
accessnow
DATA PROTECTION IN KENYA
HOW IS THIS RIGHT PROTECTED?
accessnow.org
Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

DATA PROTECTION IN KENYA

How is this right protected?

This report is an Access Now publication. It is written by Bridget Andere. We would like to thank the Access Now team members who provided support, in particular Estelle Massé, Gaspar Pisanu, Alexia Skok and Elias Okwara. We would also like to thank Mugambi Laibuta for his feedback and contributions.

For more information, please visit:
https://www.accessnow.org

Contact: **Bridget Andere** | bridget@accessnow.org

EXECUTIVE SUMMARY | OCTOBER 2021

Kenya enacted a comprehensive data protection legislation in 2019 that has often been touted as mirroring the EU General Data Protection Regulation. It has been just a few months shy of two years since the Data Protection Act in Kenya came into effect. In that time, the Office of the Data Protection Commissioner (ODPC) has been established as provided for in the Act; and with that has also come a number of operationalising provisions developed by the ODPC in consultation with the Ministry of Information, Communication and Technology.

While remaining cognizant of the reality that data protection act is progressive and contains provisions essential to the realisation of the right to privacy and general data protection, there remains room for improvements to its implementation. Growing pains are not uncommon when it comes to the implementation of new laws and two years on, the full potential of the act has yet to be realised. In the time the act has been operational, there have been separate occurrences; both new and existing that have called into question the effectiveness and efficiency of the act as it operates right now. We examine some of these occurrences in this paper.

While this paper is not exhaustive in its analysis, we seek to provide insights on some of the key elements of the data protection law and how it could be further developed to make for a stronger, more effective law for the protection of people's rights. To that end, we provide two sets of recommendations, one directed to the Kenyan Government and one to the ODPC.

TABLE OF CONTENTS

DATA PROTECTION IN KENYA: THE CONTEXT

The constitutional right to privacy, which forms the backbone of most data protection laws, has been long guaranteed by the various iterations of the Constitution of Kenya. Notwithstanding the fact that the current Kenyan constitution guarantees the right to privacy in Article 31, it has proven not enough to protect people's information in the digital age.

The world as we know it is fast-changing day by day and, in doing so, incorporating more and more technological advancements into daily life. From the mobile applications we use on a daily basis, to social media platforms, public service providers, as well as private corporations are moving toward digitization and incorporating tech into every day processes; we send and receive large volumes of data every minute of our lives, often without giving it a second thought.

In order to protect their respective citizens' rights, several countries and independent bodies have developed laws and policies to serve as frameworks for how personal data may be collected and utilised. At the same time, the organisations and people to which these frameworks apply continue to find clever ways of avoiding compliance with the very policies and laws to which they are subjected. The biggest culprits have been governments, state actors, and large corporations. This paper seeks to provide a short analysis of Kenya's Data Protection Act of 2019, highlight the current environment within which the act operates, and give recommendations on ways to improve and make the already-existing law more effective.

I. ANALYSING THE KENYAN DATA PROTECTION ACT OF 2019: THE GOOD

In 2019, the Data Protection Act[1] became law and, among other things, it introduced the Office of the Data Protection Commissioner. The act has several provisions that deal specifically with several facets of data protection including the right to privacy, rights of rectification and erasure, and freedom from discrimination. For instance, every data controller or processor (this includes ISPs and their agents, government agencies, and other consumer-heavy organisations such as supermarkets) must ensure the subjects' privacy rights are protected, the data is collected in a transparent manner and for a legitimate purpose, the data is limited to the minimum necessary for that purpose, and the rights to correction and erasure are preserved. This is outlined as the principles of data protection in **Section 25** of the Act.

The Act provides for the rights of data subjects in **Section 26** among which are the rights to erasure, correction, deletion, and consent with regard to the collection and use of their data. Significantly, the Act provides for instances in which data may be collected from a source other than the data subject, such instances include; whereby data is already part of the public record, there is consent from the subject to that collection, the data subject does not have capacity (such as in the case of a minor) and in the case of criminal investigations or proceedings. Even then, the Act further provides that reasonable steps must be taken to notify the data subject that their data is being processed; these provisions are contained in **Section 28** and **Section 29** of the Act. Failure to (reasonably) notify the subject on the part of the data processor of any procession of their personal data is classified as an offence under **Section 30(3)** of the Act.

Section 35 of the Act makes an effort to protect data subjects from discrimination in line with constitutional principles by stating that peopleshall not be subjected to "...decisions solely based on automated processing including profiling which … significantly affects the data subject".

In **Section 43**, The Act requires data controllers to give notice to the Office of the Data Protection Commissioner (ODPC) in the event of a data breach and to further give notice to the data subject if the data accessed is person identifying. The law also establishes timelines within which this action may be undertaken; notice is to be given within 72 hours if discovered in a timely fashion, or 48 hours after the discovery should a late discovery of a breach be made.

On a positive note, the ODPC has, as part of its mandate, been timely in formulating operationalising provisions(regulations) to give effect to the act; among them the Data Protection (General)

[1] Kenya Data Protection Act, 2019
http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

Regulations,[2] the Data Protection (Compliance and Enforcement) Regulations,[3] and the Data Protection (Registration of Data Controllers and Data Processors) Regulations.[4] Every process so far has rightly called for public participation before the adoption of these regulations. There are, however, some issues that stand out in the development of these provisions, which will be addressed in this paper.

[2] Data Protection General Regulations
https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf
[3]Data Protection Compliance And Enforcement Regulations
https://www.odpc.go.ke/wp-content/uploads/2021/04/THE-DATA-PROTECTION-COMPLIANCE-AND-ENFORCEMENT-REGULATIONS-2021.pdf
[4]Registration Of Data Controllers And Data Processors Regulations
https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-Registration-of-data-controllers-and-data-processor-Regulations.pdf

II. ANALYSING THE KENYAN DATA PROTECTION ACT OF 2019: THE BAD

First off, the Data Protection Act does not guarantee the independence of the ODPC. The ODPC is required to work in consultation with the Cabinet Secretary for Information, Communication and Technology (ICT); an appointee of the president and a member of the executive arm of government; and has to submit annual operational reports to the Cabinet Secretary. The Cabinet Secretary also has powers to remove the Data Commissioner from office on recommendation of the Parliamentary Service Commission and has powers to formulate the operationalisation provisions with regard to the Act. The Data Protection (General) Regulations gives mandate to the Cabinet Secretary ICT with regard to matters localisation of data.

The Act provides in **Section 8(2)** that the ODPC may collaborate with national security organs (these are constitutionally defined as the Kenya Defence Forces, the National Intelligence Service, and the National Police Service). It goes further to provide for classes of people and data that may be exempted from compliance with data protection regulations in **Section 51** including national security and/public interest; this is operationalized by the Data Protection (General) Regulations by giving discretion to the Cabinet Secretary of ICT to make decisions as to what amounts to national security. Without objective determinants toward the application of such provisions, this is a slippery slope. Historical and political context is also important in examining this aspect of the Act. The "national security" trope has long been played out and applied to the most remote of situations, more recently in the omnibus Statute Law Miscellaneous Amendment Act and the proposed Cybercrime law amendments.

What is more, the ODPC may not have the needed resources to conduct its tasks. The ODPC has been allocated Ksh 50,000,000 (≅USD 500,000) which is an incredibly low amount, in the national budget[5] this financial year. To put this into context, the European Union's Data Protection Commission received 16.9 million euros (>Ksh.2.1 Billion) in 2020 and 19.1 million euros(>Ksh. 2.4 Billion) in 2021 in funding.[6] It is next to impossible for an office with such an important and wide mandate to work with a budget this low. According to program-based budgetary documents[7] and the budget itself, the ODPC falls under the Ministry of ICT, once again highlighting the lack of independence this office has. It is not lost on us that complaints already registered with the ODPC have been dealt with in a manner that may be considered lethargic.

[5] Kenya National Budget FY 2021/2022
https://www.treasury.go.ke/wp-content/uploads/2021/05/FY2021-22-Recurrent-Expenditure-Vol-I-Votes-1011-1162.pdf
[6] Data Protection Commission Statement on Funding in 2021 Budget
https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-funding-2021-budget
[7] Kenya Programme-based Budget FY 2021-2022
https://www.treasury.go.ke/wp-content/uploads/2021/05/FY2021-22-Programme-Based-Budget.pdf

III. DATA PROTECTION IN KENYA IN PRACTICE: WHAT IS THE REALITY FOR PHONE AND INTERNET USERS?

In Kenya, in several and separate occurrences, users of leading ISP, Safaricom PLC, have received unsolicited politically charged text messages, unsolicited marketing messages and messages from private organizations and companies. It has become especially rampant in the last few years due to increased use of popular mobile money platform M-Pesa.[8] In registering for M-Pesa, one must provide their telephone number, National Identification Card number, as well as their date of birth. Much of the same information is required when withdrawing money from a mobile M-Pesa agent; one must once again provide their full name, phone number, and Identification Card number, without much information as to how this data will be protected. It is simply recorded in a physical book provided to all M-Pesa agents, presumably by Safaricom PLC, and there is no telling who has access to that record once you leave the M-Pesa kiosk, as there are no clear safeguards against the possible dissemination of data once it is recorded in one of those M-Pesa books.

It has become more and more commonplace to pay for items in an establishment then afterwards receive marketing messages[9] for weeks on end from that establishment, simply because, as you use M-Pesa for payment, there is no effort towards minimisation of data whatsoever, neither is there a guarantee that one's data will be used only for the purpose it is being collected; the establishment to which one makes payment receives one's phone number and full official name, and they do not hesitate to start sending messages of their marketing promotions and offers, a service to which one has not subscribed. Currently, most of these services operate on an opt-out basis; whenever one sends a complaint to Safaricom PLC, the response is standard: dial a particular USSD code and unsubscribe to the service, which works; why, however, does a client have to unsubscribe to a service they did not subscribe to in the first place, is the question we must ask.

Most recently, a complaint[10] was lodged with the Data Commissioner with regard to an alleged breach of duty by Safaricom PLC in relation to privacy rights of millions of subscribers following a data breach by its employees which saw the personal data of a large number of subscribers being published without their consent and knowledge. The complainant alleges that Safaricom PLC has not taken any steps to ensure that the data is removed from the public domain.

Similar to the case in Ghana a few months ago,[11] as we move towards an election period, the political messages are back. There is no explanation as to how politicians access this information as a majority of the population is not registered to any political party. Politicians' campaigns will regularly send

[8] https://www.safaricom.co.ke/personal/m-pesa
[9] Mugambi Laibuta, Data Brokers and Direct Marketing, May 2021
[10] https://twitter.com/KinyanBoy/status/1358395467462279175?s=19
[11] Graphic.com, We don't give subscribers details to marketers- telecom networks, September 2020

information to members of a particular ward, constituency, or county in an effort to solicit votes. The service providers, of course, at the time absolved themselves of any and all responsibility. Inasmuch as the Data Protection (General) Regulations require people canvassing for political support to register with the ODPC, it is difficult to envision how this will be implemented. A large number of Kenyans, a few months ago, discovered that they have been registered to political parties without their consent[12] or knowledge, with no indication as to how their personal data was collected and being used by these political parties. In the past, as evidenced by the Cambridge Analytica fiasco, Kenya has been subject to the use of personal data to influence the electorate; to therefore see such breaches happening is extremely concerning. The ODPC released a statement[13] promising action against the implicated political parties; this has yet to be seen.

[12] Nation, Data breach? Voters registered in parties without consent, June 2021
[13] ODPC Statement via Twitter , June 2021

IV. RECOMMENDATIONS

Based on the issues highlighted above, we recommend the Kenyan government, the ODPC, and related offices and agencies consider taking the following steps to ensure a robust data protection regime:

RECOMMENDATIONS TO THE GOVERNMENT OF KENYA	
GUARANTEE THE ODPC INDEPENDENCE	Work towards an independent data protection office by amending the Act to remove seemingly compulsory involvement of the Cabinet Secretary for ICT and national security organs.
RATIFY INTERNATIONAL AGREEMENTS TO PROTECT PERSONAL DATA	Take steps to ratify the data protection principles established under the African Union Convention on Cyber Security and Personal Data Protection[14] (Malabo convention) and to ratify the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[15] (108+ Convention).
CLARIFY SCOPE OF THE DATA PROTECTION ACT	Work to give clarity and objectivity to the national security/public interest exemption to ensure its fair application and restrict the scope of its application to ensure it mirrors the spirit of the constitution.
PROVIDE ADEQUATE RESOURCES TO THE ODPC	Increase budgetary allocations and personnel hiring capacity for the ODPC to ensure effectiveness and functionality in carrying out its mandate.

RECOMMENDATIONS TO THE ODPC	
IMPROVE TRANSPARENCY AND PARTICIPATION IN PROCESSES	The ODPC should make provisions for meaningful public participation. As it stands, all public participation processes have been given an extremely short period of time, capping at 14 days. While we note the concerted efforts of the ODPC to make announcements and run town halls during these processes, it may be useful to provide a longer period of time for participation to avoid locking out subjects of the act.
STREAMLINE PROCESSES	Reduce the amount of information[16] required by the ODPC from complainants when submitting a complaint and reduce the amount of information needed to register a data controller or data processor.

[14] African Union Convention on Cybersecurity and Personal data Protection
[15] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
[16] https://www.odpc.go.ke/report-a-complaint/

V. CONCLUSION

It is clear that Kenya has a progressive law and administrative body in the form of the ODPC in place. There are, however, improvements to be made to ensure the proper functioning of the Act and the office that comes with it. This starts with establishing and ensuring the independence of the Office of the Data Protection Commissioner and the establishment of meaningful public participation. We will continue to do our part to engage with the ODPC and other stakeholders.

For more information, visit our Data Protection page:

accessnow.org/issue/data-protection