
[75] African Union, "African Union Convention on Cyber Security and Personal Data Protection," June 24, 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.
[76] African Union, "African Union Convention on Cyber Security and Personal Data Protection," June 24, 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.
[77] African Declaration on Internet Rights and Freedoms Coalition, "Privacy and Personal Data Protection in Africa a Rights-Based Survey of Legislation in Eight Countries," May 2021, https://www.apc.org/sites/default/files/PrivacyDataProtectionAfrica_CountryReports.pdf.
[78] "Personal Data Protection Guidelines for Africa: A Joint Initiative of the Internet Society and the Commission of the African Union," May 9, 2018, https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf.
[79] ECOWAS, "Supplementary Act/SA. 1/01/10 on Personal Data Protection within ECOWAS," Thirty-Seventh Session of the Authority of Heads of State and Government, Abuja, February 16, 2010, https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf.
[80] Tomiwa Ilori, "Data Protection in Africa and the COVID-19 Pandemic: Old Problems, New Challenges and Multistakeholder Solutions," Association for Progressive Communications, June 15, 2020,

https://africaninternetrights.org/sites/default/files/Tomiwa%20Ilori_AfDec_Data%20protection%20in%20Africa%20and%20the%20COVID-19%20pandemic_Final%20paper.pdf
[81] "Chapter Fifteen: Electronic Commerce," US–Korea Free Trade Agreement, revised 2019, https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf.
[82] See ASEAN, "ASEAN Model Contractual Clauses for Cross Border Data Flows," 2021, https://asean.org/storage/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.
[83] Gabriela Kennedy and Karen H.F. Lee, "Finding Harmony: ASEAN Model Contractual Clauses and Data Management Framework Launched," Mayer Brown, February 8, 2021, https://www.mayerbrown.com/en/perspectives-events/publications/2021/02/finding-harmony-asean-model-contractual-clauses-and-data-management-framework-launched.
[84] "Chapter Fourteen: Electronic Commerce," Singapore–Australia Digital Economy Agreement 2020, https://www.enterprisesg.gov.sg/-/media/esg/files/non-financial-assistance/for-companies/free-trade-agreements/Singapore-Australia-FTA/Legal-text/Chapter-14/Chapter-14-Electronic-Commerce.
[85] "Nuevo Acuerdo de Comercio Electrónico del Mercosur," Marval O'Farrell Mairal, April 27, 2021, https://www.marval.com/publicacion/nuevo-acuerdo-de-comercio-electronico-del-mercosur-13969.
[86] "Cambodia, Lao PDR, and Myanmar shall not be obliged to apply this paragraph for a period of five years after the date of entry into force of this Agreement, with an additional three years if necessary. Viet Nam shall not be obliged to apply this paragraph for a period of five years after the date of entry into force of this Agreement." "Chapter 12: Electronic Commerce," Regional Comprehensive Economic Partnership, https://rcepsec.org/wp-content/uploads/2020/11/Chapter-12.pdf
[87] United States Department of Justice, "US And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online," press release, October 3, 2019, https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists#:~:text=The%20United%20States%20and%20the,and%20cybercrime%2C%20directly%20from%20tech.
[88] These agreements allow each party's law enforcement agencies to demand electronic data regarding serious crimes held by electronic communication service remote or computing services providers. However, the scope of each agreement is subject to negotiations. Regarding the US–UK agreement, both parties agreed to broadly lift restrictions for investigations and to assure providers that disclosure through the agreement are compatible with data protection laws. The US Department of Justice stated that each party "committed to obtain permission from the other before using data gained through the agreement in prosecutions relating to a party's essential interest—specifically, death penalty prosecutions by the United States and UK cases implicating freedom of speech." ACLU and civil rights groups argue that the law lowers the evidentiary threshold required for foreign countries to obtain data stored in the US. See Mathias Avocats, "First Cloud Act Agreement signed by the US and the UK," October 3, 2019, https://www.avocats-mathias.com/actualites/cloud-act-agreement-signed
[89] To be sure, these arrangements have generated questions from civil society and human rights organizations that fear that data requests undermine the US Constitution's Fourth Amendment rights against unreasonable searches and seizures and entice some foreign governments to act in bad faith to seize their own citizens' data on US servers. Jackie Watters, "Microsoft Email Privacy Case No Longer Needed; DOJ Says," CNN, March 31, 2018, https://money.cnn.com/2018/03/31/technology/microsoft-lawsuit-supreme-court-justice-department/index.html
[90] See Kati Suominen, Erica Vambell, and Mariah Furtek, "Expanding MSME Ecommerce in Developing Countries: State of Policies and Path Forward," Policy Report for USAID, 2021 (forthcoming), https://www.allianceforetradedevelopment.org/ecommerce-policy-report-index.
[91] Abraham Diaz, "Data Security and Cybercrime in Mexico," Olivares https://www.lexology.com/library/detail.aspx?g=4fcfea5a-0d5f-4702-9925-917c98db9877
[92] "Chapter 19: Digital Trade," US–Mexico–Canada Agreement, 2020 https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf
[93] "Comparison of Selected Digital Trade Provisions in the United States-Mexico-Canada Agreement (USMCA) and the Trans-Pacific Partnership (TPP)," BSA | The Software Alliance, accessed July 7, 2021, https://www.bsa.org/files/policy-filings/04112019tppvusmcacomparison.pdf
[94] "Chapter 19: Digital Trade," US–Mexico–Canada Agreement, 2020 https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf
[95] "What Is the Cross-Border Privacy Rules System?" Asia-Pacific Economic Cooperation accessed July 6, 2021, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

[96] Joan Stewart, "The USMCA's Impact on Digital Trade and Data Transfers," Wiley Newsletter, March 2020, https://www.wiley.law/pp/newsletter-Mar-2020-PIF_The_USMCAs_Impact_on_Digital_Trade_and_Data_Transfers.pdf?22478
[97] "CIPL Issues White Paper on the USMCA's Impact on US Federal Privacy Law," Hunton Andrews Kurth Blog, January 17, 2020, https://www.huntonprivacyblog.com/2020/01/17/cipl-issues-white-paper-on-the-usmcas-impact-on-federal-privacy-law/
[98] Josh Harris, "Why CBPR Recognition in the USMCA Is a Significant Development for Privacy," iapp, October 10. 2018 https://iapp.org/news/a/why-cbpr-recognition-in-the-usmca-is-a-significant-development-for-privacy/.
[99] Josh Harris, "Why CBPR Recognition in the USMCA Is a Significant Development for Privacy," iapp, October 10. 2018 https://iapp.org/news/a/why-cbpr-recognition-in-the-usmca-is-a-significant-development-for-privacy/.
[100] USMCA adds a clause that "A measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party."
[101] Nate Lore, "What Is Data Encryption? Definition, Best Practices, and More," Digital Guardian, December 1, 2020, https://digitalguardian.com/blog/what-data-encryption.
[102] See Nataraj Nagaratnam, "Confidential Computing," IBM Cloud Learn Hub, October 16, 2020, https://www.ibm.com/cloud/learn/confidential-computing: "The contents of the enclave—what data is being processed and how—can only be accessed with an authorized programming code, which is invisible and unknowable to anything or anyone else, including the cloud provider. This not only secures data in use and transit—it also helps protect firms' IP and can encourage companies to tap new efficiencies as they can move more of the sensitive data and workloads to public cloud services."
[103] "Multicloud Data Security Trends Noted in Gartner Hype Cycle for Cloud Security, 2020," Businesswire, September 2, 2020, https://www.businesswire.com/news/home/20200902005282/en/Multicloud-Data-Security-Trends-Noted-in-Gartner-Hype-Cycle-for-Cloud-Security-2020.
[104] "Gartner Report: Top Strategic Technology Trends for 2021: Privacy-Enhancing Computation," R3 Report, April 2021, https://www.r3.com/gartner-2021-privacy-enhancing-computation/.
[105] Tom Merritt, "Top 5 Things to Know About Confidential Computing," TechRepublic, October 5, 2020, https://www.techrepublic.com/article/top-5-things-to-know-about-confidential-computing/.
[106] Keri Allan, "Confidential Computing—The Next Frontier in Security," ITPro, March 18, 2021, https://www.itpro.com/security/encryption/358941/confidential-computing-the-next-frontier-in-security.
[107] See "Confidential Computing Deep Dive v1.0," The Confidential Computing Consortium, October 2020, https://confidentialcomputing.io/wp-content/uploads/sites/85/2020/10/Confidential-Computing-Deep-Dive-white-paper.pdf; "Trusted Platform Module (TPM) Summary," Trusted Computing Group White Paper, accessed July 9, 2021, https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary.