GENERAL DATA PROTECTION REGULATION (GDPR)

NOT JUST AN EU CONCERN:

THE IMPLICATIONS FOR AFRICA

January 2018

Dalberg Advisors

ACKNOWLEDGMENTS

This report was authored by Robin Miller, Keshinee Shah, Stan Getui, Simon Allan and Scott Hosking of Dalberg Advisors.

Dalberg Advisors is a strategic advisory firm focused on inclusive growth around the world. Dalberg's interest in the topic of data protection stems from a commitment to realizing the full potential of digital technology and data policy as a driver of inclusive growth.

This report was made possible by the generous contributions of time and expert knowledge from many individuals and organizations, and we would like to thank the following people: Alex B. Makulilo (Professor of Law and Technology, Open University of Tanzania), Jean-Baptiste Blanc (Business Law Attorney and Consultant; Sub-Saharan Africa legal expert), Erik van der Marel (Senior Economist, European Center for International Political Economy), Yasemin Genc (Commercial Attorney Lead, MEA CELA, Microsoft), and Louis Onyango Otieno (Director, Corporate Affairs – 4Afrika, Microsoft). This study was also invaluably shaped by the thought partnership of several colleagues at Dalberg.

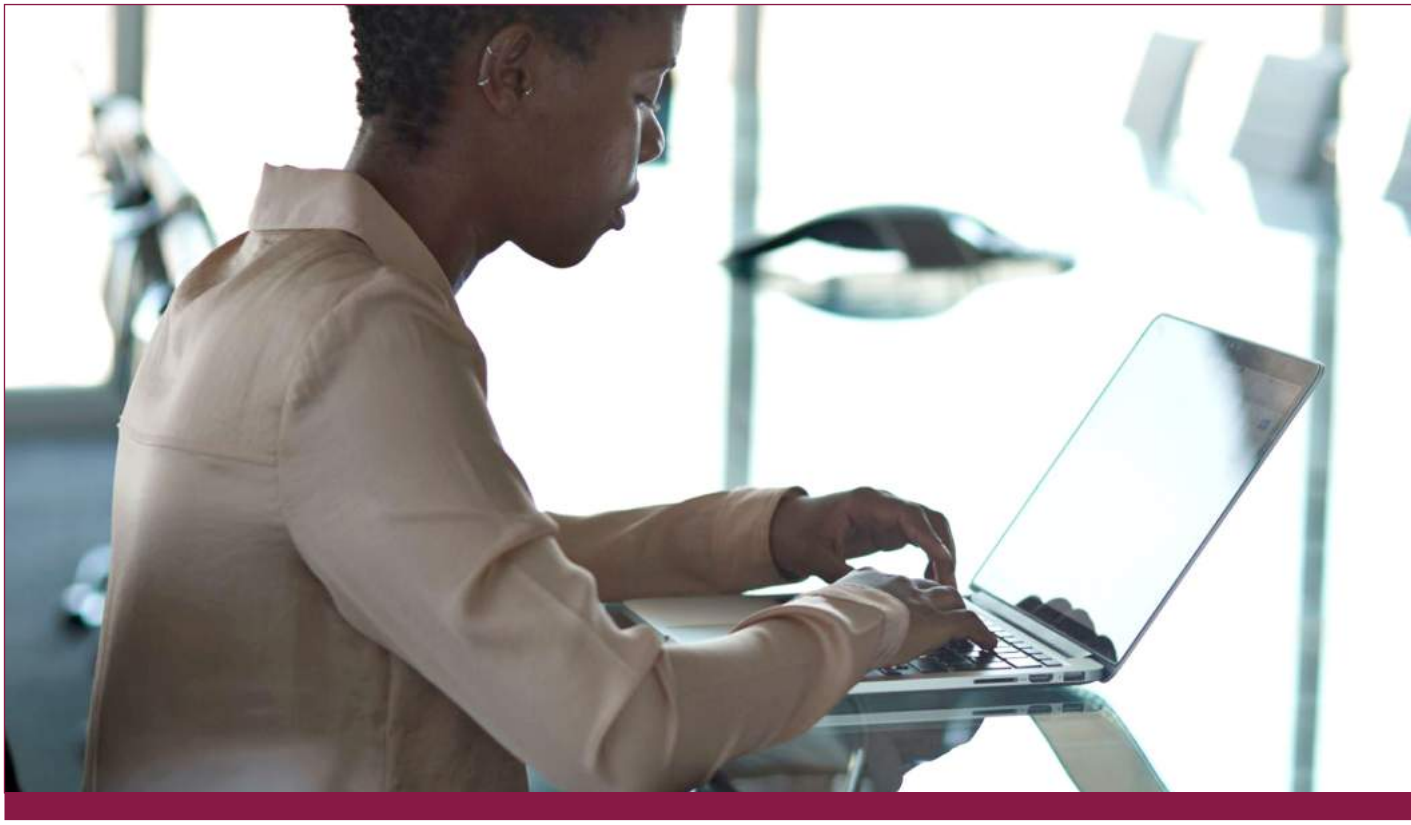
GENERAL DATA PROTECTION REGULATION (GDPR)

NOT JUST AN EU CONCERN:

THE IMPLICATIONS FOR AFRICA

January 2018

Contents



Abstract

In April 2016, the EU passed the General Data Protection Regulation (GDPR) focused on strengthening and harmonizing data protection laws across the EU and covering any global businesses that transact with the region. The GDPR comes into effect in May 2018.

The objective of this paper is to generate awareness of the forthcoming GDPR and encourage African governments to actively engage in dialogue to further data protection policies in their respective national development agendas. While the detailed merits of the GDPR are not considered here, we believe that the GDPR presents an opportunity to define the standard of consumer data protection in Africa and further the development of a regional digital economy.

These issues are expressed in the context of Nigeria and the countries that form the Common Market for Eastern and Southern Africa (COMESA). Noting their vulnerability to the impending changes, this paper aims to articulate themes to drive discussions at a regional level, and to highlight the important role of Nigeria[1] and COMESA [2] as large economic bases in Africa.

1 IMF, 2016: "World Economic Outlook – October 2016".

2 Office of the United States Trade Representative, 2017: "Common Market for Eastern and Southern Africa (COMESA)".

Executive Summary

Defining a standard of data protection is crucial to furthering the development of a regional and global digital economy. Importantly, it provides a basis for understanding the current state of data protection policies, offers an opportunity to design new frameworks that are consumer friendly and applicable to local citizens, and hence, are effective and sustainable.

The EUs General Data Protection Regulation (GDPR) presents a timely opportunity, particularly for regional trade blocs such as the Common Market for Eastern and Southern Africa (COMESA), to develop a framework for consumer data protection that is specific to the Africa region and its citizen, and safeguards trade with other countries and regions.

Importantly, as evidenced by the increasing number of countries globally aligning their data protection frameworks with the EU, the GDPR is currently deemed to be the global regulatory 'gold standard' for the protection of personal data of consumers. Essentially, countries with adequate data protection frameworks, and hence the ability to transfer data internationally, will have a distinct advantage in their ability to crowd in investment and advance trade with large consumer markets. As more countries align

$14b
of Africas digital economy export is at risk

No African Country is currently deemed compliant with GDPR

May 25, 2018
GDPR will come into effect

COMESA
can define the standard of GDPR in the region

with the EU on the importance of protecting consumer data in an increasingly global digital economy, rules on the cross-border transfer of data are likely to become stricter. Countries that do not have adequate levels of data protection face significant risks.

The absence of existing data protection frameworks and the lack of supporting services presents a significant challenge for most African countries. With no African country currently deemed to be compliant with the GDPR, its introduction risks disrupting the USD 14 billion in annual exports from Africa's digital economy to the EU. As the GDPR does not allow for partial compliance, countries will need to be deemed adequately compliant by the European Commission to protect their export industries.

The push to achieve adequate compliance with the GDPR at a national level is testament to the importance that governments place on applying a duty of care to citizens and organisations within their territory, as well protecting their national economic interest.

The GDPR comes into effect on 25 May 2018 and the pathway to achieving the required standard of adequate personal data protection is lengthy and complex. Countries within COMESA need to evaluate their legislative and enforcement frameworks as a priority. Where discrepancies arise, there is still time to engage the EU on alternative strategies or approaches.

In addition to defining the standard of consumer data protection in Africa, compliance with the GDPR is an opportunity for African countries to establish and strengthen strategic partnerships with the EU. Aligning on policy matters is often an important step towards fostering deeper relationships with large regional blocs, such as the EU

U.S. Department of Commerce Economics & Statistics Administration, 2016: "ICT-Enabled Services Trade in the EU".

1 Introduction to the General Data Protection Regulation

Defining the GDPR

The General Data Protection Regulation ("the GDPR") is a European Union (EU) regulation that aims to strengthen and harmonize laws within EU jurisdictions on: obtaining valid consent, collecting and processing data, increasing accountability, and regulating transfers of personal data across borders. It was passed as law in April 2016 and comes into effect on 25 May 2018[4]. The GDPR replaces the EU's Data Protection Directive ("the Directive"), which has been in place since 1995. The new regulation aims to develop a uniform approach to data protection in the EU and provides guidelines on how affected parties can meet adequacy requirements.

In an increasingly digital global economy, the overarching principle of the GDPR is to ensure a uniform and adequate level of data protection of EU data subjects[5]. The GDPR gives individuals full control over their personal data, emphasizing the need for explicit consumer consent to be obtained in a clear and simple manner. It has clear mechanisms for redressal and significant penalties for non-compliance. Fines under the GDPR are significant, with penalties for serious infringements set at the higher of EUR 20 million or 4% of an organisation's global annual turnover.[6]

The burden of proof under the new legislation lies with affected organisations. As a result, private organisations, particularly those with a large presence in Europe that recognize the consequences of non-compliance on their business, have begun implementing the parameters of the GDPR at an organisational level.

National compliance, however, is also important. By providing protection to all EU data subjects, the GDPR sets the tone for the global data protection agenda. Governments have a duty of care protect the data of their citizens and ensure their economies remain competitive and open to trade with dominant blocs such as the EU.

4 Official Journal of the European Union, 2016: "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (The GDPR)."

5 Data subjects are defined as any person located in the EU territory regardless of their nationality or residency

6 Ibid (note 4)

The importance of the GDPR for Africa

The GDPR's extended influence manifests itself through two channels: its extraterritorial scope and its data transfer regime.

The extraterritorial scope of the GDPR means that any organisation processing the personal data of EU data subjects, for the purposes of offering goods and services or monitoring their behaviour, is required to comply with GDPR provisions, regardless of where they are based or where the processing takes place.[7] While the responsibilities of organisations will change according to the nature of the processing, at a minimum, organisations covered by the scope of the legislation are expected to incorporate stricter security protocol, follow rules in relation to communicating with data subjects, and respect the rights enshrined in the GDPR.[8] In reality, the requirements are likely to be far more onerous. In many instances, an organisation will be expected to keep detailed records on the nature of its processing.[9] An organisation that regularly and systematically monitors data subjects on a large scale, or undertakes large scale processing of sensitive data or criminal records, is required to have both a data protection officer and an employee representing their interests based in the EU. Such organisations are also expected to undertake data protection impact assessments.[10] Figure 1 captures the likely scenarios for companies in COMESA.

Figure 1: Example scenarios of companies likely to fall under the scope of the GDPR[10]

Scenario	Directive applies?	GDPR applies?
Nigerian company without any EU subsidiaries offering free streaming services to individuals in the EU via a website hosted in Nigeria	X	✓
Ugandan hotel booking business using cookies to track past customers' (including EU-based customers) browsing in order to target specific hotel adverts to them	X	✓
Seychelles travel insurance company offering tailored packages to EU tourists based on their browsing history	X	✓
Tanzanian remittance company providing services for EU-based expatriates to send money back via a website	X	✓
Kenyan flower delivery company allowing data subjects in the EU to make orders for fulfilment in Kenya	X	✓
Egyptian gas extraction company with a branch office in Germany that has SO employees, and seeks to transfer their data to the global HR database	✓	✓
Mauritian retailer with a website for orders/deliveries. This website is accessible to individuals in the EU in English. The currency is the Mauritian rupee and the address field only allows Mautitian addresses	X	X

The data transfer regime ensures that personal data of EEA[12] data subjects is not sent to organisations in third-party countries that do not have adequate safeguards in place. As illustrated in Figure 2, meeting the standards set out in the data transfer regime can either be done at a national level – via an adequacy

7 Article 3 of the GDPR

8 For example, around direct marketing, contesting decisions on automatic processing, sensitive data and the right to be forgotten.

9 All organisations over 250 employees, and for organisations under 250 employees where the processing is of sensitive data, risky and regular.

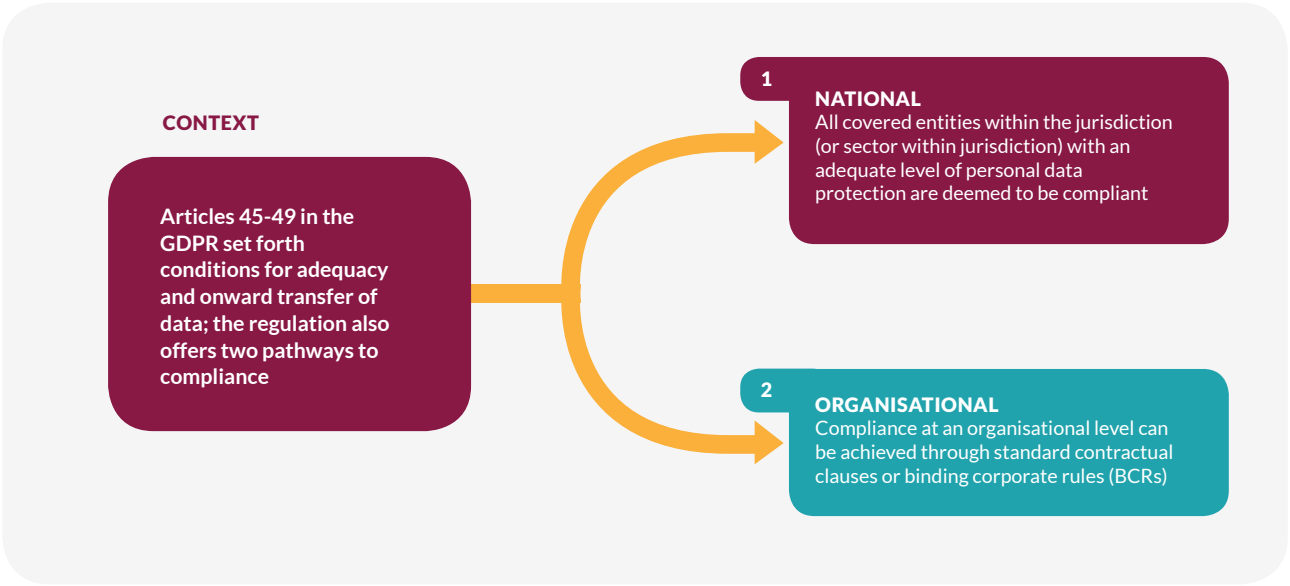
10 European Commission, 2017: "Data Protection- Better Rules for Small Businesses".

11 Based on examples from Slaughter & May 2016: "New Rules, Wider Reach: The Extra-Territorial Scope of the GDPR" and White & Case 2016: "Unlocking the EU General Data Protection Regulation: A Practical Handbook on the EU's New Data Protection Law", Chapter 4: Territorial Application.

12 The data transfer regime is applicable to all member states of the European Economic Area (including Lichtenstein, Iceland and Norway)

decision – or at the organisational level, whereby an organisation independently engages with the EU to show that it has requisite safeguards in place.[13] The first of these mechanisms involves an assessment of a country's data protection legislation and enforcement mechanisms, which are discussed later in this paper. The second of these mechanisms represents a significant barrier for African companies seeking to do business involving private data of EU data subjects. Striving for national compliance can remove these barriers and can be particularly beneficial for small and medium-sized enterprises (SMEs) that are less able to achieve compliance at the organisational level, given the resources required.

Figure 2: Pathways to compliance for the transfer of data



The data transfer regime and adequacy decisions

Adequacy at a national level does not involve point-for-point matching with the GDPR but does requires the law to offer a standard of data protection equivalent to that offered under the GDPR. Assessing whether the standard of data protection is adequate is based on evaluating whether the substance of the legislated principles and rights and their effective implementation, enforceability and supervision, deliver the required level of consumer data protection. Furthermore, a country's commitment to the rule of law and respect for human rights and fundamental freedoms, as well as international data protection commitments, are all important criteria to meet the 'adequacy' standard.[14]

The 'adequacy assessment framework' evaluates a country's data protection framework against the GDPR across three broad categories, as outlined in Figure 3. This framework is based on tests applied in assessments of adequacy under previous EU legislation, and incorporates new provisions laid out in the GDPR[15]. The first two categories capture the extent to which the provisions in a country's legal and regulatory framework align with the GDPR, and the third captures the extent to which they are effectively enforced.[16]

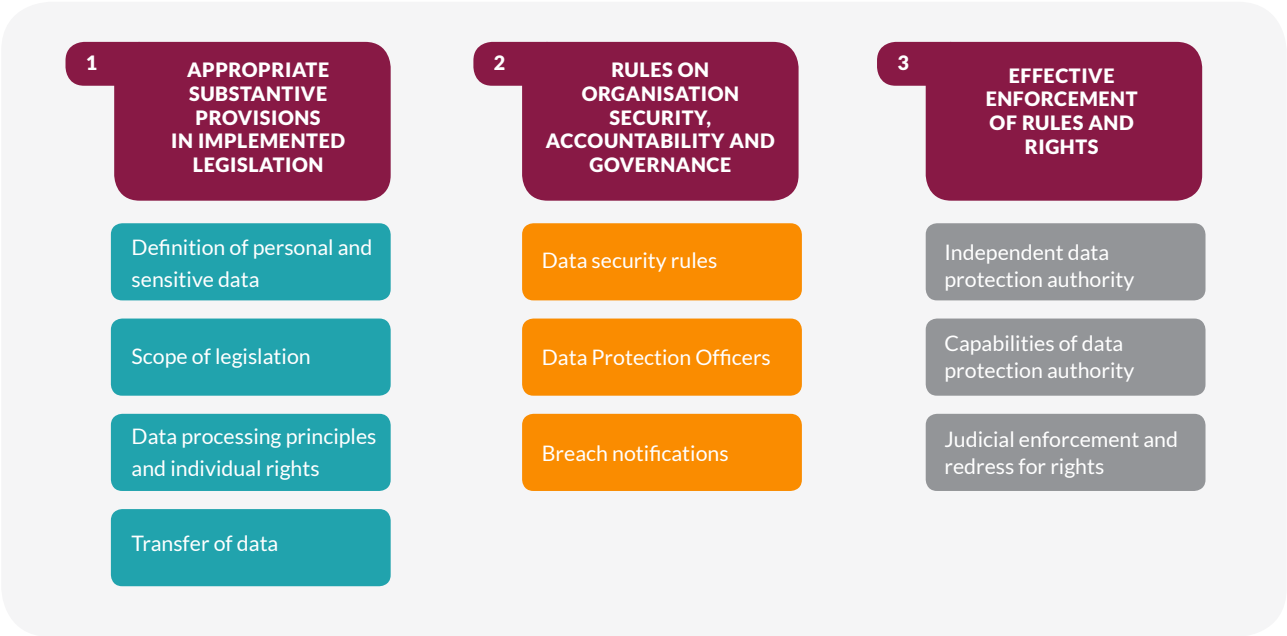
13 Articles 45-49 of the GDPR; There are isolated examples in Article 49 whereby businesses can transfer data without putting specific safeguards in place. Most importantly in this context when the data subject explicitly provides consent for the transfer.

14 European Commission, 2017: "Exchanging and Protecting Personal Data in a Globalised World"

15 Framework based on multiple sources: Article 29 Working Party: "Adequacy opinions on New Zealand and Israel"; Article 45 of the GDPR; Bird & Bird, 2017: "Guide to the General Data Protection Regulation"; DLA Piper, 2017: "Key changes in the GDPR"

16 It is important to note that African countries have almost universally used EU data privacy rules as a basis for their own privacy legislation and, therefore, in our assessment of their compliance, we directly map their legislation against the GDPR. We do however recognize that there may be some flexibility in this regard, which will emerge as adequacy decisions are made in the future.

Figure 3: Framework for adequacy assessment



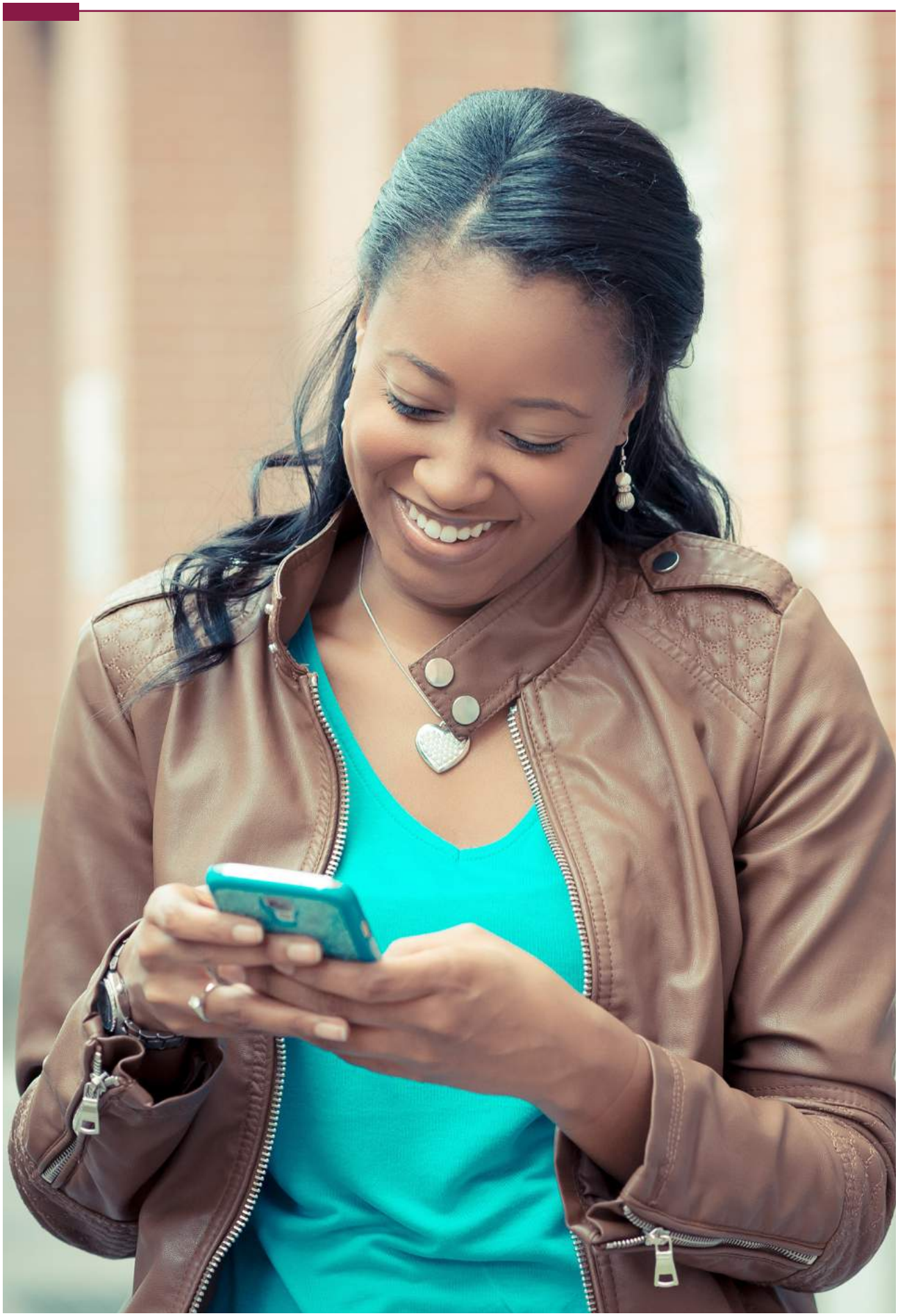
The pathway to adequacy is a journey for both countries and organisations. Figure 4 outlines proposed pathways for the two contexts. Importantly, while depicted as a linear pathway, compliance involves constantly adapting to new standards with the aim of remaining competitive.

Figure 4: Compliance journeys at the national and organisational level[17]

Highlighting step 3 of the national compliance journey – acceding to the Council of Europe Convention 108, which covers the protection of individuals with regards to automatic processing of personal data is currently deemed to be a key criterion for adequacy assessment under both the Directive and the GDPR. While accession does not automatically qualify countries for adequacy, it is the first formal step towards achieving adequacy under the GDPR.[18]

17 Based on Dalberg analysis

18 Council of Europe, 2017: "Details of Treaty No. 108".



2 How does Africa fare?

A continental lens

Regional bloc policymakers in Africa recognise the importance of data protection and have taken steps to develop data protection legislation.[19] While these steps are technically robust, to date, they have not resulted in significant changes at the country level. For example, the African Union's Convention on Cyber-Security and Personal Data Protection, which closely mirrors the former EU Directive on data protection, has had very little influence since it was adopted in 2014.

To date, the only country to ratify the Convention is Senegal; 15 countries need to do so for it to come into force. Other regional bodies that have put forward data protection codes are the East African Community (EAC) and the Southern African Development Community (SADC). However, their frameworks are non-binding and there is little evidence that they have shaped thinking at the national level. Potentially the most influential regional body in this regard has been the Economic Community of West African States (ECOWAS). The ECOWAS treaty includes a Supplementary Act on data protection, which requires member states to enact legislation to regulate the collection, processing, transmission, storage, and use of personal data.[20] Despite this, commentators have pointed out that the code has had relatively little influence at the national level; most member states that have data protection legislation, developed it prior to the Supplementary Act.[21]

At the national level, currently, only a third of African countries have comprehensive data protection legislation, with several standing out as leaders. Furthest on the journey are Mauritius and Senegal, which have been granted accession to the Council of Europe Convention 108 on data protection – an important milestone on the path to an 'adequacy decision', as noted earlier. Cape Verde, Tunisia and Morocco have also been invited to join the Convention. A closer look at Morocco provides some insight into key drivers for improving data protection legislation.

Morocco's data protection agenda has been heavily influenced by the EU's approach, and a desire to align legislation with it.[22] Several key catalysts have driven the evolution of Morocco's data protection legislation. One important driver has been the desire to protect the nation's fledgling outsourcing industry. Despite its proximity to Europe, Morocco recognized the disadvantage it had relative to other global players and adopted data protection laws to make it a more attractive market. Another key driver has been Morocco's participation as a signatory of the Euro-Mediterranean trade agreement, effective March 2000, which mandated it to institute laws that consider data protection and the fair processing of personal data. Finally, a push by the French data protection authority to ensure that all former French colonies adopted data protection laws has catalysed action in Morocco.

19 Makulilo, 2016: "Africa Data Privacy Laws".
20 The Supplementary Act becomes enforceable when published in a member state's gazette. See: Makulilo, 2016: "Africa Data Privacy Laws".
21 Stakeholder interview, 16 October 2017.
22 Ibid (note 18)


COVINOC

COMESA and Nigeria

There is some evidence that COMESA's 19-member countries or Nigeria have taken proactive steps to advance data protection; however, legislation on data protection across these countries is variable:[23]

• Three countries have data protection laws: Madagascar, Mauritius and the Seychelles.[24]
• Zimbabwe has data protection legislation that covers the public sector only, and a data protection bill currently in Parliament.
• Ethiopia, Kenya and Uganda have either draft data protection bills or bills currently in Parliament.
• Egypt, Malawi, Nigeria and Zambia have some data protection principles in common law and legislation; of these, Egypt and Nigeria have also drafted bills.
• Outside of constitutional references to data protection, Burundi, Comoros, Democratic Republic of the Congo, Djibouti, Eritrea, Libya, Rwanda, Sudan and Swaziland appear to have very limited focus on data protection in their legal systems.[25]

Among the countries that have drafted or enacted comprehensive data protection legislation, it is unlikely that any would be deemed compliant with the GDPR. Legislative gaps include weak onwards transfer regimes, limited recognition of sensitive data, and extensive derogations or exemptions in the application of the law.

Beyond this, the GDPR has introduced an additional set of standards for countries to attain 'essential equivalence' to the EU data protection regime. For example, the emphasis on accountability and security, with requirements of data protection officers, breach notifications and data protection impact assessments. It also introduces new rights for data subjects on data portability and data erasure and sets high standards with regards to consent and communication with data subjects.[26] Most of these elements are currently missing from legislation in COMESA countries and Nigeria.

In addition, the lack of an independent and effective enforcement agency is likely to be a key stumbling block for African countries seeking to improve their data protection frameworks. There are several different reasons for this; in many African countries that have data protection legislation, the data protection authority (DPA) is not completely independent and has little power. In Mauritius, for example, the DPA is materially and institutionally dependent on the Prime Minister's Office and is unable to administer fines to offenders. Similarly, in Ghana, the governing body of the DPA may receive ministerial directives on policy matters. In other cases, DPAs have simply not been established, despite being included in legislation, such as in Cape Verde.[27] More broadly, the ability of COMESA countries' legal systems to provide effective and accessible judicial redress – an important requirement for an 'adequacy decision' – is questionable, with many countries scoring poorly on the World Bank's Rule of Law Index.[28]

23 DLA Piper, "Data Protection Laws of The World"; Makulilo, 2016: "Africa Data Privacy Laws"; UNCTAD, "Data Protection and Privacy Legislation Worldwide". Norton Rose Fulbright, 2014: "Global Data Privacy Directory"

24 As of 2016, Seychelles data protection laws had not yet been fully implemented.

25 Based on high level analysis of publicly available information.

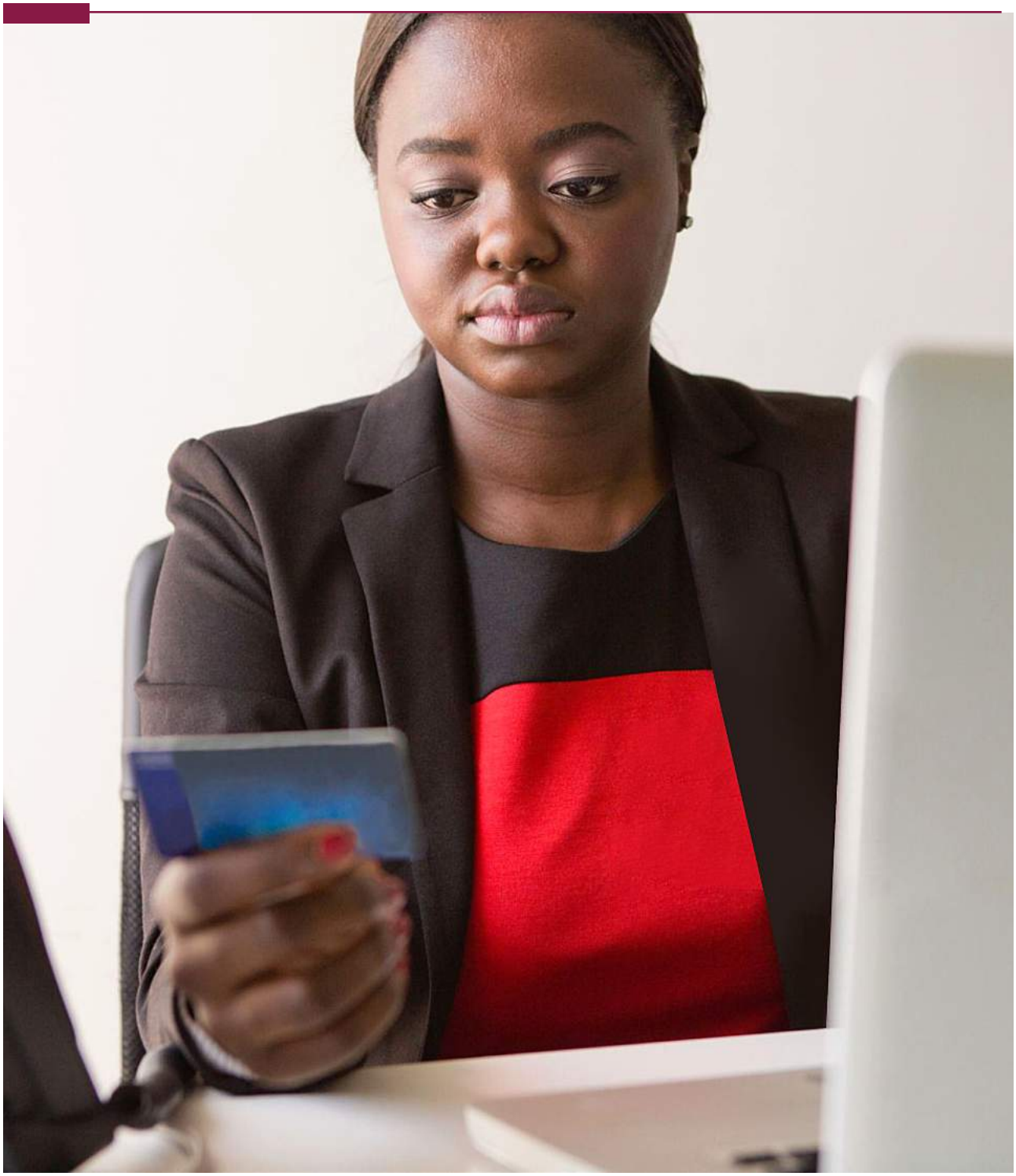
26 DLA Piper: "Data Protection Laws of The World"

27 Makulilo, 2016: "Africa Data Privacy Laws".

28 This was used as a proxy for judicial enforcement and redress for rights.

A long way to go on the journey

No country in Africa is currently compliant with the GDPR. While some countries are further along the path than others, all countries still have a long way to go. For many, data protection is simply not a priority. For others that have recognised the importance of data protection, taking the next step requires strengthening and refining provisions and adopting these provisions into national law. For the rest, improving the overall implementation and enforcement of existing legislation is key.



3 Opportunities and implications

Achieving compliance presents an opportunity for African countries to increase their participation in the global digital economy – an economy that is currently concentrated among a small set of developed economies.

New digital platforms are reducing the costs of cross-border communications and transactions, thereby lessening the barriers to entry. Moreover, the global harmonization of data protection regulation, starting with the GDPR, means that countries will likely have to comply with fewer pieces of legislation to trade within this digital market. Accelerating participation in the global digital economy has been estimated to increase national growth rates by more than 50%.[29]

Achieving national compliance is the most efficient route to connecting all organisations to this global economy. While large multinational organisations may find it easy to achieve compliance by replicating data protection systems and norms from their compliant EU-based affiliates, SMEs may be less able to achieve compliance in the short-term as they have fewer resources and less experience in dealing with international data protection regulations. This could have substantial economic impacts; the World Bank estimates that formal SMEs contribute up to 40% of national income in emerging economies.[30]

Achieving national compliance is the most efficient route to connecting all organisations to this global economy.

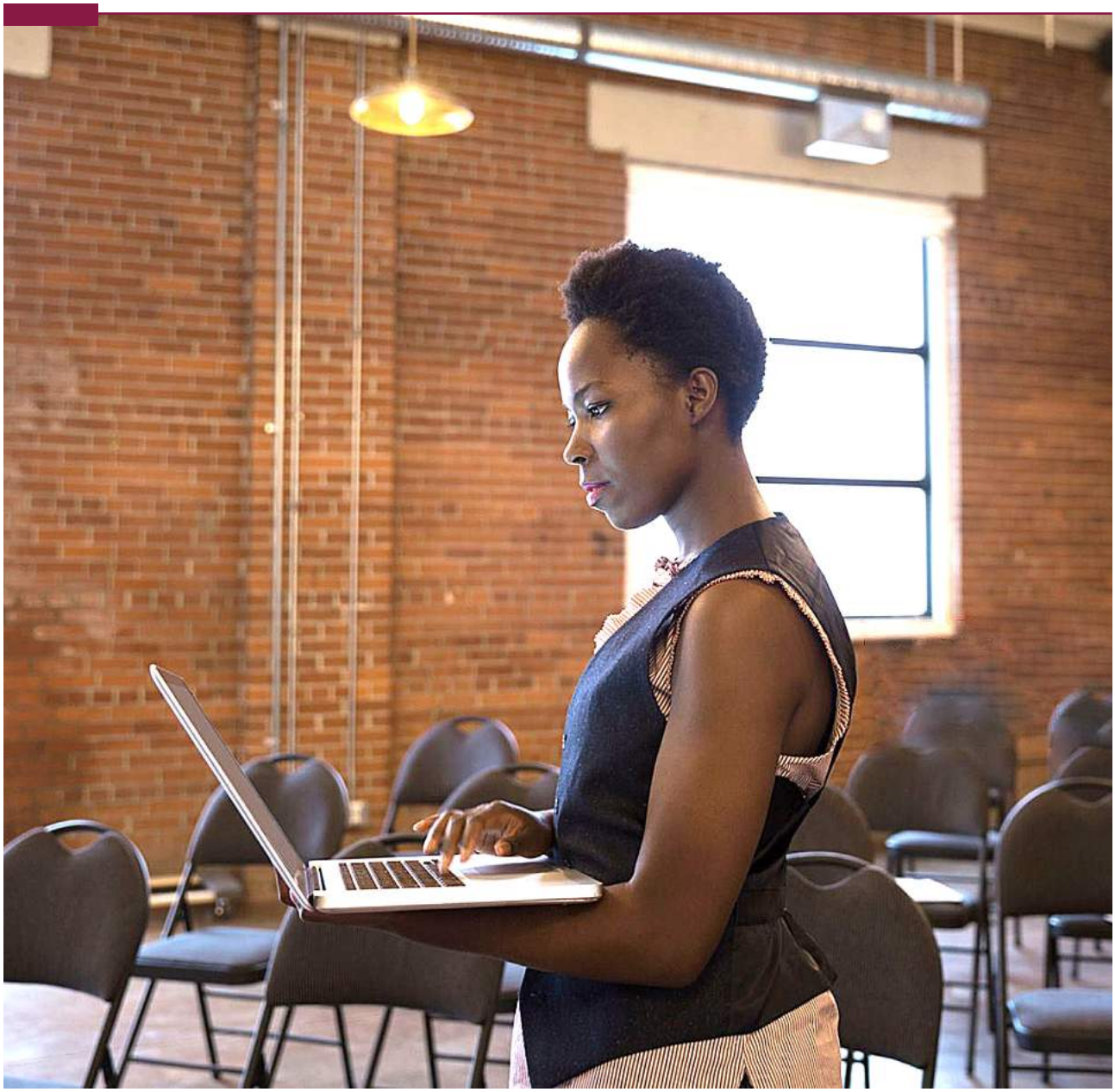
Non-compliance with the GDPR risks disrupting the USD 14 billion in annual exports from Africa's digital economy to the EU.[31] The sectors that will be most affected by the GDPR are those that currently rely heavily on cross-border flows of data – telecommunications, business and ICT services, financial services, and tourism. [32]

In the longer term, as the global flow of data continues to increase, the economic impact for Africa is expected to be increase substantially. Cross-border data flows currently generate more economic value than flows of traded goods.[34] Between 2005 and 2014, the global flow of data increased by a factor of 45 to a value of USD 2.8 trillion.[34] This upwards trend is expected to continue, driven by the increasing use of data in digital sectors and the adoption of data-intensive processes in additional sectors such as logistics and management services.[35] The EU is one of Africa's largest export markets, and the annual value of COMESA exports to the EU alone is more than USD 35 billion.[36]

28 U.S. Department of Commerce Economics & Statistics Administration, 2016: "ICT-Enabled Services Trade in the EU".
29 UNCTAD, 2015: "International Trade in ICT Services and ICT-Enabled Services, Proposed Indicators from the Partnership on Measuring ICT for Development".
30 MGI, 2016: "Digital Globalization: The New Era of Global Flows".
31 The global flow of data is measured in terms of used cross-border bandwidth (Gigabits per second). See: MGI, 2016: "Digital Globalization: The New Era of Global Flows".
32 Stakeholder interview, 09 October 2017.
33 European Commission data, Extra-EU Trade by Partner. Conversion of EUR 18.6 billion in goods exports based on average annual exchange rates for 2016 taken from Oanda. Conversion of EUR 10.9 billion in services exports based on average annual exchange rates for 2012 taken from Oanda.
34 If a U.S. company processes data on EU citizens, then it must comply with the GDPR. In this situation, the company may find it more cost-effective to apply the same regulations to all its trading partners, thus having a knock-on effect on companies and countries that may not trade with the EU, but are now subject to EU data protection regulations.
35 International Trade Statistics data, International Trade in Goods and Services, 2015.
36 MGI, 2016: "Digital Globalization: The New Era of Global Flows".

As noted earlier, the GDPR [37] is currently the global standard for data protection. As an increasing number of countries and organisations align their norms with the GDPR, and given the onward obligations of complying with the GDPR, non-compliance is likely to impact global African exports, not just those to the EU. In 2015 alone, Africa exported a total of USD 366 billion in goods and USD 100 billion in services to the rest of the world, a substantial volume of trade to risk.[38]

In addition to safeguarding trade, compliance with the GDPR provides an opportunity for African countries to establish and strengthen strategic partnerships with the EU. Aligning on policy matters is often an important step towards fostering deeper relationships with large regional blocs, such as the EU.



37 World Bank: "Small and Medium Enterprises (SMEs) Finance".

38 International Trade Statistics data, International Trade in Goods and Services, 2015.

4 What next?

Consumer data protection is crucial to the broader "Africa Rising" narrative, and should be prioritized as part of the region's agenda. COMESA is well positioned to facilitate regional cooperation in Africa by engaging its members and, on their behalf, engaging in dialogue with the EU on matters of data protection.

The shift in data protection policy is an opportunity for African countries to enact stronger laws and become leaders in the digital economy. Adequate compliance with the GDPR focuses on ensuring that a country has the right enabling environment and regulations to protect the rights of data subjects. The GDPR, therefore, acts as a standard for the protection of all citizens. COMESA countries have an opportunity to define the standard of data protection in the region and further the development of a regional digital economy.

African governments ought to take a proactive rather than reactive stance to the GDPR

COMESA countries need to urgently examine their own data protection regimes to ensure they meet the standard of adequate consumer data protection required by the GDPR and tailored to African citizens. They should evaluate their legislative and enforcement frameworks, and consider the pros and cons of moving towards alignment with GDPR. Where discrepancies arise, COMESA may be well positioned to engage the EU on alternative strategies or approaches.

African governments ought to take a proactive rather than reactive stance to the GDPR. Governments have the dual responsibility of protecting the data of their citizens while ensuring their economies remain competitive and open to trade with dominant regional blocs such as the EU. As such, national governments should facilitate the efficient development of new and updated national legislation while extending support to affected organisations in Africa. Organisations and trade unions also have a key role to play in sharing learnings with policymakers.

5 Conclusion

Providing an enabling environment for the development and enforcement of policy is a primary success factor for economic growth, and is particularly important for the digital economy.[39] A transparent system that can be trusted by all actors is essential to the use and growth of ICT, especially in emerging economies.[40] National governments and regional bodies must enact relevant laws and ensure that the regulators are sufficiently equipped to implement them. The transparency of these processes will indicate support for wider market-based regulatory reform, boost confidence in ICT sectors, and more importantly foster a culture that respects the rule of law and protects the rights of the individual.

The global digital economy creates more than USD 3 trillion in value add per year.[41] Although not immediately measurable, Africa has significant exposure to this with 30% of industries digitized[42] and mobile services contributing to 7% of the continent's annual GDP of USD 3 trillion.[43] As digital services become an integral part of doing business, the impact of data protection laws will be felt both globally and closer to home within COMESA.

In the short term, the impact on COMESA countries will be significant in terms of cost of compliance and potential ramifications of loss of trade with the EU. In the longer term, the lack of globally-accepted data protection standards is likely to impact COMESA's trade with all countries. As a trade-focused organisation, COMESA has a duty of care to minimise risk to its members.

Immediate priorities for COMESA include formalising regional engagement, increasing awareness of the GDPR, establishing a framework for data protection, and catalysing the implementation of a data protection ecosystem. There is evidence of progress but the region is still far from achieving the minimum data protection. In the absence of a governing body or data protection office in the region, COMESA – through its ICT Working Group – is well placed to take a leading role in driving this agenda.

39 Guermazi, B and Satola, D, 2005: "E-development: From Excitement to Effectiveness: Chapter 2 - Creating the "Right" Enabling Environment for ICT".
40 Ibid (note 36)
41 MGI, 2016: "Digital globalization report".
42 PwC, 2016: "Industry 4.0, building your digital enterprise".
43 Amatka, 2016: "The Future of Digital Business Models in sub-Saharan Africa".

Dalberg Advisors