Vanderbilt Journal of Transnational Law

Volume 53
Issue 2 *March 2020*

Article 6

2020

# Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets

Cara Mannion

# Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets


## ABSTRACT

*The European Union (EU) recently passed the General Data Protection Regulation—a sweeping regulatory framework that sets a new global standard for the collection, storage, and use of personal data. To ensure far-reaching compliance with the GDPR, the EU has adopted a strict take-it-or-leave-it approach: countries that wish to engage with digital users in the EU must either comply with the GDPR's expansive data obligations or risk losing access to the world's largest trading block.*

*This presents significant obstacles for several African nations. Notably, no African country currently has domestic laws that comply with the GDPR. Even if they did, several African countries lack stable judicial branches to enforce such laws, and many do not have the technological infrastructures or expertise to ensure ongoing compliance. Additionally, the GDPR's extraterritorial effects may amount to data imperialism, allowing the EU to impose its own definition of data privacy on African countries without concern for their unique social values and economic realities.*

*This Note analyzes how the GDPR negatively impacts several African countries, as well as the difficulties in solving these economic and social problems. Although there are no easy solutions for these complex issues, this Note recommends that African countries adopt data privacy legislation at the regional level, create regional enforcement authorities, and invest in technological infrastructure and training.*


## TABLE OF CONTENTS


I. INTRODUCTION ..... 686
II. BACKGROUND ..... 688
  A. *The GDPR and Its Wide-Reaching Impacts* ..... 688
    1. Key Extraterritoriality Provisions of the GDPR ..... 691
    2. Complying with the GDPR ..... 692
    3. The Costs of Failing to Comply with the GDPR ..... 693

B. *Current Data Privacy Regimes in Africa* . 695
1. South Africa: Active Legislation ..... 697
2. Kenya: Draft Legislation ..... 698
III. ANALYSIS ..... 700
A. *Stifling Innovation, Investment, and Economic Growth* ..... 701
B. *Enforcement Issues* ..... 702
C. *Issues with Technological Expertise* ..... 704
D. *Data Imperialism and the Brussels Effect* ..... 705
IV. SOLUTION ..... 707
A. *Passing GDPR-Compliant Legislation at the Regional Level* ..... 708
B. *Enforcing GDPR-Compliant Legislation at the Regional Level* ..... 708
C. *Investing in Technological Infrastructure and Training* ..... 709
V. CONCLUSION ..... 710

## I. INTRODUCTION

The European Union (EU) recently put into effect the General Data Protection Regulation (GDPR)—a landmark data privacy law that gives EU residents unprecedented control over how their personal data is collected and used.[1] In passing the GDPR, the EU intended to set global standards for data protection that extended well beyond the borders of its twenty-eight member countries.[2] This is largely achieved through an extraterritoriality feature that imposes privacy obligations on non-EU companies that offer products or services to EU residents.[3]

To give the GDPR's extraterritorial provisions some bite, the EU adopted a firm take-it-or-leave-it approach: countries that wish to engage in e-commerce with EU residents must either pass domestic laws that comply with the GDPR's expansive data obligations or risk losing access to the world's largest trading block. [4] However, compliance comes with hefty costs. [5] For example, countries not

---

1. *See* Mark Scott & Laurens Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, POLITICO, https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/ (last updated Feb. 6, 2018) [https://perma.cc/6EJW-YHDN] (archived Nov. 12, 2019).
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*; *see also* Jeremy Kahn, Stephanie Bodoni & Stefan Nicola, *It'll Cost Billions for Companies to Comply With Europe's New Data Law*, BLOOMBERG

currently in compliance must hustle to enact GDPR-friendly regulations, and these countries then must expend resources to enforce such regulations.[6] Individual companies must also pay handsomely to achieve organizational compliance with the GDPR if they wish to electronically transact with EU residents.[7]

For countries with advanced economies, the choice between GDPR compliance or market shutout is likely an easy one.[8] Many of these countries already have data protection frameworks in place, which reduces the regulatory burden of matching the GDPR's gold standards.[9] Furthermore, companies within these developed countries are more likely to be technologically sophisticated.[10]

But for developing countries, there may be no real choice between compliance or market shutout.[11] This is particularly true in Africa.[12] Notably, no African countries currently have domestic laws that comply with the GDPR.[13] In fact, some African countries lack data privacy regulations altogether, such as Algeria, Comoros, and the Central African Republic.[14] And even if an African country has some data protection laws in place, other concerns—like corruption and public safety—commonly take enforcement priority.[15]

Many of these countries face significant factors that prevent them from achieving GDPR compliance, including a lower level of technological sophistication, few supporting services, and turbulent lawmaking bodies.[16] Small businesses within these developing countries may also lack the knowledge or budgets needed to comply with the GDPR's complicated data protection rules.[17]

The stakes are high for African countries. The EU is one of South Africa's largest trading partners, comprising 40 percent of the

---

BUSINESSWEEK (Mar. 22, 2018), https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law [https://perma.cc/D737-G5KA] (archived Dec. 20, 2019).

6. *See* Scott & Cerulus, *supra* note 1.

7. *Id.*

8. *Id.*

9. *See* Tiffany Curtiss, *Privacy Harmonization and the Developing World: The Impact of the EU's Developing Economies*, 12 WASH. J.L. TECH. & ARTS 95, 108–09 (2016) (noting that developing countries face many more obstacles than developed countries).

10. *Id.*

11. Scott & Cerulus, *supra* note 1.

12. *Id.*

13. *See* DALBERG ADVISORS, NOT JUST AN EU CONCERN: THE IMPLICATIONS FOR AFRICA 7 (Jan. 2018), https://www.dalberg.com/system/files/2018-05/GDPR_Implications%20for%20Africa_EMAIL%20PDF-vFinal%20March2018.pdf [https://perma.cc/BS6P-TYZ9] (archived Nov. 12, 2019).

14. *Id.* at 14.

15. *See* Curtiss, *supra* note 9, at 111, 119 (noting corruption as a risk in choosing a developing country as an enforcing authority for the GDPR).

16. *Id.* at 108.

17. *Id.* at 110.

country's e-commerce business. [18] What is more, Africa's digital economy exports USD $14 billion to the EU every year.[19] In passing the GDPR and disallowing partial compliance, the EU has jeopardized Africa's existing e-commerce markets, as well as the continent's opportunity to help innovate the e-commerce market in the future.

This Note evaluates the GDPR's disproportionate impact on Africa's participation in the global e-commerce market. Part II of this Note explains key portions of the GDPR and evaluates current data protection regimes in Africa. Part III analyzes the factors that cause the GDPR to disproportionally impact some African countries. These factors include difficulties in enforcing breached data rights, issues with maintaining technologically educated workforces, and the stifling of economic growth. Part III also analyzes a phenomenon known as the Brussels Effect, which could result in the imposition of Eurocentric ideals on African economies and governments. Finally, Part IV explains the difficulties in solving these issues, as well as some first steps that can be taken to level the data privacy playing field in African nations. These steps include adopting data privacy legislation at the regional level, creating regional enforcement authorities, and investing in technological infrastructure and training.

## II. BACKGROUND

### A. *The GDPR and Its Wide-Reaching Impacts*

The European Union (EU) passed the General Data Protection Regulation (GDPR) in April 2016.[20] This sweeping data privacy regime gave EU residents unprecedented autonomy over their personal data.[21] According to one commentator, the GDPR will "fundamentally reshape the way in which data is handled across every sector, from healthcare to banking and beyond."[22]

---

18. *See South Africa*, EUROPEAN COMM'N, http://ec.europa.eu/trade/policy/countries-and-regions/countries/south-africa/ (last visited Feb. 27, 2019) [https://perma.cc/CWC4-ELQP] (archived Nov. 15, 2019).

19. *Id.*

20. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Council Directive 95/46/EC, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

21. *See* Manu J. Sebastian, *The European Union's General Data Protection Regulation: How Will It Affect Non-EU Enterprises?*, 31 SYRACUSE J. SCI. & TECH. L. 216, 216–18 (2015) (describing the GDPR as the most comprehensive and forward-looking piece of data protection legislation in the digital age).

22. *See The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years*, EU GDPR PORTAL, https://eugdpr.org/ (last visited Feb. 27, 2019) [https://perma.cc/9ZHS-BYUA] (archived Nov. 15, 2019) [hereinafter *GDPR is the most important change in 20 years*].

The GDPR is based on the idea that every individual has a right to have his or her data protected.[23] As such, the GDPR gives individuals a series of enforceable rights over their data privacy interests.[24] These data privacy rights include:

- The right to object to an entity processing personal data information (known as the right to object).
- The right to have personal data erased (known as the right to be forgotten).
- The right to have inaccurate data corrected (known as the right to rectification).
- The right to know what personal data is being processed, by whom, and whether other parties may receive it.
- The right to hold data collectors accountable for violating data privacy rights under the GDPR.[25]

To satisfy these enumerated individual rights, the GDPR imposes substantial obligations on parties that wish to digitally interact with EU residents.[26] For example, a party may only collect and use data that is necessary to accomplish the specific task that led to the collection of data in the first place.[27] Data processors may also be required to adopt various security safeguards, such as encrypting the identity of data subjects and buying cyber liability insurance.[28] Additionally, entities that process data must disclose any data breaches to applicable regulators within seventy-two hours of the breach.[29]

Compliance with these obligations will undoubtedly prove costly for businesses. As of March 2018, the five hundred largest corporations in the world are on track to spend a total of $7.8 billion to comply with the GDPR.[30] Microsoft tasked three hundred engineers with ensuring its software complied with the GDPR.[31] Smaller businesses are also facing heightened compliance costs under the GDPR. As Facebook Chief Operating Officer Sheryl Sandberg said at a conference in Brussels, the "GDPR holds companies of all sizes to account" since

---

23. *See* Sebastian, *supra* note 21, at 216–17 (explaining the EU's belief that personal data protection is a fundamental right that should be enjoyed by all).

24. *Id.*

25. Joseph Facciponti & Katherine McGrail, *GDPR Is Here—What If You Didn't Prepare?*, LAW360 (May 24, 2018), https://www.law360.com/articles/1047079 [https://perma.cc/2QFZ-SDQ4] (archived Nov. 13, 2019).

26. *Id.*

27. *Id.*

28. *See id.*

29. *Id.*

30. *See* Kahn, Bodoni, & Nicola, *supra* note 5.

31. *Id.*

every modern business—no matter its size—uses data to improve their services.[32]

The EU's adoption of this sweeping data privacy regime is not surprising given the region's history in the privacy arena. The EU has long been regarded as a leader in data protection laws.[33] In 1995, the European Parliament passed the EU Data Protection Directive, which sought to harmonize a patchwork of data protection regimes that had been adopted by individual member states of the EU.[34] To achieve this harmonization, the Data Protection Directive required each member state to enact national data protection legislation that served two main objectives: (1) to protect the individual right to data protection, and (2) to guarantee the free flow of personal information between member states.[35] Looking back on the directive's impact, experts say the directive was successful in deterring data breaches and helped to expand e-commerce between member states.[36]

Despite these successes, EU regulators soon recognized the need to modernize the Data Protection Directive.[37] The directive was adopted during the internet's infancy in 1995, when only 1 percent of the European population used the internet.[38] In the decade since EU regulators passed the directive, technological advancements had completely changed how companies and other entities collected, stored, and used consumer data.[39] Additionally, as a nonbinding directive, the Data Protection Directive of 1995 allowed individual member states to uniquely interpret the rules when adopting them into individual national law, which jeopardized the directive's overall mission of unifying the different member states' individual data protection landscapes.[40] Thus, EU regulators began to explore a new data protection regime that would expand EU citizens' data autonomy and further reduce the occurrences of data breaches.[41]

---

32. *Id.*

33. *See* European Data Protection Supervisor, *The History of the General Data Protection Regulation*, EUROPEAN UNION, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Oct. 28, 2018) [https://perma.cc/H5C7-4L7S] (archived Nov. 13, 2019) (noting that the EU's data protection laws have been regarded as the world's "gold standard" for years).

34. *See* Curtiss, *supra* note 9, at 99.

35. *Id.*

36. *Id.*

37. *See How did we get here? An overview of important regulatory events leading up to the GDPR*, EU GDPR PORTAL, https://eugdpr.org/the-process/how-did-we-get-here/ (last visited Nov. 13, 2019) [https://perma.cc/AH37-XCCW] (archived Nov. 13, 2019).

38. *Id.*

39. *Id.*

40. *Id.*

41. *See* Nate Lord, *What is the Data Protection Directive? The Predecessor to the GDPR*, DIGITAL GUARDIAN (Sept. 12, 2018), https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr [https://perma.cc/YW3H-B5Z5] (archived Nov. 13, 2019).

After four years of negotiations, regulators eventually adopted the GDPR in April 2016, which supersedes and phases out the Data Protection Directive.[42] Although the GDPR builds on key provisions found in the Data Protection Directive, many of its features go well beyond its predecessor. For example, the GDPR contains an expanded definition of what constitutes personal data, more stringent consent requirements, and an increasing amount of responsibility placed on companies to protect their consumers' data.[43] Yet perhaps the most sweeping reform found in the GDPR is its extraterritoriality feature, which set up a global conflict on what level of data protection governments should demand.[44]

1. Key Extraterritoriality Provisions of the GDPR

In passing the GDPR, the EU intended to set sweeping standards for data protection that extended well beyond the borders of its member states.[45] Indeed, Věra Jourová, the European commissioner for justice, told the media in 2017 that the EU intended to set a global standard when passing the GDPR.[46] The EU achieved this through two provisions that bring non-EU companies under the GDPR's purview.

First, the GDPR covers any non-EU company that monitors the behavior of individuals within the EU.[47] This includes the tracking of individuals' internet usage.[48]

Second, the GDPR applies to any company that offers goods or services to individuals located within the EU.[49] Under this provision, it does not matter whether a financial transaction takes place in the offering of goods or services.[50] Rather, a company meets this threshold by undertaking affirmative actions, however small, to solicit customers in the EU.[51] This means that the GDPR would not be triggered by an EU resident's mere access of an international entity's website.[52] However, an entity may trigger the GDPR if it accepted EU currencies on its website, provided content in EU languages, or hosted an EU-

42. *Id.*

43. *See The EU General Data Protection Regulation Questions and Answers*, HUMAN RIGHTS WATCH (June 6, 2018), https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation [https://perma.cc/6GKE-SQ7N] (archived Nov. 13, 2019) [hereinafter *GDPR Q&A*].

44. *Id.*

45. *See* Sebastian, *supra* note 21, at 242–43 (explaining the GDPR's effects on "the entire global trading system and almost every international enterprise in the world").

46. Scott & Cerulus, *supra* note 1.

47. *See* GDPR, *supra* note 20, at art. 3(1).

48. *Id.* at pmbl. 24.

49. *Id.* at art. 3(2)(a).

50. *See* Facciponti & McGrail, *supra* note 25.

51. *Id.*

52. *Id.*

based website domain—all actions that may constitute an affirmative offer of goods or services to EU residents. [53] Although these characteristics provide examples of when a non-EU company may trigger the GDPR, there is no bright-line test clearly articulating when this trigger is pulled.[54] As such, these assessments will likely be made on a case-by-case basis, creating a potential risk that companies incorrectly guess—or take the calculated risk—that the GDPR does not apply to their businesses.[55]

2. Complying with the GDPR

The GDPR sets forth two pathways to compliance: (1) national adoption of laws and regulations that comply with the GDPR or (2) organizational adoption of company procedures that comply with the GDPR.[56]

Under the first pathway, countries pass their own data protection legislation. [57] This legislation need not match the GDPR's gold standards point-for-point.[58] Instead, the GDPR requires countries to pass laws that offer a standard of data protection that is equivalent to the protection offered under the GDPR. [59] When assessing this equivalency, the EU evaluates a variety of factors, including (1) the substance of the country's legislation, (2) whether the country can effectively implement and enforce this legislation, (3) the country's commitment to the rule of law and overall respect for fundamental freedoms of the individual, and (4) international data protection commitments.[60]

Under the second pathway, individual companies can still achieve GDPR compliance even if they are located in countries that lack the regulatory framework required by the GDPR. [61] This is primarily achieved in two ways: (1) the company can independently adopt corporate rules and procedures that adequately protect consumer data under the GDPR or (2) the company can enter into contracts requiring subcontractors to maintain reasonable levels of security and obey applicable security laws. [62] However, these interorganizational

---

53. *Id.*
54. *Id.*
55. *See Long Arm of the Law – Impact of the GDPR on Middle East Organisations*, DENTONS (Sept. 28, 2017), https://www.dentons.com/en/insights/alerts/2017/september/28/long-arm-of-the-law-impact-of-the-gdpr-on-middle-east-organisations [https://perma.cc/5446-TJLB] (archived Nov. 15, 2019).
56. *See id.*
57. *See id.*
58. *See id.*
59. *See id.*
60. *See id.*
61. *See* Curtiss, *supra* note 9, at 101.
62. *Id.*

strategies have not been widely adopted.[63] As of May 2018, fewer than two hundred companies globally have received approval from a national data protection authority certifying their binding corporate rules as compliant with the GDPR.[64]

3. The Costs of Failing to Comply with the GDPR

Notably, the EU has adopted a strict take-it-or-leave-it approach: data controllers must either comply with the GDPR's expansive data obligations or risk losing access to the world's largest trading block.[65] Although this strict approach presents a difficult choice to countries around the world, some critics—like the author quoted below—argue that the EU's strong-arming could disproportionally impact developing countries.[66]

> [Achieving GDPR compliance] is mostly manageable for advanced economies like Japan, which last year set up an independent agency to handle privacy complaints to conform with Europe's privacy standards during negotiations for a new Japan-EU trade deal. But for emerging countries, the cost and administrative burden of applying the EU privacy standards can be daunting.[67]

The official deadline to become GDPR-compliant was supposed to be May 25, 2018.[68] The EU's regulators gave companies a two-year runway to achieve compliance after passing the regulations in 2016.[69] However, a large number of companies reported that they were unable to reach the deadline.[70] For example, in a study of one thousand companies conducted in April 2018, half said they would not achieve compliance by the deadline.[71] Additionally, in 2017—only one year until the deadline—61 percent of companies reported that they had yet to begin the process of working toward GDPR compliance.[72]

Despite the reality that several companies have missed the May 2018 deadline and are yet to be considered GDPR-compliant, the EU

---

63. *See List of companies for which the EU BCR cooperation procedure is closed*, EUROPEAN COMM'N (May 24, 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841 [https://perma.cc/4QJJ-KWC7] (archived Feb. 13, 2020).

64. *Id.*

65. Scott & Cerulus, *supra* note 1.

66. *See* Corey Doctorow, *The coming EU privacy regulation will end up remaking the world's web*, BOINGBOING (Feb. 3, 2018), https://boingboing.net/2018/02/03/race-to-the-top.html [https://perma.cc/855N-F7HS] (archived Nov. 15, 2019).

67. *Id.*

68. *See* Sarah Jeong, *No one's ready for GDPR*, VERGE (May 22, 2018), https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu [https://perma.cc/D56R-LUA3] (archived Nov. 15, 2019).

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.*

continues to encourage data controllers to strive toward compliance.[73] Consider the following warning from a website affiliated with the EU:

> If the GDPR deadline has been missed, it is imperative the business in question acts urgently to become compliant. Demonstrating strong data rights management is important to both customers and employees; they should understand why the data is collected and how it is handled on a legal basis. Current business data processes need to be looked at as an immediate priority so that the company doesn't risk non-compliance penalties.[74]

These warnings likely stem from the severe sanctions contemplated by the GDPR.[75] Entities that fail to comply with the GDPR face hefty costs from a variety of sources.[76] First, the GDPR empowers individuals to bring lawsuits against any company that violated their rights under the regulatory scheme.[77] Companies that violate the GDPR may also face private suits filed by corporate partners and shareholders.[78] Second, privacy regulators are entitled to impose administrative fines up to €20 million, or 4 percent of annual global turnover, whichever is higher.[79] This means that a company like Facebook could pay €2.3 billion ($2.6 billion) for a GDPR violation.[80] In fact, Google had to pay a $57 million fine in January 2019 for failing to properly notify users how it collected data to present personalized advertisements.[81] Third, each EU member state has the ability to impose additional administrative fines for noncompliance.[82] One member state's imposition of an administrative fine does not preempt another member state's ability to impose its own fine.[83] Even though the GDPR outlines specific factors that the member states should consider when determining appropriate administrative fines, in the end the fine need only be "effective, proportionate, and dissuasive."[84]

Beyond the liabilities specifically spelled out in the GDPR, noncompliant companies may also face costs in the form of lost

---

73. *See GDPR is the most important change in 20 years*, *supra* note 22.
74. *Id.*
75. *See* GDPR, *supra* note 20, at art. 58.
76. *Id.* at art. 83(4).
77. *Id.* at art. 82(1).
78. Christopher Cole, *Nielsen Hit With Shareholder Suit Over EU Privacy Impacts*, LAW360 (Aug. 27, 2018), https://www.law360.com/articles/1076082 [https://perma.cc/75FS-FCK2] (archived Nov. 15, 2019) (Nielsen Holdings is facing a shareholder lawsuit alleging it misled investors about how the GDPR affected its financial performance).
79. *Id.*
80. Curtiss, *supra* note 9, at 104.
81. Adam Satariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html [https://perma.cc/545R-VWWW] (archived Nov. 15, 2019).
82. Curtiss, *supra* note 9, at 104.
83. *Id.*
84. *Id.*

credibility or reduced customer loyalty.[85] Assuming a majority of the private sector is eventually able to achieve GDPR compliance, customers may start to expect this level of data protection from all companies with which they interact.[86] Companies that fail to do so may tarnish their images in the public's eye, thereby reducing sales numbers.[87] In turn, this loss of credibility may deter potential joint ventures, which would reduce the profitability of these companies.[88] Furthermore, noncompliant companies would be unable to hide these transgressions from their customers, shareholders, and business partners because the GDPR obligates companies to directly report any possible leaks of a user's personal data.[89]

### B. *Current Data Privacy Regimes in Africa*

Africa currently lacks a unified regulatory approach to personal data protection, even though the continent had the world's fastest growth in internet usage over the past decade.[90] Importantly, no African country currently has domestic laws that comply with the GDPR.[91] In fact, more than half of the fifty-four countries in Africa lack any data protection or privacy laws whatsoever.[92] And while some African countries have taken steps to develop legislation aimed at data protection, these steps have not culminated in any meaningful data protections at the national level.[93] For example, of the fourteen countries that currently have data protection legislation, nine lack any regulating bodies to enforce the laws.[94]

Efforts to adopt comprehensive data protection legislation in Africa have occurred at the continental, regional, and national levels.[95] For example, the African Union (AU) in 2014 passed the Convention on Cyber Security and Personal Data Protection, which aimed to establish regulatory frameworks for personal data protection at the

---

85. *See* Panda Media Center, *The GDPR Is Here: Now What?*, PANDA SEC. (May 23, 2018), https://www.pandasecurity.com/mediacenter/security/gdpr-is-here-what-now/ [https://perma.cc/RE6B-UEZQ] (archived Nov. 15, 2019).

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

90. *See* Maggie Fick & Alexis Akwagyiram, *In Africa, scant data protection leaves internet users exposed*, REUTERS, Apr. 4, 2018, https://www.reuters.com/article/us-facebook-africa/in-africa-scant-data-protection-leaves-internet-users-exposed-idUSKCN1HB1SZ [https://perma.cc/SD4A-ZKSR] (archived Nov. 15, 2019).

91. *See* DALBERG ADVISORS, *supra* note 13, at 12.

92. *See* Fick & Akwagyiram, *supra* note 90.

93. *See* DALBERG ADVISORS, *supra* note 13, at 10.

94. *See* Fick & Akwagyiram, *supra* note 90.

95. *See Data protection regulations and international data flows: Implications for trade and development*, UNITED NATIONS CONFERENCE ON TRADE & DEV. 35 (2016), https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf [https://perma.cc/M52E-FB4Y] (archived Nov. 15, 2019) [hereinafter UNCTAD].

national and regional levels.[96] However, unlike the GDPR's automatic enforceability, the AU convention lacks any legal force until African countries adopt the provisions into their national legislation.[97] As of early 2016, no African country has ratified the convention, which severely limits the AU convention's actual impact on African data protection.[98] Nonetheless, the AU convention provides a regulatory framework that African countries can use as a model to draft their own data protection legislation. [99] Furthermore, the AU convention encourages African countries to recognize the importance of protecting personal data and promoting global digitalization.[100]

Two regional initiatives are also noteworthy. The Economic Community of West African States (ECOWAS) adopted an initiative in 2010 that aimed to harmonize data protection regimes across its member states.[101] As of 2016, seven countries within ECOWAS have enacted national laws that comply with the agreement. [102] Additionally, the nineteen-member group known as the Common Market for Eastern and Southern Africa (COMESA) has brainstormed regional solutions for data privacy problems.[103] However, only three COMESA countries currently have data protection laws in place: Madagascar, Mauritius, and Seychelles. [104] Ethiopia, Kenya, and Uganda have not yet passed any data protection laws, but they are currently considering drafts of data protection bills in their Parliaments. [105] In contrast, nine members of COMESA (Burundi, Comoros, Democratic Republic of the Congo, Djibouti, Eritrea, Libya, Rwanda, Sudan, and Swaziland) lack any meaningful regulations focused on data protection—either enacted into law or up for consideration in their Parliaments.[106]

In whole, the present regulatory environment within individual African countries can be divided into four subgroups: (1) twenty-two countries currently have some sort of data privacy legislation in place, (2) seven countries have drafted data privacy legislation but have not yet passed such legislation, (3) thirteen countries lack data privacy legislation altogether, and (4) twelve countries do not process data on

---

96. *Id.*

97. *See Privacy is Paramount: Personal Data Protection in Africa*, DELOITTE 6 (2017), https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf [https://perma.cc/2VJ4-T8KQ] (archived Nov. 15, 2019) [hereinafter *Deloitte Report*].

98. *See* UNCTAD, *supra* note 95.

99. *See Deloitte Report*, *supra* note 97.

100. *Id.*

101. *See* UNCTAD, *supra* note 95.

102. *Id.*

103. *See* DALBERG ADVISORS, *supra* note 13, at 10.

104. *See id.* at 16.

105. *See id.*

106. *See id.*

a large scale.[107] This Note will evaluate examples of African countries that fall into the first two categories.

1. South Africa: Active Legislation

South Africa's e-commerce market has exploded in the past decade, due in large part to the increased use of mobile phones in the country.[108] Online spending in South Africa is projected to grow at an annual rate of 15 percent through 2021.[109] Internet penetration within South Africa has reached 54 percent as of 2018.[110] These gains in internet usage are not contained within the borders of the country. For example, the EU is one of South Africa's largest trading partners, comprising 40 percent of its e-commerce business.[111]

In 2013, South Africa passed the Protection of Personal Information Act (POPIA), which afforded South Africans the constitutional right to data privacy.[112] In basing POPIA on the EU's personal data protection framework, South Africa's legislature mirrored many provisions in the GDPR.[113] First, POPIA gives South Africans a great degree of autonomy over their personal data, including the right to be informed about how entities are collecting and using their data.[114] In addition, POPIA requires all organizations to report data breaches within seventy-two hours to the country's Information Regulator—a governmental body established under POPIA that is tasked with regulating and enforcing the act's provisions.[115] The penalties for noncompliance with POPIA include fines up to R$10

107. *See* UNCTAD, *supra* note 95.

108. *See* Carin Smith, *How Ecommerce is Exploding in SA*, FIN24 (Mar. 16, 2018), https://www.fin24.com/Economy/how-ecommerce-is-exploding-in-sa-20180316 [https://perma.cc/SJ8R-57QE] (archived Nov. 16, 2019).

109. *See South Africa – Ecommerce*, EXPORT.GOV, https://www.export.gov/article?id=South-Africa-ecommerce (last updated July 14, 2019) [https://perma.cc/EE9B-BTRS] (archived Nov. 16, 2019).

110. *See* Marcia Kaplan, *Africa: An Emerging Ecommerce Market with Many Changes*, PRACTICAL ECOMMERCE (June 13, 2018), https://www.practicalecommerce.com/africa-emerging-ecommerce-market-many-challenges [https://perma.cc/YXN3-CHDT] (archived Nov. 16, 2019).

111. *See South Africa*, *supra* note 18.

112. *See* Melanie Kirsten Hart, *South Africa: Data Protection in Terms of POPIA and the GDPR*, MONDAQ (June 29, 2018), http://www.mondaq.com/southafrica/x/713936/data+protection/Data+protection+in+terms+of+POPIA+and+the+GDPR [https://perma.cc/9NJQ-FKTH] (archived Nov. 16, 2019).

113. *See* Michael Bratt, *POPIA is still on the way...but it's taking time*, THEMEDIAONLINE (Aug. 14, 2018), https://themediaonline.co.za/2018/08/popia-is-still-on-the-way-but-its-taking-time/ [https://perma.cc/5Z9R-UTVS] (archived Nov. 16, 2019).

114. *See* Hart, *supra* note 112.

115. *See Data Protection Laws of the World: South Africa*, DLA PIPER (Jan. 28, 2019), https://www.dlapiperdataprotection.com/index.html?t=law&c=ZA [https://perma.cc/2E5R-6KS6] (archived Nov. 12, 2019).

million, ten years in jail, or damages awarded to the individual data subjects who were harmed by the entity's noncompliance.[116]

Despite passing POPIA in 2013, the South African government has yet to put the legislation into effect.[117] While limited sections of the act have been implemented, the bulk of the legislation will commence at a later date that has not yet been determined by the president.[118] Additionally, the Information Regulator is still in the process of staffing its office.[119] These delays have come at a cost. South Africa has faced several major data breaches since 2013, including the Jigsaw Holdings "masterdeeds.sql" leak, which released the home addresses and contact information of millions of South Africans.[120] Without a fully functioning Information Regulator, these cyberattacks will go largely unpunished.[121] And even once POPIA is fully in effect, the legislation's impact will not be felt for another year, given that companies have a one-year grace period to come into compliance.[122]

2. Kenya: Draft Legislation

Known as "Silicon Savannah," Kenya represents the epicenter of Africa's technology movement.[123] Kenya's internet usage has exploded over the past decade, with internet penetration surging from about 1 percent in 2000 to 26 percent in 2017.[124] Research shows that two of every three Kenyans have access to the internet.[125] And of Kenya's 44 million citizens, 8.5 million use Facebook on a monthly basis.[126] Kenya

---

116. *Id.*

117. *See Protection of Personal Information Act Summary*, MICHALSONS, https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia (last visited Feb. 13, 2020) [https://perma.cc/LT2F-MWDN] (archived Nov. 12, 2019).

118. *See* Tehillah Niselow, *Five massive data breaches affecting South Africans*, MAIL & GUARDIAN (June 19, 2019), https://mg.co.za/article/2018-06-19-five-massive-data-breaches-affecting-south-africans [https://perma.cc/J25H-SNPY] (archived Nov. 12, 2019).

119. *See Deloitte Report*, *supra* note 97.

120. *See* Hart, *supra* note 112.

121. *Id.*

122. *See* Bratt, *supra* note 113.

123. *See* Jake Bright & Aubrey Hruby, *The Rise Of Silicon Savannah And Africa's Tech Movement*, TECH CRUNCH (July 23, 2015), https://techcrunch.com/2015/07/23/the-rise-of-silicon-savannah-and-africas-tech-movement/ [https://perma.cc/K73G-2REZ] (archived Nov. 12, 2019).

124. *See* Sabina Frizell, *How Kenya's New Data Privacy Bill Could Hurt Its Economy*, COUNCIL ON FOREIGN RELATIONS (Nov. 8, 2018), https://www.cfr.org/blog/how-kenyas-new-data-privacy-bill-could-hurt-its-economy [https://perma.cc/PM6N-HNRP] (archived Nov. 12, 2019).

125. *See* Collins Omulo, *New study shows more Kenyans have internet access*, DAILY NATION (Apr. 19, 2017), https://www.nation.co.ke/news/Internet-access-grows-in-Kenya/1056-3895304-nsw0nnz/index.html [https://perma.cc/4GWZ-7YBF] (archived Nov. 12, 2019).

126. *See* Fick & Akwagyiram, *supra* note 90.

is also recognized as a hub for technology companies.[127] For example, IBM in 2013 opened a $100 million research center in the country—the company's first center in all of Africa.[128] Kenya is also home to many successful start-up companies, including M-PESA, which was one of the first mobile money services to be regularly used by African communities.[129]

Kenya's rapid rise in the digital world is largely due to its government's investment in technology infrastructure.[130] In 2011, the country launched an open government data platform, which allowed companies to use this communal data information at no cost when building their businesses.[131] The Kenyan government predicted that this open platform would increase the information technology sector's contribution to the gross domestic product to 15 percent.[132] Additionally, the Kenyan government has driven innovation by adopting a light-touch regulatory approach, which allows still-developing technology companies to flourish without fear of burdensome policy requirements.[133]

Because of this relaxed regulatory approach, Kenya currently lacks a comprehensive framework for data protection.[134] However, several election-related privacy scandals led the country to draft data protection legislation, which would offer citizens substantial protections for their data.[135] Many of the requirements within this bill echo the GDPR.[136] For example, entities must inform digital users of the personal data they are collecting, the purpose for this data collection, and how long the entities will store this data.[137] Additionally, the bill establishes security standards for the storage of data, and digital users have the right to request that their data be deleted or corrected.[138]

However, some scholars criticize this draft legislation as being too restrictive.[139] Small businesses argue that this draft legislation will cripple Kenya's still-developing digital economy by favoring incumbent

---

127. *See* Bright & Hruby, *supra* note 123.
128. *Id.*
129. *Id.*
130. *See* Frizell, *supra* note 124.
131. *See* Alex Howard, *Open Data Catches on in Kenya*, FORBES (July 15, 2011), https://www.forbes.com/sites/oreillymedia/2011/07/15/open-data-catches-on-in-kenya/#40c997767c56 [https://perma.cc/LP45-7WWN] (archived Nov. 12, 2019).
132. *Id.*
133. *Id.*
134. *See* Frizell, *supra* note 124.
135. *Id.*
136. Brian Obilo, *Kenya Data Protection Bill 2018*, INTERNET YETU (Aug. 25, 2018), https://internetyetu.org/kenya-data-protection-bill-2018/ [https://perma.cc/RC5V-94EP] (archived Nov. 12, 2019).
137. *Id.*
138. *Id.*
139. *See* Frizell, *supra* note 124.

companies.[140] For example, multinational and large local companies have the ability to shoulder costs for compliance, while small businesses may not have the capital necessary to satisfy the new requirements.[141] Additionally, large companies likely already hired staff members to advise on compliance, giving them a leg up in adapting their preexisting business practices to the new legislation.[142] Finally, newly formed companies lack the advantage of leveraging a lax regulatory environment, which greatly contributed to the success of incumbent technology companies.[143]

The draft legislation also calls for a data localization provision, which would make it illegal for entities to send Kenyans' sensitive personal data outside the country.[144] Critics of this provision argue that sensitive data is too broadly defined, thereby limiting the private sector's ability to reap the economic gains achieved through cross-border data flow.[145] This may disproportionately affect small- and medium-sized businesses, which are more likely to outsource their consumers' data to foreign experts that handle data security and storage, instead of using their limited resources to build their own local data centers.[146]

As of late 2019, Kenya has still not passed this piece of draft legislation.[147] The Ministry of Information and Technology is currently reviewing the general public's comments about the legislation.[148] If this bill passes, Kenya will join Rwanda as the only two countries in East Africa to have data protection legislation in place.[149]

## III. ANALYSIS

As more countries prioritize the protection of consumer data, the rules on cross-border data transfers will become stricter.[150] As such, countries face significant economic risks if they lack adequate data protection regimes, especially given the exponential growth of the global digital economy.[151]

---

140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.*; *see also* Data Protection Act (2019) THE LAWS OF KENYA No. 19.
145. *See* Frizell, *supra* note 124.
146. *Id.*
147. *Id.*; *see also* Kenn Abuya, *Parliament Sets Public Participation Date for Data Protection Bill 2019*, TECH WEEZ (Aug. 13, 2019), https://techweez.com/2019/08/13/public-participation-data-protection-bill-2019/ [https://perma.cc/7F9M-3NGX] (archived Nov. 12, 2019).
148. *See* Frizell, *supra* note 124.
149. *Id.*
150. *See* Curtiss, *supra* note 9, at 107.
151. *Id.*

African countries are particularly at risk.[152] Admittedly, the cultural and economic differences between each African country make it difficult to articulate a one-size-fits-all analysis. However, there are several factors shared by African countries that complicate the continent's overall ability to achieve GDPR compliance. These factors demonstrate how the GDPR disproportionately affects and jeopardizes Africa's position in the global e-commerce market.[153]

### A. *Stifling Innovation, Investment, and Economic Growth*

Similar to countries that market themselves as tax havens, several African countries have adopted a relaxed approach to data privacy in order to attract companies seeking to avoid burdensome legal requirements.[154] For example, Kenya's relaxed regulatory approach led to the emergence of nearly 3,500 tech-related ventures in sub-Saharan Africa alone.[155] This also led to an increase in venture capital financing, with over $1 billion being invested into technology start-up companies from 2012 to 2018.[156]

Under the GDPR, however, African countries will no longer be able to market their relaxed regulatory environments as a way to drum up business, causing them to lose this competitive edge over other countries.[157] In turn, this could stifle Africa's current rate of digital innovation.[158] For countries like Kenya that have previously profited from lax privacy regimes, this legislative shift may foster ill will between the government and the private sector.[159] Small businesses may argue that the adoption of strong data privacy laws deprives newly formed companies from leveraging a lax regulatory environment—an advantage that allowed incumbent companies to flourish just years before.[160]

The shift to comprehensive data privacy regimes may also motivate some companies to take undue risks.[161] In weighing the high costs of compliance with the chance of being caught for noncompliance, some companies may take the gamble and continue existing business practices that do not comply with the GDPR. However, the stakes are high for GDPR violations, including fines of up to €20 million or 4 percent of annual global turnover, whichever is higher.[162] And

---

152. *Id.*
153. *Id.*
154. *See id.* at 118.
155. *See* Bright & Hruby, *supra* note 123.
156. *See id.*
157. *See* Curtiss, *supra* note 9, at 118.
158. *See id.*
159. *See id.*
160. *See id.*; *supra* Part II.
161. *See* Curtiss, *supra* note 9, at 114.
162. *See* GDPR, *supra* note 20.

although companies across the world can engage in such risky behavior, the reputational harm associated with this behavior arguably has a larger impact in developing countries.[163] Companies within such countries are competing to gain a foothold in the global market.[164] The risky behavior of one bad actor can taint the global perception of that country's market as a whole, negatively impacting the reputations of other companies that are in compliance with the GDPR. [165] This risk is particularly high in countries that lack regulatory and judicial bodies to enforce the newly adopted data privacy regimes.[166]

Finally, African companies could face investment losses if they fail to comply with the GDPR.[167] According to a recent survey conducted by PricewaterhouseCoopers, 38 percent of companies that have finalized their GDPR-compliance programs engaged their investor relations departments to market this compliance, indicating that these companies hope to highlight their early compliance as a potential differentiator in their markets.[168] As more companies begin marketing their own compliance achievements to investors, this may become a standardized disclosure that all investors look for, thereby disadvantaging companies that do not have the financial resources or expertise to reach this level of compliance. This same argument can also be applied to customer loyalty: if multiple companies begin touting their GDPR compliance to customers in order to strengthen customer trust in their businesses, then customers may soon come to expect such promises and thus discount companies that are unable to market this level of trust.[169]

### B. *Enforcement Issues*

Assuming African countries actually adopt comprehensive data privacy legislation, some of these countries lack stable judicial branches to effectively enforce the legislation and provide redress for violated rights.[170] This may be a key stumbling block for African countries seeking to comply with the GDPR under the first pathway:

---

163. *See, e.g.*, Curtiss, *supra* note 9, at 118.
164. *Id.*
165. *Id.*
166. *See id.* at 112.
167. *See SA companies doing business with EU need to consider making changes to their data privacy*, PRICEWATERHOUSECOOPERS S. AFR., https://www.pwc.co.za/en/press-room/sa-companies-eu-customers-changes-to-data-privacy.html (last visited Feb. 13, 2020) [https://perma.cc/38SJ-KTJN] (archived Nov. 12, 2019).
168. *Id.*
169. *See id.*
170. Curtiss, *supra* note 9, at 108.

national adoption of laws and regulations that comply with the GDPR.[171]

As explained in Part II of this Note, when the EU evaluates whether a country's data privacy legislation constitutes a satisfactory equivalent to the GDPR, it assesses whether the country can effectively implement and enforce this legislation, in addition to the country's overall commitment to the rule of law.[172] However, several African countries received low scores on the World Bank's Rule of Law Index—a data set that evaluates how much confidence agents have in each country's court system, the extent to which contractual and property rights are enforced in each country, and the likelihood that the rules of society are followed in each country.[173] For example, the Central African Republic has an overall score of -1.73, putting the country in the bottom 10 percent globally.[174] Countries with questionable judicial structures thus face an uphill battle in attempting to prove that their data privacy legislation is equivalent to the GDPR.[175]

Furthermore, even if these countries can pass GDPR-equivalent legislation, many of these countries would be unable to adequately enforce the legislation because of their undependable judicial systems. Many African court systems are reported to have extreme delays.[176] Additionally, studies show that some Africans do not trust their countries' judicial branches because of corruption concerns.[177] These issues may deter citizens from seeking redress for violations of their own data privacy rights.

Additionally, many African countries lack independent agencies to implement and enforce data protection legislation.[178] For example, although Mauritius has established a Data Protection Authority, the Authority institutionally depends on the Prime Minister's Office.[179] This may reduce the authority's ability to individually impose fines on entities that violate the country's data protection laws.[180] Additionally, some countries have not established a data protection authority at all, such as Cape Verde, even though many of these countries called for the

---

171. *See* DALBERG ADVISORS, *supra* note 13, at 8.

172. *See supra* Part II.

173. *Rule of Law Index*, WORLD BANK, https://tcdata360.worldbank.org/indicators/hf5cdd4dc?indicator=370&viz=choropleth&years=2017&compareBy=region (last visited Feb. 13, 2020) [https://perma.cc/GJF7-ZEWA] (archived Nov. 12, 2019) (the Rule of Law Index is being used as a proxy for evaluating the efficacy of judicial institutions in African countries).

174. *Id.*

175. *Id.*

176. *Id.*

177. Flourish Chukwurah, *Why Africans get a raw deal in the justice system*, CNN (May 5, 2017), https://www.cnn.com/2017/05/05/africa/access-justice-africa-view/index.html. [https://perma.cc/V7V8-QTAZ] (archived Nov. 12, 2019).

178. *See* DALBERG ADVISORS, *supra* note 13, at 8.

179. *Id.* at 9.

180. *Id.*

establishment of such authorities in their legislation. [181] Without independent agencies enforcing these laws, bad actors will continue to violate consumers' data privacy, leaving consumers with no redress for these invasions and risking the country's overall access to the EU's trading block.

Last, data protection may not be a priority for many African countries, given common concerns about corruption and public health. [182] For example, if an African country is dealing with issues concerning its citizens' access to clean water or safe housing, the country likely will not prioritize the adoption of comprehensive data privacy regulations. [183] Thus, some African countries may opt to devote their resources to combating these causes rather than creating effective data protection regimes. [184]

### C. *Issues with Technological Expertise*

Although the technological capacities of many African countries have skyrocketed in recent decades, technological inferiority may still be a hurdle for African companies seeking to comply with the GDPR. [185] Research shows that this potential hurdle largely stems from two sources: (1) a lack of local schools offering technological education to African citizens and (2) the migration of skilled labor to other markets—a phenomenon colloquially known as "brain drain." [186]

The promulgation of GDPR-type legislation in Africa would require these countries to invest more resources in technological education. [187] A technologically educated workforce is crucial to achieving and maintaining GDPR compliance. While some developing countries boast strong educational opportunities that churn out a technologically educated workforce, others lack robust educational infrastructures. [188] In turn, this educational deficiency may deter larger corporations from establishing offices in these areas, given concerns that there are not enough technologically educated workers to maintain operations in these offices. [189] Thus, even if these countries invest more in their education systems, there may not be enough job opportunities in the private sector to employ the recent graduates. [190]

---

181. *Id.*
182. *See* Curtiss, *supra* note 9, at 119.
183. *See id.*
184. *See id.*
185. *Id.* at 109.
186. *Id.*
187. *Id.*
188. *Id.*
189. *Id.*
190. *Id.*

This limited pool of qualified workers becomes even more problematic when considering brain drain.[191] Research shows that in 2013 one in nine Africans with a graduate-level education left the continent to live in developed areas like Europe, North America, and elsewhere.[192] There are several reasons why educated Africans may leave the continent, including political instability and the attraction of higher pay elsewhere.[193] According to the World Economic Forum's Global Competitiveness Report from 2014 to 2015, Burundi is the African country least able to hold onto its educated workforce, with countries like Algeria, Mauritania, Chad, and Guinea close behind.[194] Of course, the generalized dangers of brain drain are not present in every African country.[195] Rwanda, for example, has been reported to retain a large proportion of its educated workforce, as well as attract international talent.[196] Additionally, a portion of African workers leaving their home countries are moving to other countries within Africa that have more developed economies and industries, such as South Africa.[197] However, the issue is prevalent enough to lead South Africa's former president Thabo Mbeki to label Africa's brain drain issue as "frightening" in 2016.[198] Without a technologically sophisticated workforce, both the public and the private sectors risk violating the GDPR.[199]

### D. *Data Imperialism and the Brussels Effect*

The GDPR's one-size-fits-all approach does not take into account the different cultural, political, and economic realities existing in countries outside the EU.[200] This indifference led one critic to argue that the GDPR is "yet another diktat handed down by former colonial powers in a form of 'data imperialism.'"[201]

This so-called data imperialism is formally known as the Brussels Effect.[202] Coined by Columbia Law professor Anu Bradford in 2012, the Brussels Effect describes how the EU's global power can influence

---

191. *See* Scott Firsing, *How Severe is Africa's Brain Drain*, QUARTZ AFRICA (Jan. 21, 2016), https://qz.com/africa/599140/how-severe-is-africas-brain-drain/ [https://perma.cc/B6VG-T84B] (archived Nov. 12, 2019).
192. *Id.*
193. *Id.*
194. *Id.*
195. *Id.*
196. *Id.*
197. *Id.*
198. *Id.*
199. *See* Jeong, *supra* note 68.
200. Scott & Cerulus, *supra* note 1.
201. *Id.*
202. *See* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 1 (2015) (identifying "the unprecedented and deeply underestimated global power" known as the Brussels Effect).

other countries to adopt regulations similar to those adopted by the EU.[203] According to this theory, the combination of the EU's market influence and its use of extraterritorial regulations allows the EU to set strict regulatory standards for countries around the globe.[204] Other countries find that it is not economically or legally practical to maintain regulatory standards lower than those set by the EU, leading to the "Europeanization" of legal frameworks in developed and developing countries alike. [205] This regulatory globalization thus creates a "race to the top," whereby domestic regulations become increasingly more stringent as the global economy becomes more integrated.[206]

In the context of data privacy, the EU approaches issues like privacy, security, data protection, and rights differently than many African nations.[207] Through the Brussels Effect, local values in Africa may become obscured by Eurocentric ideals. This is particularly problematic considering the GDPR's strict take-it-or-leave-it approach. [208] Because the EU requires countries to either pass domestic laws that comply with the GDPR's expansive obligations or risk losing access to the world's largest trading block, countries may feel economically forced to bend to the EU's definition of data privacy.[209] Although the GDPR does not require countries to replicate the GDPR's provisions word-for-word in their own legislation, the EU's equivalency standard demands stricter legislation than some countries may have drafted on their own.[210] Countries like Kenya would no longer be able to perpetuate a lax regulatory environment in order to spur technological and economic growth.[211] Because of this, critics argue that the EU is using its economic muscle to impose its own definition of data privacy on countries around the world without concern for the unique economic circumstances in each country.[212]

---

203. *See id.* at 15.

204. *Id.*

205. *See* Anu Bradford, *Exporting Standards: The Externalization of the EU's Regulatory Power Via Markets*, 42 INT'L REV. L. & ECON. 158, 170 (2015).

206. *Id.* at 159.

207. *GDPR: Will It Be the Global Standard for Data Protection?*, CONSUMERS INT'L, https://www.consumersinternational.org/news-resources/blog/posts/gdpr-will-it-be-the-global-standard-for-data-protection/ (last visited Feb. 13, 2020) [https://perma.cc/7MZQ-3L87] (archived Nov. 12, 2019).

208. Scott & Cerulus, *supra* note 1.

209. *Id.*

210. *Id.*

211. *Id.*

212. *Id.*

## IV. SOLUTION

The above discussion begs the question: How can these complex issues be solved? Unfortunately, there are no easy solutions given the litany of complicating factors listed below.

First, the GDPR affects African nations in several ways—economically, politically, and culturally. The sheer breadth of these issues, as well as their overlapping effects, create multiple obstacles for African countries seeking to comply with the GDPR. What is more, the entire range of the GDPR's effects is not yet known.

Second, each African country has unique circumstances that require individualized responses. There is no one-size-fits-all solution here. For example, different countries are at different stages in their legislative processes. There are also varying levels of technological infrastructure, educational opportunities, and cultural viewpoints in each country. As such, each country's optimal response will be different.

Third, there is the question of who is responsible for working toward a solution. Some may argue that individual African countries must shoulder this responsibility—if these countries want to compete in the global e-commerce market, they must meet the qualifications. Others may argue that the EU has a responsibility to lessen the GDPR's impact on developing nations.

Fourth, it is unlikely that the EU will carve out exceptions for developing nations. The GDPR is intended to set global standards for data protection while giving users unprecedented autonomy over their data. The EU would jeopardize these idealistic goals if it suspended liability against African nations—even for a short period of time. EU residents may not be able to discern whether their data was being processed by a company in compliance with the GDPR or a company exempted under the GDPR, robbing these users of the ability to decide who gets to process their data for what purpose. There is also a high chance that data breaches could occur during this suspension period. Furthermore, if the EU broadly suspended liability against all African companies regardless of their compliance initiatives, some African companies may rest on their laurels during this period and fail to undertake important steps toward achieving GDPR compliance. This apathy would adversely impact those companies in the long term, reducing their abilities to achieve GDPR compliance once the EU lifts this suspension. For these reasons, a carve-out exemption for African nations is likely not the optimal solution.

Despite the above challenges, there are some critical steps that must be taken to reduce the GDPR's effects on different African nations. The below considerations are by no means a cure-all for these complex issues; much more will need to be done. However, the considerations listed below represent some solid first steps toward leveling the data privacy playing field in Africa.

### A. *Passing GDPR-Compliant Legislation at the Regional Level*

African countries need to propose and debate different legislative measures for data protection. These legislative efforts should likely occur at the regional level.[213] Regional initiatives sufficiently ensure that the individual realities of each country are accounted for in the legislative process. [214] This model may also prevent individual countries from hiding behind their own apathy toward passing such laws, thereby ensuring that a greater number of countries actively participate in this legislative process.[215]

To ensure these regional legislative efforts have a tangible impact, the African regions should mirror the GDPR in structuring their legislation as binding regulations, as compared to nonbinding directives like the African Union's Convention on Cyber Security and Personal Data Protection from 2014. [216] Otherwise, individual countries may not adopt or implement these data privacy frameworks. This nonaction could risk the region's overall access to the EU trading block and jeopardize economic growth in the regions' private sectors.

Admittedly, there are several drawbacks associated with legislating on the regional level. This model could result in another patchwork scheme where certain regions achieve GDPR compliance while others fall by the wayside. Issues like brain drain and educational disparity could still be present in this model. Furthermore, there are still social, legal, and economic differences between countries in each regional block that could complicate their legislative efforts. However, the group incentive of accessing the EU market may be enough to overcome these barriers, thereby giving African nations a better shot at achieving GDPR compliance on a wide scale.

### B. *Enforcing GDPR-Compliant Legislation at the Regional Level*

Once these regions pass data protection legislation, they should appoint data protection authorities to enforce the laws. Importantly, this enforcement should occur at the regional level, as opposed to the national level. This group process creates greater enforcement power, especially considering that several individual countries lack stable prosecution offices and judicial branches.

It is imperative that African governments take action. Individual companies achieving compliance at an organizational level is not enough by itself to achieve widespread GDPR compliance in Africa.[217]

---

213. *Id.*
214. *See id.*
215. *See id.*
216. *Id.*
217. *Id.*

This is for a variety of reasons. First, the process of achieving organizational compliance with the GDPR is lengthy and expensive, which may deter many companies from undertaking such efforts.[218] Second, a solely organizational approach would disadvantage small- and medium-sized businesses that lack the resources and expertise to achieve compliance at the organizational level.[219] This would be especially problematic in African countries that have a higher proportion of small- and medium-sized businesses, thus creating a larger economic impact in these countries.[220] Finally, aggrieved customers need reassurance from African governments that companies will be held legally responsible for breaches of their data privacy rights.[221] Without the adoption of data protection regulations at the governmental level, there would be no way to ensure the private sector is adequately protecting citizens' data privacy.[222]

Admittedly, there are several unanswered questions associated with this regional enforcement model. How should these agencies be structured? How should they decide which cases to pursue? Will these enforcement bodies be stable considering the lack of stability in some individual countries' own backyards?

Despite these unanswered questions and others, the regional enforcement model is a better solution than the alternatives. If these enforcement efforts were made on a continent-wide basis, the continental data authority may overlook the unique circumstances in each country, thereby creating unworkable enforcement frameworks. On the other hand, if individual countries took on this responsibility, countries that lack stable enforcement bodies would inevitably fall behind. An enforcement patchwork would emerge: some countries in Africa would have robust data protection, while others would have none at all. Because of these issues, the regional enforcement model gives African nations the best chance of achieving widespread GDPR compliance.

### C. *Investing in Technological Infrastructure and Training*

In order to achieve meaningful GDPR compliance in Africa, the private sector must also act. In a perfect world, these companies would begin striving toward compliance as soon as possible. Even a few months of delay could lead to massive profit losses for these companies, especially as their competitors achieve compliance in other countries.[223] Investors may come to consider GDPR compliance as a

---

218. *Id.*
219. *Id.*
220. *See id.*
221. *Id.*
222. *See id.*
223. *See* Panda Media Center, *supra* note 85.

prerequisite before investing in companies. [224] Furthermore, companies may require their commercial partners to be GDPR-compliant before entering into contracts with them. [225] If African companies delay achieving compliance, they may miss out on this business.

As these companies work to achieve GDPR compliance, they should temporarily block EU customers. Although this likely will lead to profit losses for these companies, the lost profits pale in comparison to the level of fines these companies could face were the EU to label them as noncompliant.[226] Indeed, the EU's top data protection officer, European data protection supervisor Giovanni Buttarrelli, warned regulators in April to be "vigilant about [companies'] attempts to game the system." [227] As such, companies must not cut any corners or interact with EU data subjects before they have achieved a reasonable level of compliance with the GDPR.

All of this is easier said than done. Achieving compliance will undoubtedly prove costly. For example, companies may need to invest in new technologies to safely collect and store consumers' data, as well as to monitor whether breaches have occurred and what data was compromised in those breaches. [228] Additionally, companies must invest resources into training their employees so they are aware of how to handle a breach when it occurs and how to prevent breaches. These initiatives may prove too costly for certain companies. Short of some type of government subsidy or private infusion of cash, many companies will be financially unable to comply with the GDPR.

## V. CONCLUSION

The GDPR will undoubtedly strengthen data protection across the world, giving users unprecedented control over how their personal data is collected, stored, and used. However, the GDPR's idealistic vision of consumer data creates several financial and regulatory challenges for governments and companies alike. This impact may be felt strongest by certain countries in Africa, many of which lack the existing regulatory frameworks and technological infrastructures needed to comply with the GDPR. Furthermore, the GDPR's extraterritoriality features may amount to data imperialism, allowing the EU to impose its own definition of data privacy on African countries without concern for their unique social values and economic realities. This may

224. *Id.*
225. *Id.*
226. *See* GDPR, *supra* note 20.
227. *See GDPR Q&A*, *supra* note 43.
228. *Id.*

jeopardize the dynamism and economic growth of many African countries.

There are no easy solutions for these complex issues. However, African nations should begin working toward a solution by taking certain steps, including passing regional legislation, creating regional enforcement authorities, and generating investment in technological infrastructures and trainings. These actions can help reduce the GDPR's disproportionate impact on African nations, allowing Africa to continue contributing to the global e-commerce market.

*Cara Mannion*[*]

---

* J.D. Candidate, 2020, Vanderbilt Law School; B.A. and B.S., 2014, University of Florida. I would like to dedicate this Note to my family: without your love and support, I would not be where I am today. And thank you to my fiancé, who offered encouragement every step of the way.

***