
**SUMMARY REPORT:
A STUDY ON (SUB)
NATIONAL DATA
PRACTICES IN
KENYA** - Gaps and
Opportunities



TABLE OF CONTENTS

1. Background and introduction	4
2. Methodology	5
3. An Overview of Data Protection and Access to Information Laws in Kenya	6
3.1 International influences	7
3.2 National Level Statutes	8
3.3 Subnational Level	12
4. Conclusion And Recommendations	15



1. Background and introduction

Over the next decade, Kenya hopes to achieve its development objectives by harnessing the benefits of the digital economy, this is documented in Kenya's Digital Economy Blueprint as a key step to diversification and development of the Kenyan Economy¹. In 2019, Kenya published a report highlighting the potential public benefits of exploiting distributed ledger technology and Artificial intelligence.² Further, the country's Digital economy blueprint aims to have a digitally empowered citizenry living in a digital society. It recognises having a digital government as a key pillar to achieving this goal by realizing open data sources, digital identity for all, digital service delivery and an e-government.³

Undoubtedly, a digital government is able to derive high quality data that would guide decision and policy making. The World Bank recognizes the potential of exploiting data for development to improve lives by addressing poverty, managing public debt and the prudent allocation of scarce natural resources.⁴ They further recognize the benefits of data sharing among both public and private entities in realizing this goal. Kenya has a devolved system of government consisting of 47 counties at subnational level. The potential to use data to inform the allocation of resources and economic development meets the objectives of devolution under the Kenyan constitution to promote social and economic development and the provision of proximate easily accessible services throughout Kenya.⁵

Open data and digital government would also facilitate civic participation and public accountability. The Constitution of Kenya, 2010 changed the governance landscape in Kenya by recognizing public participation, transparency and accountability as important national values and principles of governance. Nevertheless, meaningful and effective public participation can only be achieved with access to the right information. Therefore, citizens have a right to access data held by public authorities in the enforcement of their rights.

Despite these benefits, personal data must still be protected and the right to privacy respected. States must also guard against data misuse and abuse by creating strong data governance mechanisms that protect personal data, reinforce the right to privacy and build trust and confidence among citizenry.

Ideally, comprehensive data protection and privacy laws ought to safeguard the integrity of data that has been collected by both state and non-state actors to ensure that it is only used for the purposes for which it was collected, stored and processed appropriately. This is particularly important considering the fact that the data collected is usually of personal nature and if misused could have dire consequences to citizens and rightful delivery of service by both state and non-state actors.

Right to information (RTI) and privacy laws can both complement and conflict with each other, depending on the situation. Only in a small number of cases do they overlap and lead to potential conflict.

In many countries, Kenya included, the two rights are intertwined constitutionally. Under the concept of habeas data- a constitutional right that permits individuals to demand access to their own information and to control its use. For instance, Article 35 (2) of the COK, 2010 provides that “every person has the right to the correction or deletion of untrue or misleading information that affects the person.”



The right to obtain personal information contained in public or private databases, has been important in many countries in exacting accountability for human rights abuses and helping countries scarred by human rights abuses reconcile and move forward, which can only be accomplished by exposing the truth and punishing the guilty.⁶

In many cases, the rights overlap in a complementary manner. Both rights provide an individual access to his or her own personal information from government bodies, data protection laws allow for access to personal information held by both public and private bodies. In this study, the government bodies of interest are the subnationals.

From the above, the Access to Information (ATI) Act, 2016 and the Data Protection Act, 2019 also mutually enhance each other: privacy laws are used to obtain policy information in the absence of an ATI law, and ATI laws are used to enhance privacy and data protection by revealing abuses.⁷

While the ODPC continues to implement the Data Protection Act 2019, there is a need to examine policy and practices at subnational level that impact the implementation of this legislation. Further, this must be balanced against established policies that promote public accountability in areas like finance. We must also determine the role of other non-state actors at the subnational level to implement the legislation as compared to the Access to Information obligations. Therefore, this report will draw recommendations from a comparative study of 5 counties; Makueni, Vihiga, Kilifi, Bomet and Taita Taveta on best policy approaches to solve the aforementioned problem.

2. Methodology

The study employed both qualitative and quantitative methods used in collecting, analysing and interpreting data and findings. The team of researchers visited each county and conducted key informant interviews with county government officials and focused-group discussions with purposefully sampled citizens. In total the study reached 58 respondents which was 77.3 percent of the respondents targeted. The collection of data occurred in Kilifi, Taita Taveta, Bomet, Makueni (where we encountered delays that impacted the final analysis) and Vihiga counties.



3

An Overview of Data Protection and Access to Information Laws in Kenya



3.1 International influences

Kenya's philosophy on access to information and privacy is informed by Kenya's participation in the international community. The Kenyan Data Protection Act bears some similarity with the EU's General Data Protection Regulation (GDPR) and, if properly implemented, may bring Kenya a step closer to achieving adequacy status from the EU. We also note that there are 4 critical instruments at the international level that obligate states to guarantee access to information and privacy rights to citizens. Kenya has ratified three of them (with the exception of the African Union Convention on Cyber Security and Personal Data Protection). These include:

1. Universal Declaration of Human Rights (UDHR), Article 12 and 19.

By virtue of its membership in the UN, Kenya is obligated to adhere to the principles of the UDHR.⁸

2. International Covenant on Civil and Political Rights (ICCPR), Article 17 and 19.

Kenya acceded to the ICCPR on 1st May 1972.⁹ Going a step further to safeguard the right to privacy and access to information, the Human Rights Committee adopted General Comment 16 of 1988¹⁰ and General Comment 34 of 2011 respectively.

3. African Charter on Human and People's Rights (ACHPR)¹¹.

The ACHPR explicitly provides for the right to information under Article 9, on the other hand, while the African Charter on Human and Peoples' Rights does not explicitly guarantee the right to privacy, it may be inferred from several articles relating to the integrity of the person, the right to dignity and the right to property. Kenya acceded to the ACHPR on 23 January 1992¹².

4. African Union Convention on Cyber Security and Personal Data Protection.¹³

The African Convention is not yet a legally binding document but is persuasive given it was drafted and approved by all African Justice and ICT Ministers prior to presentation before the African Heads of States for ratification and domestication.

3.2 National Level Statutes

Constitution of Kenya 2010: Kenya is party to several international legal instruments that provide for the right of access to information by dint of Article 2(6) of the Constitution.¹⁴

Vignette:

In April 2020, the Court of Appeal reversed a High Court decision precluding the government's plan to implement the Device Management System (DMS), a mechanism for identifying counterfeit and illegal phones.¹⁵ The High Court had ruled that the system, which gives the CA access to mobile subscriber data, including call records, would infringe on subscribers' right to privacy, among other concerns.¹⁶ The Court of Appeal ruled that the High Court lacked evidence to reach this conclusion.¹⁷ In June 2020, after the coverage period, the Law Society of Kenya appealed the case to the Supreme Court; though the DMS will be implemented while the appeal is being considered.



Access to Information Act, 2016

The Act came into force in 2016 with the primary objective of giving effect to Article 35 of the Constitution on the right of access to information. It does so by inter alia, providing a framework for public entities and private bodies to not only provide information upon request but also proactively disclosing information that they hold in line with the constitutional principles relating to accountability, transparency and public participation and access to information.¹⁸

The Data Protection Act, 2019

Kenya enacted the Data Protection Act, 2019 in November 2019. The act comprehensively governs the collection, processing and storage of personal data by government and private actors.¹⁹ It does so by establishing an intricate ecosystem of rights and obligations that operationalise the right to privacy, as espoused under the Bill of Rights.²⁰

Consumer Protection Act, 2012

The Act was enacted to give effect to the right to consumer protection provided for under Article 46 of the Constitution by improving consumer awareness and encouraging responsible and informed consumer choice and behaviour. Part I of the Act²¹ states the objects and purpose of the Act which is to protect consumers from all forms of unconscionable, unfair, unreasonable, unjust, or otherwise improper trade practices and reduce any disadvantages experienced by consumers in accessing supply of goods and services.

The Kenya Information And Communication Act, 1998- Revised Edition 2011 (2010)

The Act establishes the Communications Authority of Kenya as an independent body to license and regulate postal, information and communication services²² while respecting freedom of the media²³.

The Kenya Information and Communication (Consumer Protection) Regulations 2010

These regulations provide for rights and obligations of customers of any licensed operator under the Act. The customer has a right to information about the terms and conditions of any service and personal privacy and protection from unauthorized use of a subscriber's personal information²⁴.

Finance Acts:- Finance Act of 2019, Finance Act of 2020 and Finance Act of 2021

The Finance Act introduced the Digital Service Tax, a tax levied on income derived from a digital marketplace. The Tax is levied on taxable supplies such as subscription based media including news, magazines and journals, or over the top services including streaming tv shows, films, podcasts etc. Following the introduction of DST, pricing in several services such as Netflix Plans for Kenyan consumers increased²⁵. This, as stated, increases the cost of accessing information.

National Intelligence Service Act, 2012

The service is informed by guiding principles such as upholding the Bill of Rights, values and principles of governance under Article 10(2), the values and principles of public service under Article 232(1) and the principles of national security in Article 238(2).²⁶

Prevention of Terrorism Act, 2012

The Act confers police officers with powers to make ex-parte applications to a Magistrate's Court to gather information when investigating suspected terrorist activities.²⁷ The Act further provides for limitation of certain rights subject to Article 24 of the Constitution in the pursuance of terrorism investigation, detection or prevention.²⁸

Mutual Legal Assistance Act, 2011

Part IV of the Act provides for the interception of communications, preservation of communications data and covert electronic surveillance. Kenya may, for the purpose of a criminal investigation execute a request from a requesting state for the interception, recording and transmission of telecommunications;²⁹ preservation of communications;³⁰ or for the deployment of covert electronic surveillance.³¹

The Computer Misuse and Cybercrimes Act, 2018

The operation of this law is crucial to the implementation of data protection and access to information. This is due to the growing commercial value of data, which incentivises cybercrime geared towards data leaks and the invasion of privacy at a large scale.³²

However, thus far the utilisation of the Cybercrimes Act has tilted towards limiting the constitutional right to access to information.³³ This is despite the fact that a very specific focus has been placed on the said right, along with the protection of the right to privacy and freedom of expression.³⁴

Vignette:

On 29 May 2018, in *The Bloggers Association of Kenya v Attorney General & 3 Others*, the implementation of the act was challenged, based on its potential to infringe on the privacy of individuals, freedom of expression, speech, opinion and access to information online.³⁵ The high court responded by suspending certain sections of the Act based on the principle of unconstitutionality. On full determination of the case in February 2020, the court upheld the constitutionality of the entire Act and this matter is now subject of appeal.

Thus far, the precedent set based on the Cybercrimes Act has been limited, as majority of the cases making references to the law have involved challenges to its constitutionality, prosecutions based on illegally obtained data that would undermine the freedom of access to information³⁶ and decisions that have labelled the provisions relating to data protection insufficient.³⁷



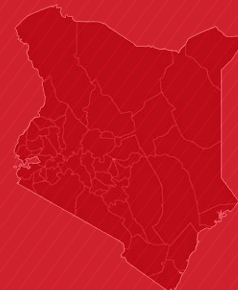
Kenya Standards Act, 2012:

Recently, the Kenya Bureau of Standards (KEBS) approved 40 new standards to enhance information and cybersecurity and safeguard consumer privacy. The standards outline techniques and methods of securing corporate information through managers charged with the responsibility of data safety. Moreover, they stipulate a framework to ensure privacy of ICT systems storing and processing personally identifiable information.³⁸

County Government Act, 2012:

Access to information in the Act is provided for under Part X. It provides for the right of every citizen upon request, to have access to information held by any county government or any other state organ.³⁹ It goes further to make provisions for every county government to designate an office to be used to ensure access to information.⁴⁰

3.3 Subnational Level



Each of the 47 subnationals in Kenya have rolled out different measures, procedures and in some cases regulations and policies to fulfil their obligations to protect, promote and fulfil both the right to access information and the right to privacy for its citizens in general and to ensure personal data protection in particular. Below are some of the policies touching on data protection or privacy at the subnational level in the counties we visited:

1. Taita Taveta County Health Services Bill, 2020⁴¹

Under Section 25 of the Bill, it explicitly provides for confidentiality of information on all users with information being disclosed under patient's consent or under order of court or for health research and policy planning purposes. We note that this document is still a Bill and not yet an Act and thus has not been fully operationalised.

2. Kilifi County Maternal, Newborn and Child Health Act, 2016⁴²

Under section 25 of the Act, it explicitly protects the confidentiality of information on HIV/AIDS status of children.

3. Makueni County Maternal, Newborn and Child Health Bill, 2017⁴³

Under section 24 of the Bill, it explicitly provides for confidentiality of information on HIV status of children. We note that this document is still a Bill and not yet an Act and thus has not been fully operationalised.

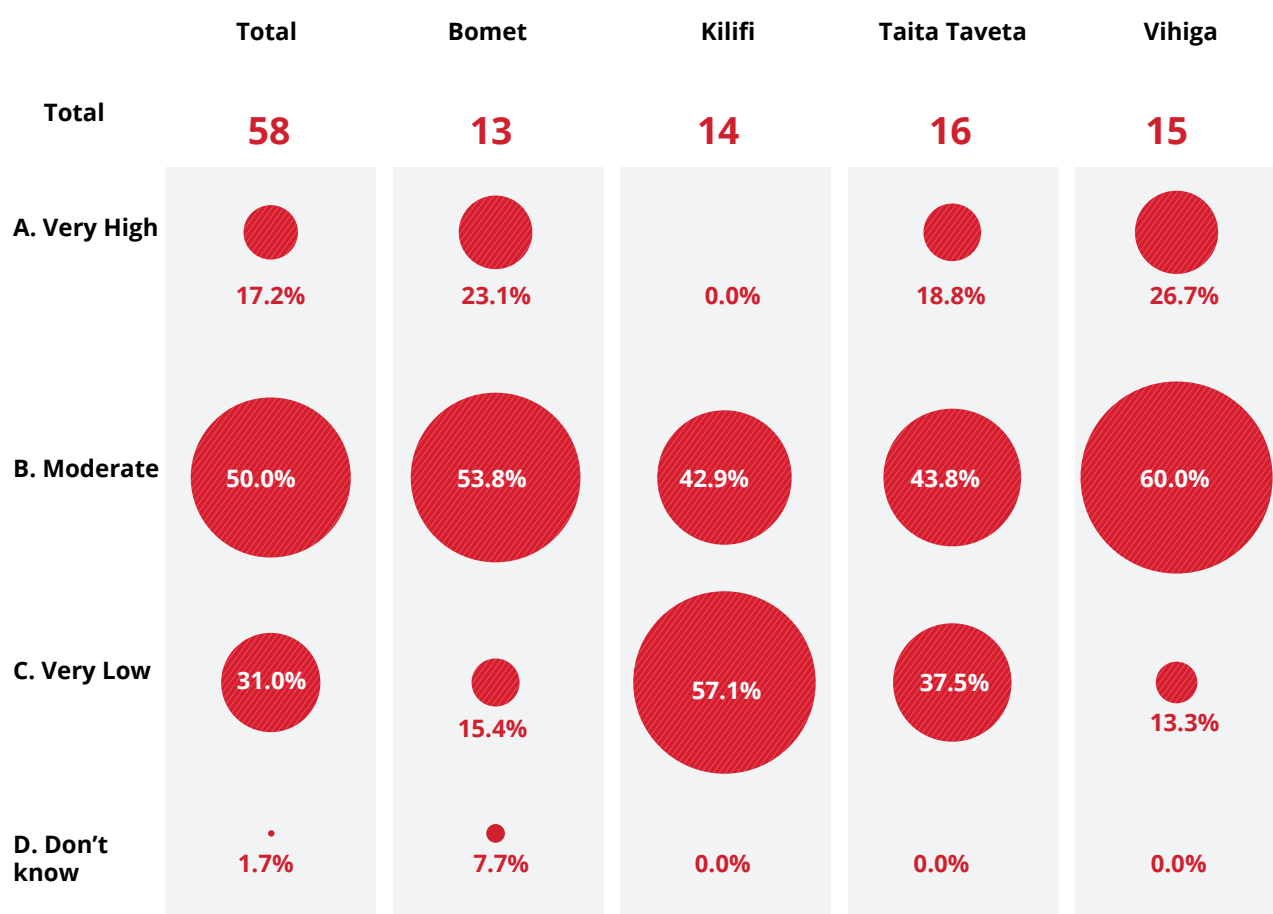
4. Vihiga County Health Care Service Bill, 2019⁴⁴

Under section 22 of Bill states, "... (1) Information concerning a patient, including confidentiality information relating to his or her health status, treatment or stay in a health facility is confidential except where such information is disclosed under order of court or informed consent for health research purposes..." We note that this document is still a Bill and not yet an Act and thus has not been fully operationalised.

County governments collect data on citizens on a number of occasions. These include public events, when citizens are applying for various permits from the county government, and for purposes of enabling the county governments to offer an array of services. In both the structured questionnaire survey and focus group discussion sessions, citizens expressed awareness that county governments collected their personal data.

With regard to the safety of personal data of citizens, we sought to establish county government officials' perceptions of the safety of citizen data. The table below presents the findings on this aspect. The data on Makueni was not obtained by the time of writing this report.

Table: How would you rate the County Government's capacity to protect citizen data?

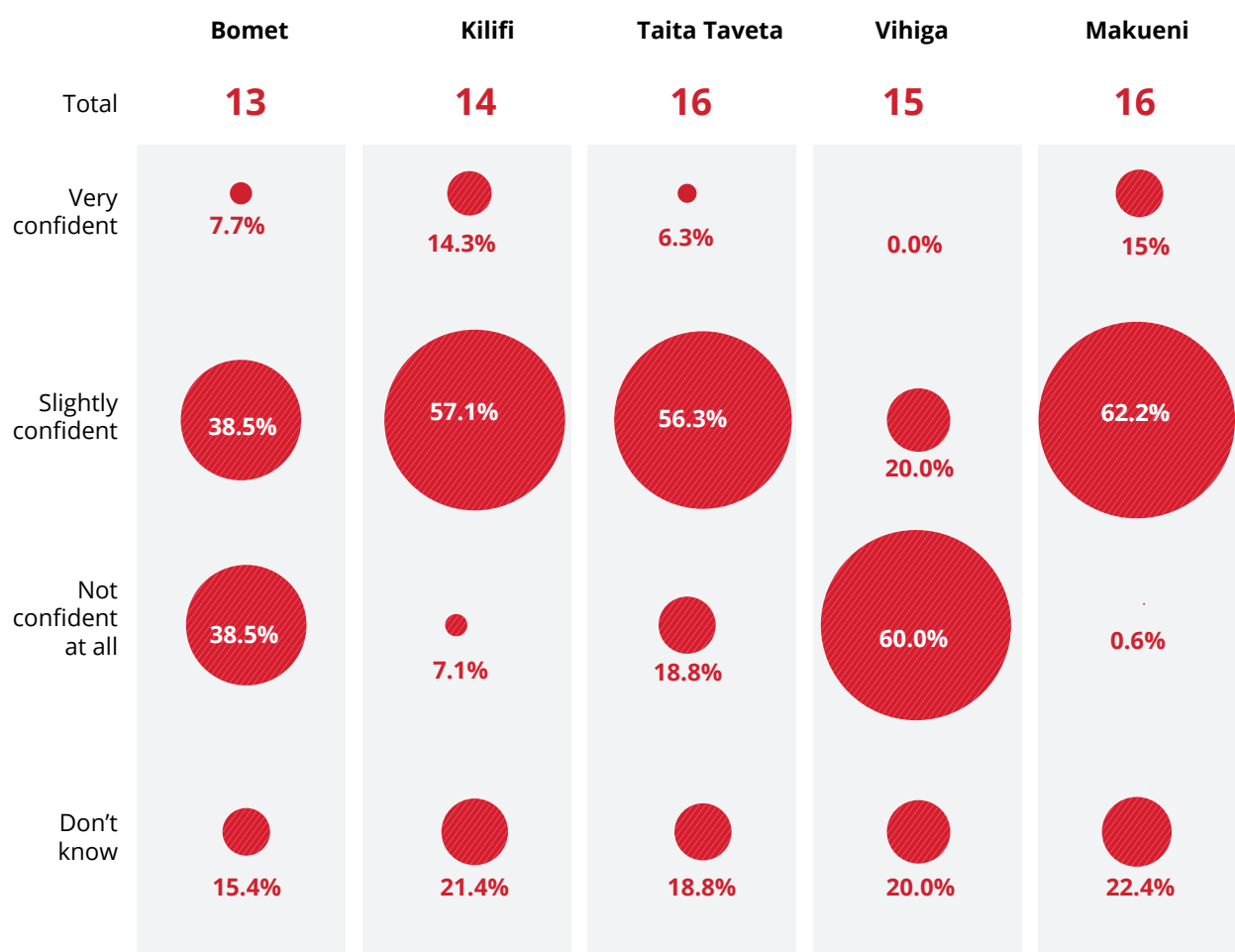


Though county government officials were very confident (50 percent) that the citizen data in their custody is secure, a significant number lacked information on data protection and access to data laws, policies and procedures within their respective subnationals. This is because there are no dedicated personnel dealing with the data protection docket except those working in the human resources. Similarly, when asked about how likely they thought citizen data could be put to unauthorized use, 14.3 percent of the officials thought this was highly likely, 42.9 percent thought it was possible but not very likely, while 38.1 percent reasoned that it was highly unlikely. Combined, the percentages of those holding the, highly likely and possible but not very likely views, give 57.2 percent which is a clear indicator that data subjects are likely to suffer data breaches in the status quo.

The views of county government officials differed from those held by ordinary citizens. For instance, only 6.9 percent of all citizens interviewed across four counties – Makueni excluded - are confident that their personal data which include details on birth, death, travel, passports, marriage, elections, tax, drivers, education, health insurance and social security and education details, held by either national or county governments cannot be put to unauthorized use; 21.4 percent are not confident at all, while 50 percent mentioned that they are slightly confident.

The table below presents citizen perceptions of data protection and privacy. Counties collect personal data in hospitals and health centres. These include sensitive personal data on medical records. It collects personal data on land ownership etc.

Table: Citizen perception on safety of personal data collected by the County Government from abuse, or unauthorized use



4

Conclusion and Recommendations

The study reveals that data protection is quite a complex subject matter and a fairly new subject matter to many of the counties in Kenya. It will take some time to be fully comprehended and applied by stakeholders. There is no holistic understanding of the concept of “information rights” and a full account of the notion and how it may apply to the national government and the county governments in Kenya.

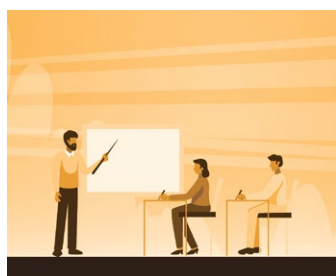
Efforts at national and county levels are fragmented and disarticulated. There is a need for an immediate effort to develop working collaboration between the two oversight mechanisms for the access to information and data protection to ensure that public bodies at national and county levels have a holistic understanding of the information rights.

All the five counties have developed some mechanisms to implement access to information laws through various protocols, mechanisms and procedures. They have also designated information officers. However, none of the five counties studied have passed comprehensive access to information laws even though the Model Law on Access to Information was developed by the Commission on Administrative Justice.

The five subnationals have designated some officers to assist in facilitating access to information. These officers largely are trained journalists and communication experts. There is a need to bolster the respective departments with data scientists to help augment the functions of managing information and data in ways that adhere to internationally accepted fair information practices.

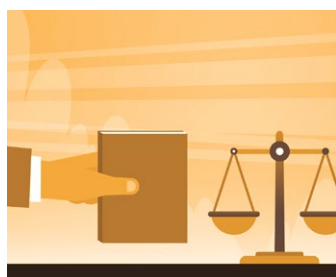
County governments have an obligation to facilitate the realisation of information rights of its citizenry even as they ensure they have requisite information management systems that ensure that personal and sensitive personal information collected, processed, stored and transferred is managed in ways that respect and meet the fair information principles.

The study makes the following recommendations:



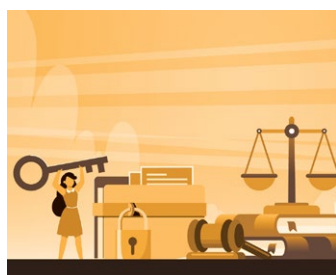
1. Capacity Building for citizens/community groups and public officers

There is a clear need for the development and implementation of a targeted county public awareness and education programme on information rights. The programme should be able to show the complementarity and conflict between the right to access to information and the right to privacy in general and data protection rights in particular.



2. Support counties to make annual reports to the Commission on Administrative Justice

All the counties studied have not submitted a single annual report to the Commission on Administrative Justice since 2016. Preparation and submission of the annual reports would serve two purpose: meeting their legal obligations pursuant to section 27 of the Access to Information Act, 2016; and enabling the county to reflect and understand what is working and what changes they ought to initiate to meet fulfil their legal obligations and be accessible and accountable to their diverse communities of their populations.



3. Develop and adopt clear and comprehensive access to information and data protection policies and legislations

County governments should establish policy, legislative and institutional frameworks to facilitate effective and timely access to information and data protection in all their administrative and service provision processes. They should also develop and resource all institutional and administrative frameworks up to sub-ward levels and ensure that they proactively disclose information within the confines of the Access to Information 2016



4. Build the capacity of counties to undertake Data Protection Impact Assessment

Undertaking a timely and comprehensive DPIA is one way in which County Governments can readily demonstrate to the oversight mechanism (Office of the Data Protection Commissioner) that they comply with the Data Protection Act, 2019. This situation may be attributed to the fact that all the five counties did not have any data scientists and experts on data protection and security in their stables as they may not have fully recognised their obligations under the Data Protection Act, 2019.

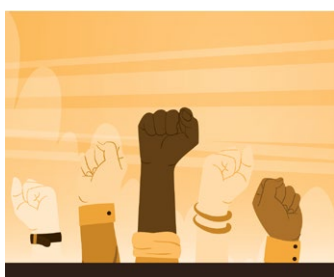
A credible DPIA must contain the following elements:

1. A systematic description of the envisaged processing operations and purposes of processing, including where applicable, the legitimate interest pursued by the controller;
2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
3. An assessment of the risks to the rights and freedoms of data subjects; and
4. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure protection of personal data and to demonstrate compliance with the DPA.



5. Hire and train dedicated Data Protection Officers

County governments process a number of different data sets of personal data that require qualified and dedicated Data Protection Officers to ensure they safeguard them and remain in compliance with the DPA. This must therefore be a minimum requirement for all counties. County governments should create financial resource measures to ensure that the office of the data protection authority is able to operate with offices in each county. Once data protection officers are hired, counties could work with the Office of the Data Protection Commissioner to develop tailor-made training and certification programmes.



6. Strengthen civil society organisations information rights and data governance programmes

Civil Society Organisations (CSOs) play a critical role in ensuring citizen-agency and county governments should take advantage of the social capital, skills, knowledge in CSOs to establish the mechanisms for interaction and co-learning to ensure better data governance practices that ensure data justice to all. CSOs working at the national and county levels should deepen and strengthen their programmes on information rights. They should engage with the national and county governments to ensure compliance with international human rights standards, including the UN Guiding Principles on Business.



7. To the private sector at the national and county levels

- Carry out a Data Protection Impact Assessment to ensure that all data collected is in strict compliance with the three-part test under international human rights law, and data protection principles, including data minimisation and privacy by design.
- Engage with the national and county governments to ensure compliance with international human rights standards, including the UN Guiding Principles on Business and Human Rights, and national laws protecting the rights to privacy, and access to information.




8. Protecting data rights of children


There is a need to undertake further research on how data protection and information rights affect children and their rights. This is very significant because children are less able to fully understand the implications of their rights to privacy and often do not have the opportunities or power to communicate their opinions⁴⁵. Children also often lack the resources to respond to instances of bias or to rectify any misconceptions in their data; and it is often the case that national statutes and regulations (in fact the DPA 2019 mentions children only once) including ethical guidelines rarely speak to the needs of children. Whereas this is out of scope for this study, it is recommended that more research is undertaken to generate evidence in this particular area for policy development.

References

1. Republic of Kenya, Digital Economy Blueprint, Powering Kenya's transformation, <<https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf>> accessed 18 August 2021
2. Republic of Kenya, Emerging Digital Technologies for Kenya, Exploration and Analysis (Ministry of Information, communication and Technology, July 2019) < <https://www.ict.go.ke/blockchain.pdf>> accessed 18 August 2021
3. Republic of Kenya, Digital Economy Blueprint, Powering Kenya's transformation, <<https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf>> accessed 18 August 2021
4. The World Bank, World Development Report 2021: Data for better lives, <<https://wdr2021.worldbank.org/the-report/>> accessed 18 August 2021
5. See article 174 of the Kenya: The Constitution of Kenya, 2010 [Kenya], 27 August 2010, <<https://www.refworld.org/docid/4c8508822.html>> accessed 18 August 2021
6. Cyrus Farivar, Habeas Data: Privacy vs. the Rise of Surveillance Tech (Melville House, 2018), Cyrus Farivar, 2018. Privacy Vs The Rise of Surveillance Tech, Melville House. See also Daniel J. Solove and Paul M. Schwartz, Consumer Privacy and Data Protection (3rd edn, Wolters Kluwer 2020)
7. David Banisar, The Right to Information and Privacy: Balancing and Managing Conflicts, The World Bank 2011, <<https://openknowledge.worldbank.org/handle/10986/23022>> accessed 18 August 2021
8. The Universal Declaration of Human Rights is not a treaty to which states become parties by signing the document, but is considered an authoritative universally accepted statement on human rights that states must adhere to.
9. University of Minnesota Human Rights Library, 'Ratification of International Human Rights Treaties - Kenya' <<http://hrlibrary.umn.edu/research/ratification-kenya.html>> accessed 20 June 2021
10. UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988 < <https://www.refworld.org/docid/453883f922.html>> 18 August 2021
11. African Union, 'African Charter on Human and Peoples' Rights' <<http://www.achpr.org/instruments/achpr/>> accessed 18 August 2021
12. University of Minnesota Human Rights Library, 'Ratification of International Human Rights Treaties - Kenya' <<http://hrlibrary.umn.edu/research/ratification-kenya.html>> accessed 20 June 2021
13. African Union Convention on Cyber Security and Personal Data Protection. Date of Adoption: June 27, 2014 <<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>> accessed 18 August 2021
14. Constitution of Kenya, 2010, Art 2(6), Laws of Kenya
15. Freedom House, 'Kenya: Freedom on the Net 2020' Available at < https://freedomhouse.org/country/kenya/freedom-net/2020#footnote1_6pbjlr9> accessed 18 August 2021
16. Okiya Omtatah Okioti v Communication Authority of Kenya & 8 others [2018] eKLR
17. Communications Authority of Kenya v Okiya Omtatah Okioti & 8 others [2020] eKLR
18. Access to Information Act, 2016, s 3. Laws of Kenya
19. The Data Protection Act of 2019, Section 3
20. The Constitution of Kenya 2010, Article 31
21. Section 3(4) of Kenya: Consumer Protection Act, 2012 [Kenya], <<http://www.parliament.go.ke/sites/default/files/2017-05/ConsumerProtectionActNo46of2012.pdf>> accessed 18 August 2021
22. Section 3 of the Kenya: Information And Communication Act, 1998- Revised Edition 2011 (2010) [Kenya], <<https://www.ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf>> accessed 18 August 2021
23. Section 5B of the Kenya: Information And Communication Act, 1998- Revised Edition 2011 (2010) [Kenya], <<https://www.ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf>> accessed 18 August 2021
24. Regulation 3 of the Kenya: The Kenya Information and Communication (Consumer Protection) Regulation 2010 [Kenya] <<https://www.ca.go.ke/wp-content/uploads/2018/02/Consumer-Protection-Regulations-2010-1.pdf>> accessed 18 August 2021
25. Lynet Igadwah, 'Netflix hikes rates on inclusion of VAT tax charge' (The East African, 07 May 2021) < <https://www.theeastafican.co.ke/tea/business/netflix-rates-inclusion-of-vat-tax-charge-3391120>> accessed 18 August 2021
26. Ibid, s 3
27. Ibid, s 34
28. Ibid, s 35(2)
29. Ibid, s 27
30. Ibid, s 31
31. Ibid, s 32
32. Ng'ang'a, Alexander Mwaura. "Toward a regional ICT hub: Need for cyber laws in Kenya." Information Security Journal: A Global Perspective 18.1 (2009): 47-50.
33. Ibid.
34. The Computer Misuse and Cybercrimes Act, No. 5 of 2018, Section 3(d)
35. The Bloggers Association of Kenya (BAKE) v Attorney General & 3 Others, Constitutional Petition No 206 of 2018
36. Cyprian Nyakundi & another v Director of Criminal Investigations & 2 others; Victoria Commercial Bank (Interested Party), Constitutional Petition E284 of 2020
37. Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties), Petition 56, 58 & 59 of 2019 (Consolidated)
38. Fredrick Obura, "40 new privacy standards approved as cybercrime soars by 50 percent" The Standard (Nairobi 24 May 2021)<<https://www.standardmedia.co.ke/business/sci-tech/article/2001413799/40-new-privacy-standards-approved-as-cybercrime-cases-soar-50-per-cent->> accessed 18 August 2021
39. County Governments Act, No 17 of 2012, Section 96(1)
40. County Government Act , No 17 of 2012, section 96(2)
41. Kenya: Taita Taveta County Health Services Bill, 2020 [Kenya], <<http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2020/TaitaTavetaCountyHealthServicesBill2020.pdf>> accessed 18 August 2021
42. Kenya: Kilifi County Maternal, Newborn and Child Health Act, 2016 [Kenya], <https://www.kilifi.go.ke/lib.php?com=5&res_id=567#:~:text=AN%20ACT%20of%20the%20Kilifi,connected%20therewith%20and%20incidental%20thereto.> accessed 18 August 2021
43. Kenya: Makueni County Maternal, Newborn and Child Health Bill, 2017 [Kenya], <<http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2017/MakueniCountyMaternalNewbornandChildHealthBill2017.pdf>> accessed 18 August 2021
44. Kenya: Vihiga County Health Care Service Bill, 2019 [Kenya], <<http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2019/VihigaCountyHealthCareServiceBill2019.pdf>> accessed 18 August 2021
45. <https://www.unicef.org/globalinsight/featured-projects/ai-children>



 P.O Box 50474, Nairobi 00100, Kenya

 hello@openinstitute.africa

 <https://openinstitute.africa>