United States International Trade Commission
Journal of International Commerce and Economics
February 2021

# Data Protection Laws in Africa: A Pan-African Survey and Noted Trends

Brian Daigle

***Abstract***

As the 55 African countries of the African Union (AU) move towards greater integration of trade policies through the African Continental Free Trade Agreement (AfCFTA), one area of noted trade policy divergence is the governance of digital trade. In particular, African nations' rules governing the protection of personal data are a patchwork, with some countries offering little to no protection policy while others have extensive digital governance frameworks. Given that internet connectivity, broadband access, and digital trade have coincided with broader economic development, the extent to which African nations form policies governing the digital landscape can also shape development across the whole continent. This paper explores how personal data are currently governed among AU member states, noting common trends and areas of divergence. It also takes a closer look at the data protection policies of Egypt, Kenya, Botswana, Ghana, and Rwanda.

Suggested citation: Daigle, Brian. "Data Protection Laws in Africa: A Pan-African Survey and Noted Trends." *Journal of International Commerce and Economics*, February 2021. https://www.usitc.gov/journals.

The author would like to thank the two anonymous referees for their comments on earlier versions of this paper.

# Introduction

Many of the 55 states of the African Union have spent considerable efforts to update and amend laws and regulations to encourage the establishment of a larger digital trade economy, both within countries and between African nations. These efforts include updating—or in some cases creating—laws which govern the protection and privacy of personal data. This interest in creating data protection laws for a 21st-century digital landscape extends far beyond the African Union, to countries as diverse as Japan, Israel, Canada, Brazil, and India. In addition, within the United States several states are either amending or drafting legislation to govern the protection of personal data online.

The proliferation of regulatory changes around the world—particularly the 2016 General Data Protection Regulation (GDPR)[1] of the European Union (EU)—has likely spurred increased interest in the regulation and governance of personal data throughout Africa. Also, the economies of both Africa and the EU have a strong interest in preserving the free flow of personal data between them. In Africa, the significance of GDPR is potentially more far-reaching than in other regions, due in part to the gaps in some countries' current governance of data protection: either data protection laws that were established several years ago must be updated to align with data protection laws in other economies, or no data protection laws exist at all. Such gaps, however, have given countries opportunities to leapfrog into establishing more robust data protection structures by benefiting from the trial-and-error of previous decades while other countries were establishing data protection laws within a shifting digital landscape.

Despite the policy gaps, African countries have shown significant interest in establishing data protection and data privacy laws, both in comments by policymakers and draft legislation in several AU countries. At the AU level, the 2014 Malabo Convention on Cybersecurity and Personal Data Protection called for the adoption of a common framework on the protection of data. In addition, the absence of a common data protection policy in the upcoming African Continental Free Trade Agreement (AfCFTA) has been noted as a potential hindrance to establishing a common market for pan-African trade in digital goods and services.[2] At the country level, in 2019 Kenya, Nigeria, Togo, and Uganda enacted data protection policies. They were followed by Egypt, which in April 2020 became the most recent AU member to create a data protection framework with its Personal Data Protection Law. Next came South Africa, whose Protection of Personal

[1] In 2016, the European Union (EU) promulgated EU Regulation 2017/679. Also known as the EU General Data Protection Regulation (GDPR), this regulation reshaped the governance of personal data in the EU. It created new mechanisms for EU member states to enact fines for noncompliance with data protection principles and created EU-wide boards to govern implementation and disputes among EU member states on enforcement. Further information can be found in Brian Daigle and Mahnaz Khan, "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities," Journal of International Commerce and Economics, April 2020. https://www.usitc.gov/sites/default/files/publications/332/journals/jice_gdpr_enforcement.pdf.

[2] Moshood, Ibrahim, and Solagbade Sogbetun, "The Impact of Data Protection Rules on the Digital Economy Aspect of the African Continental Free Trade Agreement (AFCFTA)," ALP, n.d. (accessed December 17, 2020).

Information Act came into force in June 2020. Other countries are amending existing data protection policies or working to establish structures to enforce existing laws and regulations.

This paper explores these recent trends in the establishment of data protection and privacy laws. It will begin with an overview of the digital trade market in Africa, looking at the significant growth potential of several subsectors of the African digital economy. It continues with a survey and analysis of all African nations and their respective data protection policy status, noting the countries that have adopted data protection laws, those that have not, and those that have adopted data protection policies since the adoption of GDPR in 2016. This section also includes case studies of the data protection laws of Egypt, Kenya, Ghana, Botswana, and Rwanda. The paper concludes with an exploration of the possible trade implications of this patchwork of data protection and privacy laws, noting the position of U.S. industries in this field.

# The Digital Trade Market in Africa

The digital trade market in Africa is characterized by significant growth, though operating with a smaller market than those in Europe, Asia, and North America. Africa's entire e-commerce market, for example, was valued at $19.8 billion in 2020, while the e-commerce market in France was valued at $54 billion that same year.[3] Africa's digital advertising market (sometimes viewed as a proxy for the social media market) was valued at $5.5 billion in 2020, while in Europe it was $70 billion.[4]

One example of the growth of the digital trade market in Africa is the expansion of ridesharing and ride-hailing, which relies on mobile applications (apps). This market is estimated to grow about 20 percent annually until 2023, reaching $1.1 billion that year with 11.2 percent consumer penetration.[5] An analysis of the ride hailing market in Uganda specifically noted that formalizing the industry there could lead to 1 million formalized jobs in a country of 43 million people.[6]

Additionally, the increasing availability of mobile broadband in Africa is aligning with that of other continents and is currently one of the fastest growing among major global regions.[7] In 2019, Africa surpassed North America, South America, and the Middle East in the number of daily internet users, though the level of internet usage is lower than in these other regions.[8] However, internet penetration varies substantially by country. More than 80 percent of Kenyans use the internet at least once a month, while in Nigeria that figure, in 2019, was about 60 percent.[9] The

[3] Statista, "eCommerce Africa," n.d. (accessed October 16, 2020); Statista, "eCommerce France," n.d. (accessed October 16, 2020).
[4] Statista, "Digital Advertising: Africa," n.d. (accessed October 16, 2020; Statista, "Digital Advertising: Europe," n.d. (accessed October 16, 2020).
[5] TechSci Research, "Middle East and Africa Ride Hailing Market 2017–2023," October 2018.
[6] Henry, Nzekwe, "A Rare Win Is Coming for Regulation-Hit Ride-Hailing in Africa," Wee Tracker, May 11, 2020.
[7] GSMA, "Connected Society: The State of Mobile Internet Connectivity 2019," 2019, 5-8.
[8] Council on Foreign Relations, "Last Month, Over Half a Billion Africans Accessed the Internet," July 25, 2019.
[9] The World Bank estimates that individual use of the internet as a share of the population is lower with Kenya at 17.8 percent in 2017 and Nigeria at 7.4 percent that year. World Bank, "Individuals using the Internet (% of

market penetration rate across the continent was approximately 40 percent, though that figure is growing.[10]

Even with robust digital trade growth and development, there are still significant barriers to the development of digital trade markets in Africa, ranging in form from structural to regulatory. Among the structural barriers, infrastructure for telecommunications remains problematic despite substantial improvements since the early 2000s, when many African countries' internet penetration rates were less than 5 percent.[11] The deregulation of many telecommunications monopolies and the creation of telecommunications infrastructure and services regulators have contributed to the expansion of telecommunications infrastructure and services throughout the region (though at lower levels than in other developing markets).[12] Despite these improvements, one 2019 report estimated that sub-Saharan Africa accounts for 40 percent of the world population not currently covered by a mobile broadband network.[13]

Regulatory barriers can also hamper the development of digital trade in several African markets. These hindrances can include the forced localization of data in certain countries (in particular Nigeria);[14] restrictions on ride-hailing/ridesharing applications (apps) and services (notably in Kenya, South Africa, and Egypt);[15] and e-commerce restrictions introduced during the COVID-19 outbreak (like those in South Africa).[16] Additionally, only four African nations—Egypt, Mauritius, the Seychelles, and Morocco—are members of the Information Technology Agreement (ITA),[17] a 1997 trade agreement that lowered or removed tariffs on technology goods. The ITA currently counts among its signatories the United States, the EU, China, Russia, and covers more than 95 percent of the world market for information technology products.[18] If they do not accede to this agreement (or liberalize technology tariffs outside the agreement), many African nations face tariff barriers to the importation of technology products ranging from cell towers and cables to smartphones and routers. Among the 4 AU member states currently in the ITA, only Mauritius is a member of the ITA's 2015 expanded list of tariff-free products, which added dozens of electronic products to the list of items covered by the ITA's zero-tariff coverage. The expanded

population)-Nigeria" (accessed February 5, 2021); World Bank, "Individuals using the Internet (% of population)-Kenya" (accessed February 5, 2021); Council on Foreign Relations, "Last Month, Over Half a Billion Africans Accessed the Internet," July 25, 2019.

[10] Council on Foreign Relations, "Last Month, Over Half a Billion Africans Accessed the Internet," July 25, 2019.

[11] CIPESA, "State of Internet Freedom in Africa 2019," September 2019, 8.

[12] CIPESA, "State of Internet Freedom in Africa 2019," September 2019, 8.

[13] GSMA, "Mobile Internet Connectivity 2019: Sub-Saharan Africa Factsheet," 2020.

[14] USTR, "2018 Fact Sheet: Key Barriers to Digital Trade," March 2019.

[15] Henry, Nzekwe, "A Rare Win Is Coming for Regulation-Hit Ride-Hailing in Africa," Wee Tracker, May 11, 2020.

[16] Xinhuanet, "Africa lifts ban on e-commerce under COVID-19 restrictions," May 15, 2020.

[17] Background information on the Information Technology Agreement can be found at the WTO Trade Topics site: https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm.

[18] ITA, "Trade Guide: WTO Information Technology Agreement," n.d. (accessed October 16, 2020).

list includes Japan, the United States, the EU, China, South Korea, and Taiwan, among others, as members.[19]

These regulatory and structural challenges have been somewhat offset by Africa's unique market conditions, which have provided numerous opportunities for creativity in the digital provision of goods and services. For example, the inability of many Africans to procure formal banking services has contributed to substantial growth in "mobile money," or mobile banking through online third-party intermediaries such as MTN Group Mobile Money. One firm estimates that the sub-Saharan Africa region accounts for nearly half (45.6 percent) of global mobile money activity occurring outside traditional banking structures.[20] In fact, Africa was one of the global leaders in the development of mobile money. Kenya rolled out a mobile-phone payment system as early as 2007—first operating through short message service (SMS) communications and later adding internet-based mobile payments—years before the widespread adoption of similar systems in the United States and Europe.[21]

A similar development is currently taking place in the ride-hailing and ridesharing market. In contrast to more developed market economies, many African ride-hailing markets have been characterized by extensive, bifurcated, and informal structures. One 2017 market report estimated that as a result of these structural traits, nearly 60 ride-hailing and ridesharing apps and startups were operating across Africa, with more entrants likely in the future.[22] With rising mobile phone penetration into the African economy, growth in this sector and other mobile phone-reliant sectors is likely to continue. For example, while it was estimated in 2018 that 39 percent of African consumers had adopted smartphones, this number was projected to rise to nearly two-thirds of consumers by 2025.[23]

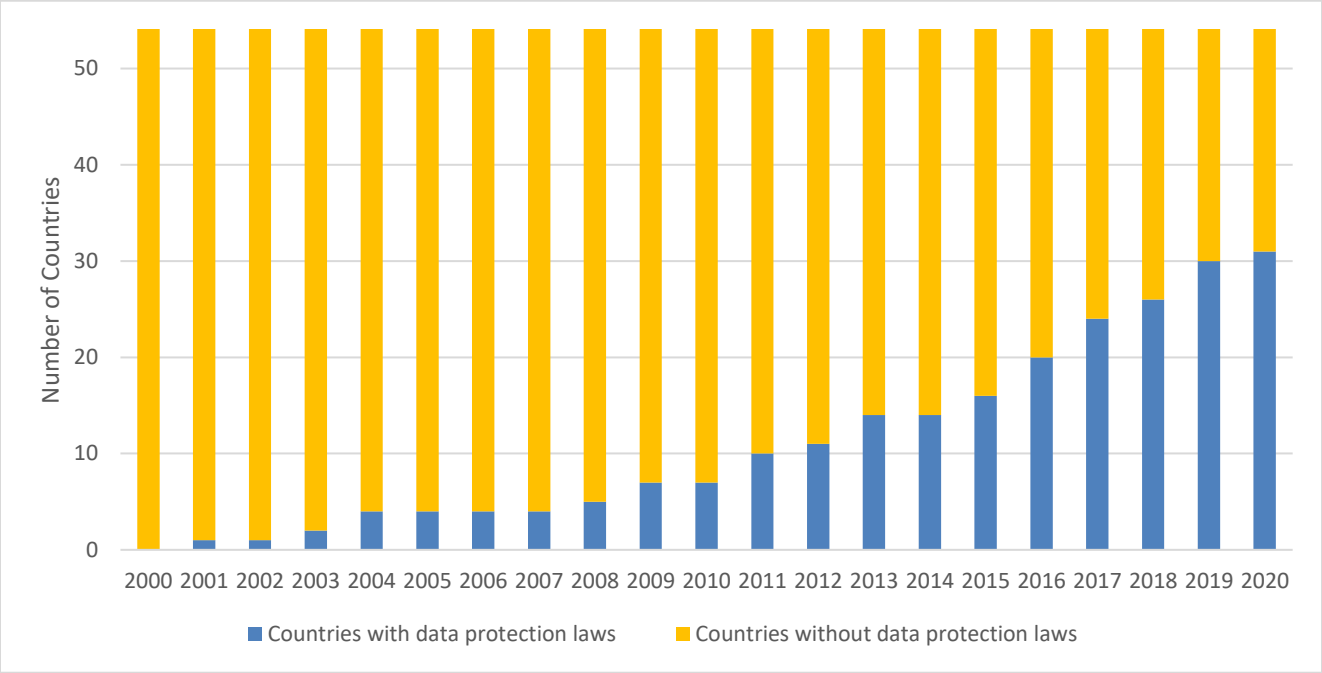
Finally, the rise of urbanization in Africa, coupled with the development of a growing middle class, is contributing to the growth of Africa's digital trade economy.[24] Both within cities and across borders, digital solutions are being used with increasing frequency to facilitate the trade of goods and services, particularly through mobile phones.[25] The increasing urbanization of Africa and its growing middle class are also contributing to the development of startups in the region. The number of tech hubs in Africa grew by almost 50 percent between 2019 and 2020, concentrated in Mauritius, Kenya, South Africa, Egypt, Nigeria, Tunisia, and Ghana.[26]

[19] European Commission, "The Expansion of the Information Technology Agreement: An Economic Assessment," 2016, 16.
[20] Awosanya, Yinka, "Sub-Saharan Africa has 48.8% of the Total Active Mobile Money Accounts in the World," Tech Point Africa, February 27, 2019.
[21] Hughes, Nick, and Susie Lonie, "M-PESA: Mobile Money for the 'Unbanked' Turning Cellphones into 24-Hour Tellers in Kenya," Innovations, 2007, 1–3.
[22] Mourdoukoutas, Eleni, "Africa's app-based taxis battle Uber over market share," Africa Renewal, August 2017.
[23] GSMA, *State of the Industry Report on Mobile Money*, 2018.
[24] Ngatane, Nthakoana, "Digital Trade the Only Tool for Africa's Economic Recovery," *Eyewitness News*, May 5, 2020.
[25] Mene, Wamkele, "Digital trade is the next big thing in Africa," *Africa Renewal*, July 14, 2020.
[26] Net Imperative, "Digital Africa: Top 10 cities for start-ups," February 26, 2020.

# The Landscape of Data Protection Laws in Africa

The rise of so many digitally enabled markets in Africa means that more consumers are being asked to give access to their personal data, including financial, demographic, and geolocation facts. As a result, the regulations governing the protection of personal data are becoming increasingly important. While many countries across Africa have adopted rules governing a generalized right to privacy (often in their constitutions), the adoption of laws governing the protection of personal data in the region has gone more slowly. Before 2016 (the year GDPR was enacted), only 16 of 55 nations had adopted specific data protection laws.[27] However, as of August 2020, that number had quickly risen to 31 countries (figure 1).

Figure 1: Total African countries with data protection laws by year, 2000–2020

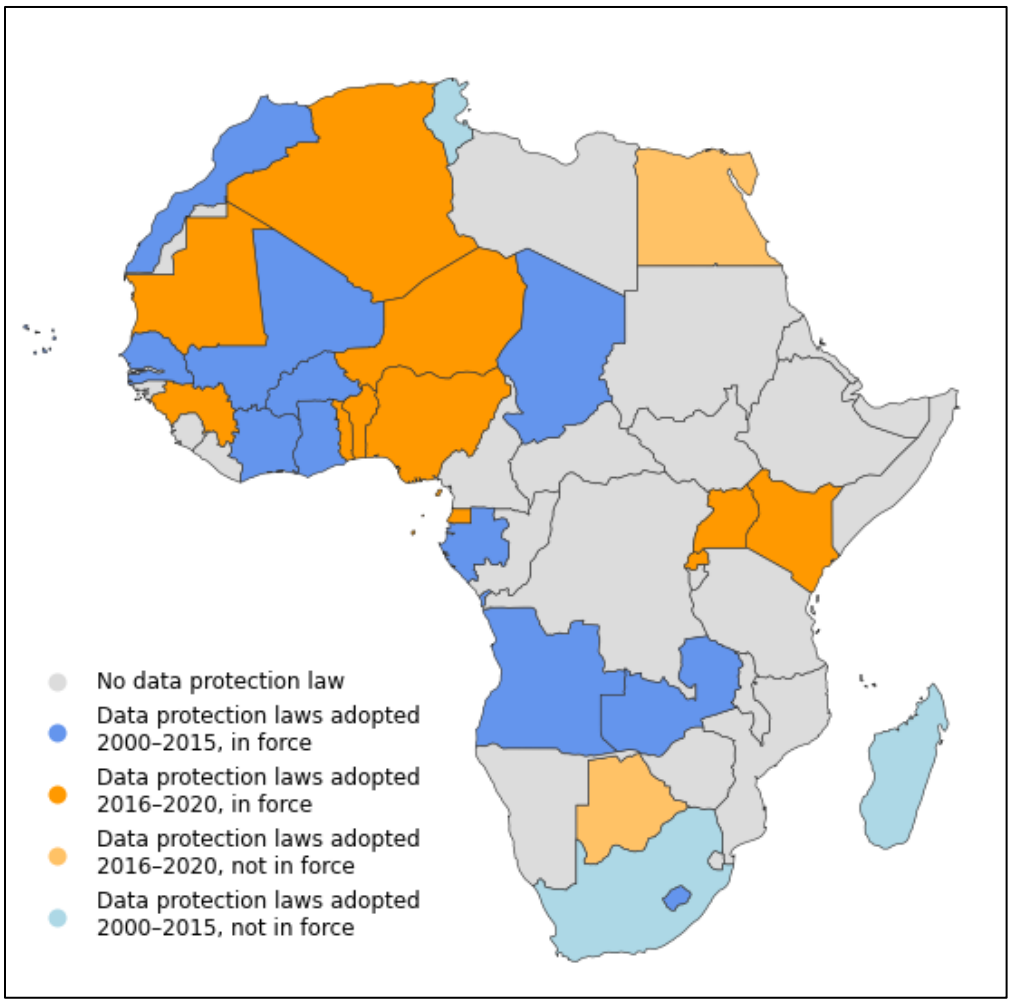



Note: The list of countries with data protection laws are those that have passed data protection laws. This includes countries with data protection laws which may not currently be in force or are only partially in force, as well as those currently in force. Sources were compiled by the author, and are noted in appendix A.

By 2019, most African nations had codified a data protection law, though some data protection laws are not yet in force; they often require the establishment of necessary regulations or regulatory authorities before enforcement (figure 2). Measured by GDP, a significant majority of the economy of the African Union is governed by data protection laws: in April 2020, with the addition of Egypt to the list of countries with data protection laws, more than 80 percent of the African economy was governed by such laws, either codified in law and in force or not yet in force (appendix A).

[27] These countries are Cabo Verde (2001), Seychelles (2003), Burkina Faso (2004), Tunisia (2004), Senegal (2008), Zambia (2009), Morocco (2009), Gabon (2011), Lesotho (2011), Angola (2011), Ghana (2012), Côte d'Ivoire (2013), Mali (2013), South Africa (2013), Chad (2015), and Madagascar (2015).

Figure 2: Status of national data protection laws in Africa, 2000–September 2020




Source: Compiled by author.

Regionally, the majority of West African countries have adopted data protection regulations, almost evenly split between laws adopted before and after GDPR's adoption in 2016. Many countries in Central and East Africa have not adopted any major data protection regulations, apart from Kenya, Uganda, and Rwanda. In Southern Africa, there is an uneven patchwork of regulations. Several countries (South Africa, Botswana, Madagascar) have adopted data protection laws that are not currently in force, and no major countries in Southern Africa have adopted a data protection law after GDPR's adoption. (South Africa is currently updating its data protection regulations, which were first promulgated in 2013.)

These laws differ substantially in a variety of ways. First, the scope of their coverage often diverges. So do definitions of what constitutes "personal" data (and whether there is a specific subset of "sensitive" personal data); the obligations of firms that hold or process personal data; and the structure of governance, such as whether to create a new enforcement agency or fold it into the responsibilities of an existing agency. Additionally, penalties for noncompliance vary; some countries require only fines for noncompliance, while others can remove a firm's legal ability

to process personal data or may hold noncompliant firms criminally liable. To illustrate these differences, the data protection laws of four countries—Mali, Mauritius, Nigeria, and Togo—are described briefly in table 1 (next page), reflecting divergences in how personal data are defined, the rights of data subjects, and the obligations of data controllers and data processors.[28] Additionally, more detailed case studies of other African data protection laws—Egypt, Kenya, Botswana, Ghana, and Rwanda—appear in the following section.

One noteworthy development affecting data protection laws established from 2016 onward is that several of these laws align closely with the regulatory standards of GDPR. In addition, some African countries have updated existing data protection laws following the publication of GDPR, with the explicit goal of aligning their existing privacy laws and frameworks with the EU data protection and privacy framework. In early 2019, Nigeria repealed its existing 2013 framework for the protection of personal data (the "Data Protection Guidelines") and replaced it with the Data Protection Regulation; also in 2019, Mauritius updated its 2004 data protection regulations with the Law 2019-014 Relating to the Protection of Personal Data. Both of these new regulations enshrine several major components of GDPR, in particular the rights of data subjects and the legal obligations of controllers and processors of personal data. In 2017, Benin, having replaced its existing 2009 data protection law, was described by one industry representative as having "enacted the most GDPR-like legislation outside the EU. Its 'Code du numérique' (enacted 13 June 2017) is a comprehensive 'cyberlaw' of more than 650 articles."[29]

[28] Controllers of personal data are defined as the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Processors are defined as a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

[29] Similarities between the Benin law and the EU GDPR include "extra-territorial application, privacy by design, direct liability of processors, data breach notification to the data protection authority (DPA) and to the data subject, approved codes of conduct, onus of proof on the data controller in most cases, detailed requirements for adequacy of the level of protection offered by third countries, data protection impact assessment, mandatory data protection officers, meaningful information required about the logic involved in automated data decisions, a right to data portability, and a right to be forgotten." Greenleaf, Graham, "Global Data Privacy Laws 2019: 132 National Laws a& Many Bills," *Privacy Laws & Business International Report,* February 8, 2019, 4.

**Table 1: Data protection laws in Mali, Mauritius, Togo, and Nigeria**

| Country | Name of Law | Year | Personal Data Definition | Sensitive Data Provision | Rights of Data Subject | Selected rules for controllers and processors | Specific Agency | Enforcement penalties |
|---|---|---|---|---|---|---|---|---|
| **Mali** | Law No. 2013-015 on the Protection of Personal Data | 2013 | Race, ethnicity, political/philosophical/religious opinions, health or sexual life, prosecutions, criminal or administrative sanctions | Yes | Right to know identity of controller, purposes of processing, type of data processed, recipients of data, right to object, and access data, details of transfer, duration of processing. | Processor must notify of data processing prior to processing, data controller must ensure data security | Yes: Malian Data Protection Authority (APDP) | Fines and imprisonment |
| **Mauritius** | Data Protection Act (updated from 2004 law) | 2017 | Any information relating to a data subject. | Yes | Right to know of processing and to receive copy of data, right to revision, right to erasure, controller must inform subject of processing and reason for processing, right to learn criteria for determining how long data are kept. | Processor and controller must register with agency, all processing actions recorded. Controller has burden of proof establishing consent. Must conduct DPIA. Written agreement between controller and processor required. | Yes: Data Protection Commissioner | Fines and imprisonment |
| **Togo** | Law 2019-014 Relating to the Protection of Personal Data | 2019 | Any information relating to a person's ID number or physical, physiological, genetic, psychological, cultural, social, or economic identity. | Yes | Data subject must give consent, right to know identity of controller and purposes for processing data, right to object, recipient of data, right to erasure and rectification, information on transfers to foreign countries. | Controller must ensure that identity of third parties to whom data are transmitted can be verified and prevent unauthorized disclosures. Processing on behalf of controller requires written contract. Data protection office must be appointed. | Yes: Togo Data Protection Authority (IPDCP) | Fines and imprisonment |
| **Nigeria** | Nigeria Data Protection Regulation 2019 | 2019 | ID number, location data, an online identifier of any physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. | Yes | Data subject has right to request information on use of data, provide data to subject, period data will be stored, can withdraw consent at any time, lodge complaints with authority, information on out-of-country transfers. | Privacy policy of firm must be clearly noted, and firms must take security measures to protect data. Transfers out of Nigeria allowed only in certain circumstances. DPO must be appointed, audit of privacy practice | National Information Technology Development Agency | Fines |

# Case Studies

The following case studies, on Egypt, Kenya, Botswana, Ghana, and Rwanda, show a diverse array of data protection laws adopted between 2000 and 2020. The case studies reveal the breadth of legal complexities and detail of Africa's data protection laws while highlighting regional diversity and reflecting the different periods in which these laws were adopted, examining laws before GDPR (Ghana), after GDPR (Egypt, Kenya, and Botswana), and currently in draft form (Rwanda).

# Ghana

The government of Ghana enacted its Data Protection Act in 2012.[30] In contrast to many of the data protection regulations which followed the adoption of GDPR in 2016, the Ghanaian regulation offers a more flexible framework in defining both personal data and the parameters around the legal processing of data. This contrasts with the more prescriptive standards adopted by many African countries following the adoption of GDPR.

The Ghana Data Protection Act (DPA) has several elements which distinguish it from the standards adopted by other African countries between 2001 and 2016. First, it gives the Ghana Communications Ministry the authority to specify whether legal processing has occurred if the processing is likely to (1) cause damage to the data subject, or (2) to prejudice the rights of the data subject.[31] Second, it creates a register of data controllers under the Data Protection Commission for firms that qualify as controllers entitled to hold personal data—this exists in some, though not all, African nations with data protection regulations.[32] Finally, the Ghana Data Protection Act applies to both state and public authorities in addition to private firms (the Act qualifies government departments as data controllers).[33]

The Ghana DPA applies to data controllers and processors in several circumstances, in recognition of the fluidity of the movement of data that are hosted and moved online. The regulations and obligations of the Ghana DPA apply in instances where the data controller is established within Ghana or the data are processed in Ghana; where the controller is not established in-country but uses equipment or a data processor to carry out business within Ghana; or where the processing of the information outside Ghana consists of data wholly or partly derived from data originating in Ghana. This comprehensive framework for data governance, recognizing the fluidity of data flows across markets, is unique among data protection regulations across Africa, but closely aligns with EU regulations.[34] Additionally, the Ghanaian data protection regulation distinguishes between obligations for both data processors and data controllers, while in many jurisdictions only data controllers have specific data protection obligations.[35]

[30] Data Guidance, "Ghana Data Protection Overview," OneTrust, December 2019.
[31] Data Guidance, "Ghana Data Protection Overview," OneTrust, December 2019.
[32] Data Guidance, "Ghana Data Protection Overview," OneTrust, December 2019.
[33] Data Guidance, "Ghana Data Protection Overview," OneTrust, December 2019.
[34] Data Guidance, "Ghana Data Protection Overview," OneTrust, December 2019.
[35] Data Guidance, "Ghana Data Protection Overview," OneTrust, December 2019.

In terms of data subject rights, the Ghana data protection regulations follows some African data privacy laws and EU regulations by defining both personal data and "sensitive" personal data, the latter of which falls under stricter regulations. Processing both personal and sensitive data requires the consent of the data subject, as well as imposes obligations on the firm for the circumstances in which data can be legally processed. In addition, sensitive personal data must be processed only for purposes relating to legal proceedings, obtaining legal advice, exercising legal rights, and the administration of justice, or for medical purposes by a health professional.[36]

# Egypt

Egypt is the most recent African economy to adopt a widespread regulation governing the protection of personal data. In July 2020, President Sisi signed Law No. 151 for 2020—the Egyptian Personal Data Protection Law—which establishes a governing structure for the protection of personal data in Egypt.[37] This regulation, reflecting a recent effort by Egypt to "modernize and safeguard the way digital interactions occur," came into force formally in October 2020, with enacting regulations (called Executive Regulations in Egypt) expected in spring 2021.[38]

The rights for personal data subjects envisioned by the Egyptian Personal Data Protection Law are extensive, and closely align with GDPR. This includes a right for a person to know what personal data are being processed and by whom; to withdraw consent to process data; to correct, change, and delete personal data; to limit processing of personal data; and to be notified of a personal data breach covering that person's data.[39]

Several of the requirements that the Egyptian data protection law places on firms have many similarities with GDPR; this is fairly common for the 15 African countries that have adopted data protection regulations from 2016 onward.[40] These obligations include a requirement that a data protection officer be hired to ensure compliance, and that this officer report any breaches to the (to be created) Egyptian Data Protection Centre.

Despite the clear connections to GDPR, the Egyptian data protection law contrasts with EU data protection laws in some ways. For example, the law requires that a data protection officer[41] be approved and licensed by the Egyptian Data Protection Centre. (A similar requirement occurs in the data protection laws of countries such as Ghana, Equatorial Guinea, Mauritius, Algeria, and

[36] Data Guidance, "Ghana Data Protection Overview," OneTrust, December 2019.
[37] The Egyptian Personal Data Protection Law can be accessed at (in Arabic) Elkanon.com, "Egyptian Legislation: Law No. 151 of 2020 promulgating the Personal Data Protection Law," n.d. (accessed February 26, 2020).
[38] Iskander, Maher, "Egypt: Data Protection Law No. 151 for 2020 (Legal Alert 118)," Andersen Tax & Legal, July 23, 2020.
[39] Nour, Ayman, and Nick O'Connell, "Egypt Passes New Personal Data Protection Law," Al Tamimi & Co., July 21, 2020.
[40] Iskander, Maher, "Egypt: Data Protection Law No. 151 for 2020 (Legal Alert 118)," Andersen Tax & Legal, July 23, 2020.
[41] A data protection officer (DPO) is an assigned person within a firm who is designated with ensuring the firm complies with the relevant provisions of the data protection law.

Kenya).[42] In addition, that officer must submit reports on a regular basis to the data protection center.

Also in contrast to GDPR, the penalty for noncompliance can include imprisonment of up to six months as well as fines of up to 100,000 Egyptian pounds ($6,293).[43] Several other African data protection regulations mandate the possibility of both fines and imprisonment, while others contain other potential punishments, including a firm losing its legal ability to process personal data. GDPR only envisions fines for noncompliance.

The Egyptian data protection regulation comes into effect in two stages. The first stage, implemented in October 2020, triggers the data protection obligations for firms working with the data of Egyptian residents. The second stage, in spring 2021, will establish Egypt's national-level enforcement structure to ensure compliance.[44]

# Kenya

Kenya is the second recent country to inaugurate a new set of data protection regulations. In November 2019, President Kenyatta signed into law the Kenya Data Protection Act, which established the requirements for the protection of personal data in Kenya.[45] The law came into force on November 25, 2019.[46]

The Kenya Data Protection Act derived much of its underlying principles from a 2018 government policy paper, the Kenya Privacy and Data Protection Policy (the Policy). The Policy noted that the Kenyan constitution defines a fundamental right to privacy. The Policy was therefore designed to inform the development of privacy and data protection laws; to comply with international good practices; to ensure protection of personal data by identifying, monitoring, and mitigating privacy risks; and to establish an institutional framework for privacy and data protection.[47] The Policy also laid out many of the principles enshrined by GDPR: limiting the collection of personal data for specific purposes, ensuring data are accurate and confidential, and safeguarding the rights of data subjects.[48]

The Data Protection Act largely aligned its legislative text and regulatory structure with the principles and priorities outlined by the 2018 Policy. It established a Data Protection Commissioner to oversee enforcement of Data Protection Act provisions, and sets registration

[42] Countries that require registration of a DPO or firm before processing and/or controlling personal data with a national data protection authority include Ghana, Equatorial Guinea, Mauritius, Algeria, and Kenya.
[43] Iskander, Maher, "Egypt: Data Protection Law No. 151 for 2020 (Legal Alert 118)," Andersen Tax & Legal, July 23, 2020.
[44] Iskander, Maher, "Egypt: Data Protection Law No. 151 for 2020 (Legal Alert 118)," Andersen Tax & Legal, July 23, 2020.
[45] The Kenya Data Protection Act can be accessed at Government of Kenya, "Data Protection Act, 2019," Kenya Zazette Supplement No. 181 (Acts No. 24), November 18, 2019.
[46] Data Guidance, "Kenya: Overview of the Data Protection Act, 2019," OneTrust, December 2019.
[47] Iskander, Maher, "Egypt: Data Protection Law No. 151 for 2020 (Legal Alert 118)," Andersen Tax & Legal, July 23, 2020.
[48] Kenya Ministry of ICT, Innovation, and Youth Affairs, "Privacy and Data Protection Policy 2018: Kenya," 2018.

requirements similar to those of other countries in Africa (see the description of Egypt above). These rules mandate that data controllers and processors first register with the Commissioner before using personal data.[49]

From the perspective of data subjects' rights in Kenya, the Data Protection Act also aligns closely with GDPR. Data subjects must be informed of the use of their personal data, and they must be able to access the data upon request, to object to the processing of all or part of their data, and to correct or delete incorrect information.[50]

Many of the Data Protection Act's obligations for data processors and controllers are also very similar to those of GDPR. First, it distinguishes specific obligations for both the processors and controllers of personal data,[51] while many other data protection laws in Africa (and outside the EU) only distinguish either controllers or processors of data as legally responsible.[52] Also unlike many other African data privacy laws, the Kenyan act also requires that data processors and controllers practice what is referred to as "privacy by design," where technology practices and systems incorporate privacy elements by default, rather than as an addition or alteration to an existing system.[53] Like many data protection standards in Africa designed after GDPR was enacted, the Kenya data privacy regulation also requires that firms conduct a data protection impact assessment (DPIA), a process designed to ensure a firm identifies and minimizes any systemic privacy risks within its operations.[54]

Other parallels between the Kenya Data Protection Act and GDPR distinguish it from many of the privacy laws set by African nations before 2016. For example, the Kenyan law sets out detailed procedures for a firm to follow once it has discovered a data breach, mandating that the Data Protection Commissioner be informed within 72 hours of becoming aware of the breach and notifying data subjects in writing if their personal data was at risk. (Several of the data protection standards promulgated in Africa between 2000 and 2015 do not set out specific provisions in the event of a data breach.)[55]

# Botswana

In August 2018, the Botswana Parliament assented to the Botswana Data Protection Act (DPA).[56] Although the DPA has received parliamentary approval, it is currently not in force.[57] However,

[49] Data Guidance, "Kenya: Overview of the Data Protection Act, 2019," OneTrust, December 2019.
[50] Data Guidance, "Kenya: Overview of the Data Protection Act, 2019," OneTrust, December 2019.
[51] As noted previously, controllers of personal data are defined as the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Processors are defined as a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
[52] Data Guidance, "Kenya: Overview of the Data Protection Act, 2019," OneTrust, December 2019.
[53] Internet Privacy Guy, "7 Principles of Privacy By Design," Medium, November 20, 2017.
[54] ICO, "What Is a DPIA?" n.d. (accessed October 4, 2020).
[55] Data Guidance, "Kenya: Overview of the Data Protection Act, 2019," OneTrust, December 2019.
[56] The Botswana Data Protection Act can be accessed at Government of Botswana, "Data Protection Act 2018," August 3, 2019.
[57] DLA Piper, "Data Protection Laws of the World: Botswana," n.d. (accessed October 1, 2020).

according to multiple industry experts, the DPA contains numerous provisions which align with the EU GDPR, and much of the structure of the law as well as the rights of individuals are very similar to the EU data protection law.[58]

First, the Botswana DPA lays out obligations for controllers and processors of personal data. For personal data to be processed legally in Botswana, the consent of the data subject must be gathered (this consent can also be revoked). In certain circumstances, this consent will not be required—i.e., if data must be processed in order to complete the terms of a contract to which the data subject is a party, to comply with a legal obligation, to protect the data subject's "vital interests," or to perform an activity in the public interest.[59] Data must also be kept for no longer than necessary, and its processing must have a clearly defined purpose.[60] Moreover, firms must ensure that they have taken appropriate security and technical measures to prevent the theft of personal data (though the law does not define what measures specifically must be taken).[61] Fines for noncompliance can reach as high as 500,000 Botswana pula (approximately $43,000) and can include imprisonment for up to nine years.[62]

Additionally, an overarching regulatory agency, the Data Protection Commission, will be established to ensure enforcement of and compliance with the DPA.[63] The Data Protection Commission will be tasked with creating and maintaining a register of all controllers of personal data (though not data processors). Data controllers who intend to process data in an automated fashion are required to notify the Data Protection Commission before any such processing.[64] The Data Protection Commission is expected to conduct investigations of possible noncompliance by firms and to handle complaints from data subjects who believe their data were misused or used without their consent.[65]

Again, like many of the data protection laws enacted after GDPR, the Botswana DPA outlines many rights for Botswana data subjects analogous to EU data subject rights.[66] For data subjects' data to be processed, they must give their consent to have their data processed, must be able to access the information, and must have the right to rectify and remove incorrect personal data.[67] In addition, if the personal data are determined to be sensitive (a distinction made in the EU GDPR

[58] Data Guidance, "Botswana Data Protection Act 2018," OneTrust, March 2019.
[59] DLA Piper, "Data Protection Laws of the World: Botswana: Collection and Processing," n.d. (accessed October 1, 2020).
[60] DLA Piper, "Data Protection Laws of the World: Botswana: Collection and Processing," n.d. (accessed October 1, 2020).
[61] DLA Piper, "Data Protection Laws of the World: Botswana: Collection and Processing," n.d. (accessed October 1, 2020
[62] DLA Piper, "Data Protection Laws of the World: Botswana: Collection and Processing," n.d. (accessed October 1, 2020).
[63] DLA Piper, "Data Protection Laws of the World: Botswana: Registration," n.d. (accessed October 1, 2020).
[64] DLA Piper, "Data Protection Laws of the World: Botswana: Registration," n.d. (accessed October 1, 2020**]**
[65] DLA Piper, "Data Protection Laws of the World: Botswana: Registration," n.d. (accessed October 1, 2020).
[66] DLA Piper, "Data Protection Laws of the World: Botswana: Collection and Processing," n.d. (accessed October 1, 2020).
[67] DLA Piper, "Data Protection Laws of the World: Botswana: Collection and Processing," n.d. (accessed October 1, 2020).

and in some other African data protection laws), the data subject must consent in writing before the data are processed, and the data subject must have made the data public first.[68] However, Botswana's personal data breach policy does differ from the EU's breach policy: while the Botswana DPA requires the Data Protection Commission be informed of a data breach that impacts personal data, there is no analogous requirement that the data subjects themselves be informed of such a breach.[69]

With a small population (around 2.4 million residents) and limited opportunities as a landlocked country, the Botswana digital trade market is one of the smaller among the case studies analyzed here. Its e-commerce market, for example, was estimated to be worth around $117 million—about 3 percent of the size of the neighboring South African market.[70]

# Rwanda

Following consultation with multiple domestic government agencies and international forums, in 2019 Rwanda released a draft text of its data protection regulation, the Data Protection and Privacy Law.[71] This law, which as of summer 2020 was still in draft form and had not been enacted, was preceded by a patchwork of laws and regulations governing a variety of digital sectors that approached data protection from different angles. The draft law, if enacted, will bring together the existing laws under a unified framework, outlining the obligations for the controllers and processors of personal data as well as the rights of data subjects.

Under existing policy, Rwanda governs information and communications technology (ICT) and data protection under a variety of regulations. These include the 1976 Decree-Law No 43/76 on the organization of the Rwandan postal service (and communications), the 2001 Telecommunications Law, Law No. 18/2010 on electronic messages, and Law No. 24/2016 governing information and communication technology.[72] Law No. 24/2016 largely supplanted many of the previous laws governing telecommunications and communications policy.[73] Despite containing significant elements of ICT legal policy in Rwanda, this law contains only a very small mention of data privacy; article 124 of this law states that "notwithstanding other provisions of this Law, every subscriber or user's voice or data communications carried by means of an electronic communications network or services, must remain confidential to that subscriber and/or user for whom the voice or data is intended."[74]

[68] DLA Piper, "Data Protection Laws of the World: Botswana: Collection and Processing," n.d. (accessed October 1, 2020).
[69] DLA Piper, "Data Protection Laws of the World: Botswana: Collection and Processing," n.d. (accessed October 1, 2020).
[70] The digital advertising market ($52 million in Botswana, $738 million in South Africa) is similarly sized. Statista Statista. "Digital Advertising: Africa," n.d. (accessed October 16, 2020).
[71] Government of Rwanda. "Law No. _____/2020 of _____/_____/____ on Data Protection and Privacy: Draft," January 30, 2020.
[72] Nkusi, Fred, "New ICT law embodies data privacy protection," *The New Times*, February 13, 2017.
[73] Nkusi, Fred, "New ICT law embodies data privacy protection," The New Times, February 13, 2017.
[74] Nkusi, Fred, "New ICT law embodies data privacy protection," The New Times, February 13, 2017.

The 2020 Data Protection and Privacy Law draft, expected to be passed by the Rwandan parliament and signed by President Paul Kagame, would substantially change the regulations governing data privacy and build off the 2016 regulation, particularly with respect to data subject rights.[75] Structured very similarly to the EU data protection regulation, articles 23 through 29 of the draft regulation outline the right of data subjects to object to the processing of personal data, the right to rectify or erase incorrect information, and the right of data portability, along with data subjects' right to be exempted from automated individual decision-making. These articles also include regulations governing the personal data of deceased people, as well as the right of data subjects to representation in instances where the data subject is a minor or is otherwise held in guardianship by someone else, where the data subject is mentally/physically unfit, or where the person authorizes, in writing, someone else to act as their proxy.[76]

The draft regulation also lays out the requirements governing the controllers and processors of personal data. It notes that both data controllers and data processors are required to register with the Authority under a (to be created) Data Protection Register before the collection and movement of personal data. In addition, the Authority has the right to withdraw that registration, effectively banning the firm from collecting or processing personal data, if it determines that firm cannot comply with the terms and conditions of the law.

Finally, the draft 2020 law also lays out the legal obligations and duties of data controllers and processors. Principally, it requires that any controller or processor must ensure that personal data are processed lawfully; that they are collected for explicit and legitimate purposes; that the scope is narrow, encompassing only necessary ends; that the data are accurate and up-to-date; and that they are processed in accordance with data subject rights.[77]

The obligations for controllers mirror the rights of data subjects, particularly with respect for the conditions in which data subjects may object to data collection and the rights they have over their own personal data. It does have some exceptions regarding compliance, in particular when the data subject already has their own data (in instances where the data have been requested by the data subject), when the data was not collected from the data subject, or when the recording or disclosure of such data contravenes other laws. The law also governs the regulations around notification of personal data breaches. In such cases, a processor must inform a data controller within 24 hours of a data breach and must inform a data subject, as well as the Authority, within 24 hours after notifying a data controller (with some caveats).[78]

Of the markets studied in this case study section, Rwanda has the smallest economy overall and is the least economically developed; in 2018, nearly 90 percent of Rwandans still worked in

[75] Nkusi, Fred, "New ICT law embodies data privacy protection," The New Times, February 13, 2017.
[76] Government of Rwanda, "Law No. _____/2020 of _____/_____/____ on Data Protection and Privacy: Draft," January 30, 2020.
[77] Government of Rwanda, "Law No. _____/2020 of _____/_____/____ on Data Protection and Privacy: Draft," January 30, 2020.
[78] Government of Rwanda. "Law No. _____/2020 of _____/_____/____ on Data Protection and Privacy: Draft," January 30, 2020.

subsistence agriculture, and the digital infrastructure of the Rwandan economy is limited.[79] Despite these limitations, the Rwandan government has expressed interest in establishing the country as a technology hub: it is one of the few countries in Africa to ratify the African Union's Convention on Cyber Security and Personal Data Protection, and government officials have expressed a strong interest in aligning laws and regulations with global best practices.[80]

# Trade Implications and the U.S. Perspective

From the U.S. trade perspective, many of the African data protection laws currently in development or already in force are likely to impact a variety of digital sectors that have significant participation from U.S. firms. Personal data are highly valued and much used in many market sectors with a strong U.S. firm presence. These include social media (U.S. firms such as Twitter, Snapchat, Facebook, and Facebook-owned WhatsApp and Instagram), search engines (Google and Microsoft's Bing), and e-commerce platforms (Amazon, eBay, Craigslist). The establishment of new data protection laws in a variety of African jurisdictions can alter the way these firms and their competitors are able to use the personal data of African consumers, either for internal practices (such as processing payments, keeping records of transactions, and handling contracts) or for commercial purposes (such as targeted advertising and data analytics).

As many countries around the world work to update or create laws and regulatory practices to protect personal data and ensure consumer privacy online, industry representatives from sectors that work extensively with personal data have noted significant costs of regulatory compliance. Industry groups and associations have made several economic impact assessments of the GDPR framework, which in addition to being one of the earliest regulatory frameworks for the protection of personal data also governs one of the world's largest digital markets. One 2020 industry assessment noted that GDPR lessened investment in Europe in data-reliant firms and younger ventures, with a 26 percent reduction in monthly EU investment deals and a 33 percent reduction in the average dollar amount raised per deal.[81] Another analysis by USITC authors noted that firms have incurred over $500 million in fines from EU regulatory authorities in less than two years of enforcement.[82] Still another indicated that the Global Fortune 500 firms are likely to spend over $8.2 billion in GDPR compliance costs. This spending mainly involved hiring more compliance staff, changing data management and privacy practices, and forgoing data-based economic opportunities.[83]

[79] Ali, Sajjad, "World Top 10 Countries with Highest Proportion of Farmers," April 7, 2013.
[80] Other ratifiers of the AU Convention on Cyber Security and Personal Data Protection include Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, and Senegal. Other countries which have signed, but not ratified, the convention include Togo, Tunisia, Zambia, São Tomé and Príncipe, Sierra Leone, Mauritania, Guinea-Bissau, the Republic of the Congo, Comoros, Chad, and Benin. African Union, "List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection," June 18, 2020.
[81] Data Catalyst Institute, "Analysis: GDPR Data Regulation Hurts EU Economic Growth," January 28, 2020.
[82] Daigle, Brian, and Mahnaz Khan, "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities," *Journal of International Commerce and Economics*, June 2020.
[83] Chivot, Eline, and Daniel Castro, "What the Evidence Shows about the Impact of the GDPR after One Year," Data Innovation, June 17, 2019.

In Africa, the expected economic impacts of country-level data protection and privacy standards will be more difficult to calculate, for several reasons. First, many of these regulations are currently in the process of being developed: in some cases, regulatory authorities to enforce data standards have not been created or staffed. As a result, firms may not have yet changed their data practices even in countries with data protection regulations in force. Second, Africa's data protection policies can vary significantly by country. As noted above, some countries have no data protection regulation at all, while others have recently developed extensive data protection regulations covering a wide variety of firm practices. This is quite different from the situation with GDPR, which is a uniform set of principles and obligations applied to the 27 EU member states (with enforcement at the member state level). Finally, the degree of enforcement remains an open question for many of these regulations: without existing regulatory agencies to carry out these regulations, data protection enforcement may confront a learning curve.

Despite the ambiguity of many of the data protection laws in Africa, and their wide variability from country to country, their economic and trade impact on technology firms impacted by such laws will likely be minor. The reason for this is that—as noted in the Digital Trade Market in Africa section above—the size of the African digital market, while growing, is also small.

From the perspective of U.S. firms, their level of exposure to the African digital trade market is lower than their exposure to markets in Europe, the United States, and the larger Asian economies (such as Japan, China, Taiwan, South Korea). In 2019, Facebook, a large U.S. firm that works extensively with personal data for advertising purposes, received less than 9 percent of its global revenue from the African market, and likely less than 5 percent. Facebook's U.S. revenue that year was about 46 percent of global revenue, its revenue from Europe was 24 percent, and its revenue from the Asia-Pacific region was 22 percent.[84] This small share of African markets as a source of global revenue is similar to the situation for other large U.S. based-technology firms that operate with consumer data, such as Google and Amazon.[85]

However, large U.S. tech firms' investments in the African market are increasing, in recognition of the large population and growing economy of the region. In May 2020, Facebook announced it would be developing a 23,000-mile undersea cable connecting southern Europe to 23 markets in Africa in an effort to expand internet access in the region.[86] Google has announced the construction of its own undersea cable for the same purpose, and Twitter has announced it will be expanding its market presence in the region.[87]

[84] Facebook classifies its revenue outside the United States/Canada, Europe, and the Asia-Pacific as "Rest of the World (ROW)." In 2019, revenue for ROW was $6.3 billion out of $70.7 billion (8.9 percent) in global revenue. Pratap, Abhijeet, "Facebook Revenue by Geography," Statstic, August 23, 2020.
[85] For Amazon, approximately 90 percent of global revenue comes from the United States, Germany, the United Kingdom, and Japan. African revenues constitute likely less than half of the remaining 10 percent of Amazon revenue. Statista, "Net sales of Amazon in leading markets 2014–2019," May 25, 2020.
[86] Browne, Ryan, "Facebook is building a huge undersea cable around Africa to boost internet access in the continent," CNBC, May 14, 2020.
[87] Browne, Ryan, "Facebook is building a huge undersea cable around Africa to boost internet access in the continent," CNBC, May 14, 2020.

Despite the current limited exposure of U.S. technology firms to the African market, the variety of regulations across African countries will likely mean that compliance costs for U.S. firms operating with personal data will rise as a proportion of expected revenue. The 55 African countries constitute less than 10 percent (and in some cases less than 5 percent) of global revenue, yet firms will be required to operate with the distinct data protection and privacy policies of more than 30 countries. It follows that compliance costs will likely rise as African countries begin strictly enforcing their data protection and privacy standards.

In certain instances where technology companies have identified regulatory challenges which require a change in business behavior, they have sometimes withdrawn from markets rather than incur the compliance costs of participating in the market.[88] While there is no indication so far that a U.S.-based technology firm would leave an African market as a result of a data protection regulation passed by a country, it is possible that such a firm may alter its business practices. The EU data protection regulation created significant compliance challenges for U.S. firms, and many firms' practices within Europe (particularly with respect to data retention, data use, and the rights of consumers to opt out) had to be changed to comply with the EU regulation. As enactment and enforcement of data protection regulations in Africa continue to spread in the near future, U.S. industries may have to similarly change certain business practices to remain compliant with African data protection laws, stay in these markets, and avoid regulatory censure (likely in the form of fines).

The challenges of the complicated patchwork of data protection laws in Africa's many markets may be ameliorated by the creation and adoption of a pan-African data protection and privacy policy, akin to the approach taken by the EU. This has been noted as an area where other international forums could take similar steps, like the Association of Southeast Asian Nations (ASEAN), the Asia-Pacific Economic Cooperation (APEC), and the South American union Mercosur.[89] The African Union itself has noted an interest in developing a pan-African digital trade framework; in May 2020 the AU announced its Digital Transformation Strategy for Africa 2020–2030. This strategy contains 16 objectives that include the development of a unified digital single market, unified policies and regulations governing digital trade, and promotion of digital trade across the continent.[90] However, these proposals are currently in the earlier stages of development.

In 2014, the AU's Malabo Convention on Cyber Security and Personal Data Protection (Convention) was already designed partially to address the concern of a bifurcated digital landscape and establish an Africa-wide common standard for the protection of personal data. Many

[88] For example, in 2014 when a Spanish court required Google to remunerate publishers for the snippets of information it provided in its Google News feature, Google opted to remove its Google News feature from the Spanish market rather than engage in licensing negotiations with Spanish publishers. Williams, Oscar, "Google News Spain to Be Shut Down: What Does It Mean?" *The Guardian*, December 12, 2014.
[89] Moeller IP, "The MERCOSUR-EU Agreement and the Legislation on Data Protection in the Countries of the Region," September 18, 2020; Tan and Azman, "The EU GDPR's impact on ASEAN data protection law," September 2019.
[90] African Union, "The Digital Transformation Strategy for Africa (2020–2030)," May 18, 2020, 1–3.

of its standards and principles resemble those which underpin EU data protection law, likely due in part to the EU Data Protection Directive, which preceded GDPR. Articles 11 and 12 mandate the establishment of a national data protection authority for each party, as well as the duties and powers of those authorities, while articles 13 and 14 lay out the legal conditions in which a firm may carry out the processing of data. Finally, articles 17 through 19 lay out the basic rights of data subjects, while article 20 through 23 highlight the legal obligations of controllers.

Despite an AU-wide data protection policy's potential for unifying many disparate policies under a single framework, adoption of this Convention has been very limited. In the six years following conclusion of the agreement, only 8 countries had formally ratified the Convention (Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwanda, and Senegal); 11 others had signed but not ratified it (Zambia, Tunisia, Togo, São Tomé and Príncipe, Sierra Leone, Mauritania, Guinea-Bissau, the Republic of the Congo, Comoros, Chad, and Benin). Most major African economies, including South Africa, Egypt, Nigeria, Kenya, and Ethiopia, have not signed on to the Convention, and several Convention signatories do not currently appear to have the national elements needed to comply with the Convention mandates. As data protection policies develop in countries both outside and inside Africa, it is uncertain whether the AU will continue to encourage countries to join the existing Cybersecurity Convention or instead attempt to adopt a new one.

Without a common framework for data protection regulations across Africa, U.S. and foreign firms operating with personal data will need to confront data protection and privacy laws in a variety of jurisdictions. These laws differ in their scope, the rights conferred on consumers, the obligations for controllers and processors of data, and the enforcement measures regulatory authorities can take. This patchwork can complicate the growth of Africa's digital economy, and may present digital trade issues for U.S., international, and African data-intensive sectors and firms.

# Bibliography

African Union. "List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection," June 18, 2020. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf https://www.ktpress.rw/2020/02/rwandas-personal-data-protection-bill-due-march/#:~:text=Currently%20Rwanda%20guarantees%20one's%20data,and%20Rwanda%20Defense%20Force%20respectively.&text=Rwanda%20was%20among%20the%20few,Guinea%20on%2027th%20June%202014.

African Union. "The Digital Transformation Strategy for Africa (2020–2030)," May 18, 2020. https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030

Ali, Sajjad. "World Top 10 Countries with Highest Proportion of Farmers." CountriesNow, April 7, 2013. https://www.countriesnow.com/world-top-ten-countries-with-highest-proportion-of-farmers/

Awosanya, Yinka. "Sub-Saharan Africa Has 48.8% of the Total Active Mobile Money Accounts in the World." Techpoint Africa, February 27, 2019. https://techpoint.africa/2019/02/27/sub-saharan-africa-has-48-active-mobile-money-accounts/.

Browne, Ryan. "Facebook is Building a Huge Undersea Cable Around Africa to Boost Internet Access in the Continent." CNBC, May 14, 2020. https://www.cnbc.com/2020/05/14/facebook-building-undersea-cable-in-africa-to-boost-internet-access.html

Chivot, Eline, and Daniel Castro. "What the Evidence Shows About the Impact of the GDPR After One Year," Data Innovation, June 17, 2019. https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA). "State of Internet Freedom in Africa 2019: Mapping Trends in Government Internet Controls, 1999–2019," September 2019. https://cipesa.org/?wpfb_dl=307.

Council on Foreign Relations. "Last Month, Over Half a Billion Africans Accessed the Internet," July 25, 2019. https://www.cfr.org/blog/last-month-over-half-billion-africans-accessed-internet.

Daigle, Brian, and Mahnaz Khan. "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities." *Journal of International Commerce and Economics*, June 2020. https://www.usitc.gov/sites/default/files/publications/332/journals/jice_gdpr_enforcement.pdf.

Data Catalyst Institute. "Analysis: GDPR Data Regulation Hurts EU Economic Growth," January 28, 2020. https://www.prnewswire.com/news-releases/analysis-gdpr-data-regulation-hurts-eu-economic-growth-300994464.html#:~:text=Key%20findings%20include%3A,dollar%20amount%20raised%20per%20deal.

DataGuidance. "Botswana Data Protection Act 2018." OneTrust, March 2019. https://www.dataguidance.com/opinion/botswana-data-protection-act-2018.

DataGuidance. "Ghana Data Protection Overview." OneTrust, December 2019. https://www.dataguidance.com/notes/ghana-data-protection-overview#:~:text=The%20purpose%20of%20the%20Data,personal%20information%2C%20and%20related%20matters.

DataGuidance. "Kenya: Overview of the Data Protection Act, 2019." OneTrust, December 2019. https://www.dataguidance.com/opinion/data-protection-act-kenya.

DLA Piper. "Data Protection Laws of the World: Botswana," n.d. https://www.dlapiperdataprotection.com/index.html?t=law&c=BW#:~:text=32%20of%202018%2C%20(%E2%80%9Cthe,their%20personal%20data%20is%20maintained (accessed October 1, 2020).

DLA Piper. "Data Protection Laws of the World: Botswana: Collection and Processing," n.d. https://www.dlapiperdataprotection.com/index.html?t=collection-and-processing&c=BW (accessed October 1, 2020).

DLA Piper. "Data Protection Laws of the World: Botswana: Registration," n.d. (accessed October 1, 2020). https://www.dlapiperdataprotection.com/index.html?t=registration&c=BW (accessed October 1, 2020).

Elkanon.com. "Egyptian Legislation: Law No. 151 of 2020 promulgating the Personal Data Protection Law." N.d. (accessed February 26, 2020). https://www.elkanon.com/2020/09/law-151-2020.html.

European Commission. *The Expansion of the Information Technology Agreement: An Economic Assessment*, 2016. https://trade.ec.europa.eu/doclib/html/154430.htm.

Government of Botswana. "Data Protection Act 2018." August 3, 2019. https://www.bocra.org.bw/sites/default/files/documents/DataProtectionAct.pdf

Government of Kenya. "Data Protection Act, 2019." Kenya Gazette Supplement No. 181, Acts No. 24. November 18, 2019. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf.

Government of Kenya. Ministry of ICT, Innovation, and Youth Affairs. "Privacy and Data Protection Policy 2018: Kenya," 2018. https://www.ict.go.ke/wp-content/uploads/2018/08/Kenya-Data-Protection-Policy-2018-15-8-2018.pdf.

Government of Rwanda. "Law No. _____/2020 of _____/_____/____ On Data Protection and Privacy: Draft," January 2020. https://minict.gov.rw/fileadmin/user_upload/Data_Protection_and_Privacy_Law__30-JAN-2020_Thursday__Final_Draft.pdf

Government of the United Kingdom (UK). Information Commissioner's Office (ICO). "What Is a DPIA?" n.d. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/ (accessed October 4, 2020).

Greenleaf, Graham. "Global Data Privacy Laws 2019: 132 National Laws and Many Bills." *Privacy Laws & Business International Report* 157, February 8, 2019. "https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3381593_code57970.pdf?abstractid=3381593&mirid=1#:~:text=Benin%20has%20enacted%20the%20most,of%20more%20than%20650%20articles.&text=Mauritius%20updated%20its%202004%20law,Protection%20Act%202017%20(Act%20No.

GSMA. *Connected Society: The State of Mobile Internet Connectivity 2019*, 2019. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/GSMA-State-of-Mobile-Internet-Connectivity-Report-2019.pdf.

GSMA. "Mobile Internet Connectivity 2019: Sub-Saharan Africa Factsheet," 2020. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/Mobile-Internet-Connectivity-SSA-Factsheet.pdf

GSMA. *State of the Industry Report on Mobile Money, 2018*, 2019. https://www.gsma.com/r/wp-content/uploads/2019/05/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2018-1.pdf.

Henry, Nzekwe. "A Rare Win Is Coming for Regulation-Hit Ride-Hailing in Africa." Wee Tracker, May 11, 2020. https://weetracker.com/2020/05/11/e-hailing-regulation-africa/.

Hughes, Nick, and Susie Lonie. "M-PESA: Mobile Money for the 'Unbanked' Turning Cellphones into 24-Hour Tellers in Kenya." *Innovations*, Winter/Spring 2007. http://nixdell.com/classes/Tech-for-the-underserved/m-pesa.pdf.

Internet Privacy Guy. "7 Principles of Privacy By Design," Medium, November 20, 2017. https://medium.com/searchencrypt/7-principles-of-privacy-by-design-8a0f16d1f9ce#:~:text=Privacy%20by%20Design%20is%20an,other%20purposes%20the%20system%20serves.

Iskander, Maher. "Egypt: Data Protection Law No. 151 for 2020 (Legal Alert 118)," Andersen Tax & Legal, July 23, 2020. https://www.mondaq.com/data-protection/968902/data-protection-law-no-151-for-2020-legal-alert-118.

ICO. *See* Government of the United Kingdom (UK). Information Commissioner's Office (ICO).

ITA. *See* U.S. International Trade Administration (ITA).

Mene, Wamkele. "Digital Trade Is the Next Big Thing in Africa." *Africa Renewal*, July 14, 2020. https://www.un.org/africarenewal/magazine/july-2020/digital-trade-next-big-thing-africa.

Moeller IP. "The MERCOSUR-EU Agreement and the Legislation on Data Protection in the Countries of the Region," September 18, 2020. https://www.moellerip.com/the-mercosur-eu-agreement-and-the-legislation-on-data-protection-in-the-countries-of-the-region/.

Moshood, Ibrahim, and Solagbade Sogbetun. "The Impact of Data Protection Rules on the Digital Economy Aspect of the African Continental Free Trade Agreement (AFCFTA)." ALP, n.d. https://www.alp.company/sites/default/files/ALP%20Review%20-%20THE%20IMPACT%20OF%20DATA%20PROTECTION%20RULES%20ON%20THE%20DIGITAL%20ECONOMY%20AND%20AfCFTA.pdf (accessed December 17, 2020).

Mourdoukoutas, Eleni. "Africa's app-based taxis battle Uber over market share." *Africa Renewal*, August 2017. https://www.un.org/africarenewal/magazine/august-november-2017/africa%E2%80%99s-app-based-taxis-battle-uber-over-market-share.

Net Imperative. "Digital Africa: Top 10 cities for start-ups," February 26, 2020. http://www.netimperative.com/2020/02/26/digital-africa-top-10-cities-for-start-ups/

Ngatane, Nthakoana. "Digital Trade the Only Tool for Africa's Economic Recovery—-Wamkele Nene." *Eyewitness News*, May 5, 2020. https://ewn.co.za/2020/05/05/wamkele-nene-to-review-afcfta-priorities-for-post-covid-19-africa.

Nkusi, Fred. "New ICT law embodies data privacy protection." *New Times*, February 13, 2017. https://www.newtimes.co.rw/section/read/207958.

Nour, Ayman, and Nick O'Connell. "Egypt passes new Personal Data Protection Law" Al Tamimi & Co., July 21, 2020. https://www.lexology.com/library/detail.aspx?g=2dccd758-ff8e-47c0-a93c-55d5e1cd31ef#:~:text=Egypt's%20Personal%20Data%20Protection%20Law,expected%20by%2014%20April%202021.

Pratap, Abhijeet. "Facebook Revenue by Geography." Statstic, August 23, 2020. https://statstic.com/facebook-revenue-by-geography/

Statista. "Digital Advertising: Africa," n.d. https://www.statista.com/outlook/216/630/digital-advertising/africa (accessed October 16, 2020).

Statista. "Digital Advertising: Europe," n.d. https://www.statista.com/outlook/216/102/digital-advertising/europe (accessed October 16, 2020).

Statista. "eCommerce: Africa," n.d. https://www.statista.com/outlook/243/630/ecommerce/africa (accessed October 16, 2020).

Statista. "eCommerce: France," n.d. https://www.statista.com/outlook/243/136/ecommerce/france (accessed October 16, 2020).

Statista. "Net sales of Amazon in leading markets 2014–2019," May 25, 2020. https://www.statista.com/statistics/672782/net-sales-of-amazon-leading-markets/

Tan, Sharon, and Nurul Syahirah Azman. "The EU GDPR's impact on ASEAN data protection law." *Financier Worldwide*, September 2019. https://www.financierworldwide.com/the-eu-gdprs-impact-on-asean-data-protection-law#.X3d0OmhJHIU.

TechSci Research. "Middle East and Africa Ride Hailing Market 2017–2023," October 2018. https://www.techsciresearch.com/report/middle-east-and-africa-ride-hailing-market/3435.html.

U.S. International Trade Administration (ITA). "Trade Guide: WTO Information Technology Agreement," n.d. https://www.trade.gov/trade-guide-wto-it-agreement#:~:text=The%20Agreement%20invites%20all%20WTO,WTO%20to%20become%20ITA%20members.&text=As%20of%20July%202015%2C%20the,trade%20in%20information%20technology%20products (accessed October 16, 2020).

U.S. Trade Representative (USTR). "2018 Fact Sheet: Key Barriers to Digital Trade," March 2019. https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital

Williams, Oscar. "Google News Spain to Be Shut Down: What Does It Mean?" *The Guardian*, December 12, 2014. https://www.theguardian.com/media-network/2014/dec/12/google-news-spain-tax-withdraws#:~:text=In%20a%20move%20that%20has,news%20publishers%20for%20their%20stories

World Bank. "Individuals Using the Internet (% of Population)." https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=NG (Accessed February 5, 2021).

Xinhua Net. "Africa Lifts Ban on E-commerce under COVID-19 Restrictions," May 15, 2020. http://www.xinhuanet.com/english/2020-05/15/c_139057569.htm.

# Appendix A

List of African nations with and without data protection laws, by year

| Year | Country | Data protection law enacted | Data protection law in force | Share of African GDP |
|---|---|---|---|---|
| 2001 | Cabo Verde | Yes | Yes | 0.1% |
| 2003 | Seychelles | Yes | No | 0.1% |
| 2004 | Burkina Faso | Yes | Yes | 0.6% |
| 2004 | Tunisia | Yes | No | 1.6% |
| 2008 | Senegal | Yes | Yes | 1.0% |
| 2009 | Morocco | Yes | Yes | 4.9% |
| 2009 | Zambia | Yes | Yes | 0.9% |
| 2011 | Angola | Yes | Yes | 3.9% |
| 2011 | Gabon | Yes | Yes | 0.7% |
| 2011 | Lesotho | Yes | Yes | 0.1% |
| 2012 | Ghana | Yes | Yes | 2.7% |
| 2013 | Côte d'Ivoire | Yes | Yes | 2.4% |
| 2013 | Mali | Yes | Yes | 0.7% |
| 2013 | South Africa | Yes | No | 14.4% |
| 2015 | Chad | Yes | Yes | 0.5% |
| 2015 | Madagascar | Yes | No | 0.6% |
| 2016 | Equatorial Guinea | Yes | Yes | 0.5% |
| 2016 | Guinea | Yes | Yes | 0.6% |
| 2016 | Rwanda[91] | Yes | Yes | 0.4% |
| 2016 | São Tomé and Príncipe | Yes | Yes | 0.0% |
| 2017 | Benin | Yes | Yes | 0.6% |
| 2017 | Mauritania | Yes | Yes | 0.3% |
| 2017 | Mauritius | Yes | Yes | 0.6% |
| 2017 | Niger | Yes | Yes | 0.5% |
| 2018 | Algeria | Yes | Yes | 7.0% |
| 2018 | Botswana | Yes | No | 0.8% |
| 2019 | Kenya | Yes | Yes | 3.9% |
| 2019 | Nigeria | Yes | Yes | 18.4% |
| 2019 | Togo | Yes | Yes | 0.2% |
| 2019 | Uganda | Yes | Yes | 1.4% |
| 2020 | Egypt | Yes | Yes | 12.4% |
| **Total** | — | — | — | **82.8%** |
| — | Burundi | No | No | 0.1% |
| — | Cameroon | No | No | 1.6% |
| — | Central African Republic | No | No | 0.1% |

[91] As noted in the Rwanda case study, an existing 2016 ICT law that guarantees the protection of private communications between data subjects may be expanded in a 2020 draft law, the Data Protection and Privacy Act.

| | | | | |
|---|---|---|---|---|
| — | Comoros | No | No | 0.0% |
| — | Congo (DRC) | No | No | 1.9% |
| — | Congo (Republic) | No | No | 0.4% |
| — | Djibouti | No | No | 0.1% |
| — | Eritrea | No | No | 0.1% |
| — | Eswatini | No | No | 0.2% |
| — | Ethiopia | No | No | 3.9% |
| — | Gambia | No | No | 0.1% |
| — | Guinea-Bissau | No | No | 0.1% |
| — | Liberia | No | No | 0.1% |
| — | Libya | No | No | 2.1% |
| — | Malawi | No | No | 0.3% |
| — | Mozambique | No | No | 0.6% |
| — | Namibia | No | No | 0.5% |
| — | Sierra Leone | No | No | 0.2% |
| — | Somalia | No | No | 0.0% |
| — | South Sudan | No | No | 0.5% |
| — | Sudan | No | No | 0.8% |
| — | Tanzania | No | No | 2.6% |
| — | Zimbabwe | No | No | 0.9% |
| **Total** | — | — | — | **17.2%** |

Sources for data protection laws compiled by author. Source for country GDP shares of African gross GDP is the World Bank https://data.worldbank.org/indicator/NY.GDP.MKTP.CD. (accessed February 1, 2021).