# Challenges and Prospects of the **General Data Protection Regulation (GDPR) in Africa**

**July** 2018

## Introduction

Privacy is a fundamental human right guaranteed by international human rights instruments including the Universal Declaration of Human Rights in its article 12 and the International Covenant on Civil and Political Rights, in its article 17. Further, these provisions have been embedded in different jurisdictions in national constitutions and in acts of Parliament.

In Africa, regional bodies have invested efforts in ensuring that data protection and privacy are prioritised by Member States. For instance, in 2014 the African Union (AU) adopted the Convention on Cybersecurity and Personal Data Protection. In 2010, the Southern African Development Community (SADC) developed a model law on data protection which it adopted in 2013. Also in 2010, the Economic Community of West African States (ECOWAS) adopted the Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWAS. The East African Community, in 2008, developed a Framework for Cyberlaws. Notwithstanding these efforts, many countries on the continent are still grappling with enacting specific legislation to regulate the collection, control and processing of individuals' data.

On May 25, 2018, the European Union's General Data Protection Regulation (GDPR) came into effect. The GDPR is likely to force African countries, especially those with strong trade ties to the EU, to prioritise data privacy and to more decisively meet their duties and obligations to ensure compliance. In this brief, we explore the consequences of GDPR for African states and business entities.

## Application and Force of the General Data Protection Regulation

Prior to the coming into effect of the General Data Protection Regulation (GDPR) in May 2018, entities based in America and the European Union (EU) made frantic updates and changes to their privacy policies and end user agreements in order to comply with the GDPR. Among the key areas of compliance is Article 1 of the GDPR, which lays down the subject matter and objectives of the regulation as protecting EU natural persons (subjects) with regards to the processing of personal data and rules relating to the free movement of personal data. It makes it a requirement for companies and entities serving EU subjects to ask for subjects' data in a clear and accessible language. Additional requirements include the deletion of data should a subject request for it; accounting of how and why subjects' data is processed; and upon request, providing subjects with copies of their data in machine readable format. Further, other rights that accrue to the data subject such as the right to erasure, data portability, consent, right to know, rectification, and right to be informed, have been prioritised.[1] Infringement of provisions of the GDPR may result in administrative fines of up to Euro 20 million, or up to 4% of an entity's annual turnover.[2]

The GDPR applies in jurisdictions outside the EU provided they handle personal data of EU citizens. It is an important step towards individuals' participation in privacy regimes and sets a benchmark for global best practice in privacy and data protection. Below, we explore the challenges and prospects of the Regulation in Africa.

1 *Data subject rights and personal information: data subject rights under the GDPR, https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/; see also the GDPR, Chapter III on the rights of the data subject especially article 12 on transparency; article 13, 14 and 15, on information and access to personal data; article 16 and 17, 18, 19, on rectification and erasure; article 20 on data portability; and articles 21 and 22 on the Right to object and automated individual decision-making.*

2 *What is GDPR? The summary guide to GDPR compliance in the UK, http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018; see also GDPR fines: How high are they, and how can you avoid them?, available at http://www.itpro.co.uk/general-data-protection-regulation-gdpr/31025/gdpr-fines-how-high-are-they-and-how-can-you-avoid*

## Inadequacy and Unavailability of Data Protection and Privacy legislation

With the coming into force of the GDPR, African countries are expected to hasten the processes of passing data protection and privacy legislation, or ensuring that protections in existing legislation are aligned with the GDPR.

To-date, only 16 out of 54 countries in Africa have data protection laws. These are Angola (2016), Benin (2009), Burkina Faso (2004), Equatorial Guinea (2016), Gabon (2011), Ghana (2012), Ivory Coast (2013), Lesotho (2012), Madagascar (2014), Mauritania (2017), Morocco (2009), Senegal (2008), South Africa (2013), Mali (2013), Tunisia (2004), and Zimbabwe (2003).[3] A few others, such as Uganda, Kenya, Nigeria, Tanzania and Niger, have Bills awaiting enactment.[4] Moreover, the Convention on Cyber Security and Personal Data protection adopted by the African Union in 2014 has only ten signatories (Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia) and two ratifications (Mauritius and Senegal).[5]

Even with the existing legislation in some African states, the EU may not fully recognise their capacity to adequately protect personal data and privacy especially in respect to data collection, control and processing.[6] Below are some ways in which African legislations falls short.

## Consent to Data Collection

Consent to collection of one's personal data is an important aspect of the GDPR.[7] Further, valid consent must be obtained prior to the collection of data, especially through clear stipulation of the purpose of data collection and indication of the need for additional consent where personal data might be shared with third parties.[8] The GDPR requires that data controllers take and keep record of consent of individuals. Further, there must be provision for withdrawal of consent by the data subject at any time. Many of the African legislation and bills either lack, or do not adequately provide for the element of consent. For example, in Lesotho, section 15 (2) and 17 (1) (b) of the Act provides for explicit consent and collection to data processing respectively yet under section 25 there are arbitrary circumstances where the data controller may not comply with consent provisions in respect of personal data. Further, the Data Protection and Privacy Bill, 2015 for Uganda merely provides that collection and processing of personal data may only be done with the consent of the data subject but does not spell out the different ways and processes of obtaining consent nor does it spell out the extent of consent that should be obtained. Similarly, section 20 of Data Protection Act, 2012 for Ghana has similar provisions to Uganda's.

Hence under the GDPR, data of European subjects may not be collected by African governments, organisations and businesses in violation of or noncompliance with regulation.[9] Such an action would have costs, including loss of EU clients.[10] Further, governments may have to invest more resources in law making processes to ensure that data is given due protection. Nevertheless, controversy may arise especially in cases where users and visitors of websites do not bother to read terms and conditions and privacy policies but rush to the check box to swiftly access the site. It still remains a challenge for enforcement where there is breach.[11]

3 *What African Countries Can Learn from European Privacy Laws and Policies, https://cipesa.org/2017/07/what-african-countries-can-learn-from-european-privacy-laws-and-policies/*
4 *Ibid.*
5 *Status of ratification is available at https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf*
6 *Data protection around the world, https://www.cnil.fr/en/data-protection-around-the-world*
7 *For example article 7 of the GDPR provides for conditions for consent to data processing*
8 *The top five impacts of GDPR on the financial services industry, https://www.consultancy.uk/news/14478/the-top-five-impacts-of-gdpr-on-the-financial-services-industry (accessed May 23, 2018).*
9 *What is GDPR? Everything you need to know before the 2018 deadline, http://www.itpro.co.uk/it-legislation/27814/what-is-gdpr-everything-you-need-to-know*
10 *Businesses in Africa Prepare for EU General Data Protection Regulation, https://www.lexology.com/library/detail.aspx?g=9d6900e5-be97-475f-9a64-08d28c778467*
11 *GDPR and how it will affect your website, https://kaleidoko.com/gdpr-will-affect-website/*

## Data Processing

In established data protection regimes, data controllers are required to process personal data within the law, in a transparent manner and for an intended purpose.[12] In addition to the GDPR and the Convention on Cyber Security and Personal Data protection, the requirement for personal data protection and processing has been emphasised in the Organisation for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data.[13] The OECD guidelines emphasise eight principles including limitation in data collection; data quality control; data collection purpose; user limitation; establishment of security safeguards; openness, the individual's right especially regarding participation; and accountability for compliance with measures undertaken.[14] In Burundi, Egypt, Ethiopia, Kenya, Mauritania, Nigeria, Rwanda, Senegal, South Sudan, Tanzania, Uganda and Zimbabwe, there has been no strict adherence to data processing principles with data breaches such as surveillance, interception by state security agencies and private entities remaining rampant.[15] With the cross border application of the GDPR, Africa entities will be required to comply and ensure that that personal data only serves intended purposes beyond which it should be collected. This will also guarantee protection and safety of personal data.

## Transferability of Data

The GDPR imposes a potentially huge administrative fine to illicit transfers of personal data to a recipient in a third country or international organisation.[16] A few exceptions can only arise in cases of limited transfers based on legitimate interests but with high level regard to protection of personal data.[17] Further, transfers may be permitted in cases of international agreements between the EU and third countries.[18] According to articles 44 to 50 of the GDPR, data transfers are subject to sufficient safeguards in accordance with the Regulation. The requirement for appropriate safeguards places an obligation on African countries to sufficiently address the issue of data portability and transferability of personal data across borders. Although some African countries attempt to address transferability and data processing in other jurisdictions, the provisions are inadequate.

For instance, Uganda's Bill on Data protection and Privacy under clause 15 imposes a duty on the data processor or data controller who processes personal data to ensure that a country in which data is processed has adequate measures for personal data protection. A similar provision is found in section 18 of the Data Protection Act, 2012 of Ghana. However, section 64 of the Data Protection Act, 2013 of Lesotho imposes the control measures to non-SADC member countries. African countries are accordingly expected to offer similar detailed personal data protection as the GDPR when handling European data subjects.

## Reporting Data Breaches

Given the absence of data protection and privacy legislation in majority of African countries, most data breaches may go undocumented or unreported to the data subjects. For instance, section 31 of the Data Protection Act, 2012 of Ghana and section 23 of the Data Protection Act, 2013 of Lesotho also provide for delay of informing the data subject of breaches in some situations. The Uganda Data Protection and Privacy Bill, 2015 under clause 19 requires a data collector, data processor or data controller to report data breaches to the authority, and it is the authority required to determine and notify the data controller whether they should notify the data subject of the breach.

In some countries, such as Cape Verde Egypt Angola Seychelles, Zimbabwe; and Nigeria; with either data protection laws or scanty provisions on data protection in various pieces of legislation, it is not mandatory to report data breaches to the authority. [19] Further, in countries like Madagascar; Mauritius there is no general or specific obligation to notify the data authority or data subject of a data security breach.[20] The GDPR, under article 33, requires reporting of data breaches within 72 hours to the supervisory authority and to concerned parties if the breach poses an implementation challenge. Data protection and privacy laws in Africa will therefore have to establish adequate notification mechanisms in the event of data breaches.

12 *What is GDPR? Everything you need to know before the 2018 deadline, http://www.itpro.co.uk/it-legislation/27814/what-is-gdpr-everything-you-need-to-know; see also articles 5, 6, 7, 8, 9, 10, 11 of the GDPR processing of personal data.*

13 *The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data are available at https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf*

14 *Ibid.*

15 *See for instance, The Right to Privacy in Uganda, https://cipesa.org/?wpfb_dl=217; Provision Of Real-Time Lawful Interception Assistance, http://www.telecomindustrydialogue.org/resources/kenya/ GDPR, Third Countries https://gdpr-info.eu/issues/third-countries/*

16 *Paragraph 6 of the Preamble to the GDPR.*

17 *Paragraph 101 and 102 of the Preamble to the GDPR*

18 *Data Protection Laws of the World Full Handbook, https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all*

19 *https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all*

20 *Ibid.,p.304*

## Possible impact on African Businesses

In November 2017, the EU announced a Euro 44 billion fund towards its External Investment Plan (EIP) for of sustainable investment for Africa and the EU neighbouring countries.[21] With this increased business investments in Africa by the European Union through Economic Partnership Agreements (EPAs), adherence to the GDPR by African entities will likely determine whether they attract or retain more European business partners.[22] Besides, the pressure to adhere will be prevalent among those entities which frequently interact with EU subjects' data. One such example is the airline industry, a sector which is increasingly growing on the continent.[23] Indeed, some operators have issued GDPR compliance notices to their clients.[24]

To ensure that innovators and business entities in Africa remain competitive and avoid hefty fines under the GDPR, capacity enhancement in infrastructure and human resources to ensure appropriate data collection, storage and processing will be required. They must for instance ensure that privacy by default is part of their software creations and find ways of avoiding being data processors.[25] Additionally, they must take all the necessary precautions to ensure that all software designed is either categorised as having access to personal data or take the necessary precautionary measures.[26] Inevitably, this would have cost implications and the threat of multiple lawsuits from aggrieved EU based data subjects.[27]

## Conclusion

The GDPR is a reality that buttresses mechanisms for protection of data and individual privacy across the globe for EU subjects. It offers challenges and opportunities for African countries to firstly comply with key personal data aspects including collection and processing, consent by data subjects, portability and transferability of data as well as access to personal data by the data subject. Secondly, it provides the opportunity for the data subjects to enforce their rights in cases of breach by the relevant authority.

To the contrary while the GDPR guarantees extra-territorial protection to EU subjects, it is unclear how it will be enforced especially in cases where EU subjects deal with other jurisdictions taking into consideration the state sovereignty doctrine and enforcement of judgments.

Finally, the GDPR offers African nations an opportunity to strengthen their data protection and privacy policy and practice towards attracting partnerships with EU-based businesses and governments and remaining competitive in an increasingly global marketplace. Further, harmonisation of data protection regimes would ensure that individual rights are placed over and above the interests of governments, business and organisations.

21 *The European Union's External Investment Plan: Green Light for the First Five Investment Areas,http://europa.eu/rapid/press-release_IP-17-4884_en.htm*

22 *GDPR - what it means to South African companies, https://www.itweb.co.za/content/rxP3jqBp6XY7A2ye*

23 *Aviation as a catalyst for growth in Africa, https://www.howwemadeitinafrica.com/aviation-catalyst-growth-africa/*

24 *Kenya Airways, Our Privacy Policy, https://www.kenya-airways.com/privacy-policy/en/ ; and Avocats Sans Frontières, Legal notices & privacy policy, https://www.asf.be/legal-notices/ ; see also Air Help, https://www.airhelp.com/en/privacy/*

25 *What Should Software Engineers Know about GDPR?, https://www.infoq.com/articles/gdpr-for-software-devs*

26 *3 things software engineers need to know about the GDPR, https://www.itgovernance.eu/blog/en/3-things-software-engineers-need-to-know-about-the-gdpr*

27 *GDPR - what it means to South African companies, https://www.itweb.co.za/content/rxP3jqBp6XY7A2ye .*

.

**About CIPESA**

CIPESA

CIPESA was established in 2004 under the Catalysing Access to Information and Communications Technologies in Africa (CATIA) initiative, which was mainly funded by the UK's Department for International Development (DfID). CIPESA is a leading centre for research and the analysis of information aimed to enable policy makers in East and Southern Africa understand ICT policy issues and for various stakeholders to use ICT to improve governance and livelihoods.

programmes@cipesa.org @cipesaug @cipesaug www.cipesa.org