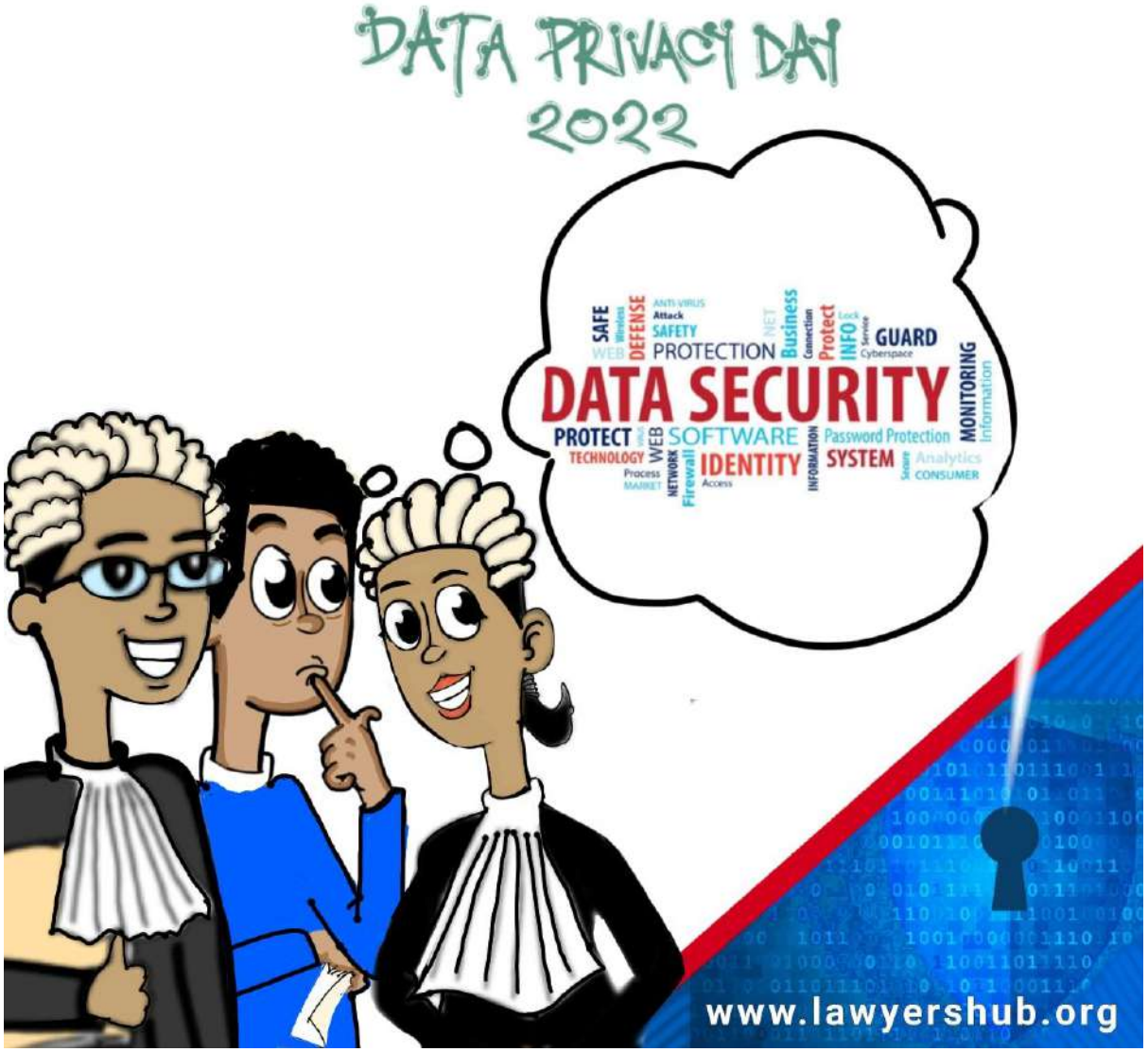
FRAMING KENYA'S DATA PROTECTION LANDSCAPE IN THE YEAR AHEAD



Data Privacy Day 2022 - Framing Kenya's Data Protection Landscape in the Year Ahead.

Preface

The Lawyers Hub notes the importance of Strategic Advocacy in raising awareness on privacy and the digital issues affecting the growth of Kenya's Digital Economy, Digital Rights and Access to Justice.

As such, on this Data Privacy Day 2022, Lawyers Hub reflects on the progress Kenya has made in asserting the right to Privacy through various legislative, institutional and policy intervention(s).

This publication addresses the developments in privacy practises and principles and projects on the steps ahead, towards achieving a desirable regulatory environment.

It reviews the operations of the Regulator, the Data Protection Commissioner, towards ensuring effective data privacy laws and efforts aimed at achieving implementation.

Important determinations by Kenyan courts have also been identified and discussed in a bid to assess judicial approaches to enforcement of privacy legislation, including framing of issues by Digital Rights Litigators.

In closing, the publication examines recent trends in the privacy sphere and further projects trends and key areas to look out for in the coming days as regards privacy and data protection.

Happy Data Privacy day 2022 from the Lawyers Hub Team.

Email: info@lawyershub.ke | Location: 6th Floor, ACK Garden House, Upper Hill on 1st Ngong Avenue| Phone: +254207840228 +254784840228 | P.O Box 2468-00621 Nairobi, Kenya | www.lawyershub.org

Foreword

The right to privacy in Privacy laws is more relevant today than ever before. Given that the digital age requires continuous proliferation and with data crossing borders as a result of increased internet penetration and increased use of social media, it is becoming more important to ensure that personal data is protected, processed and used for the correct purpose.

For Kenya, the enactment into law of the Data Protection Act (the "DPA") in November 2019 was a watershed moment. The DPA, which was designed to protect personal data from exploitation in the 21st century,[1] presents a significant step forward by facilitating lawful use of personal data, including research, and thus strengthening individuals' fundamental rights.

The Act establishes the Office of the Data Protection Commissioner (the "ODPC"), regulates the processing of personal data and makes provision for strategic action in privacy and data protection matters.

Even so, its implementation has not come without challenges. It has resulted in an inevitable change in culture and a significant change in terms of how data relating to data subjects is handled.[2]

This well segmented publication provides an avenue for readers, researchers, policy makers and stakeholders to interrogate these issues affecting the rights of data subjects and the obligations of data controllers and processors.

It interrogates the data protection landscape in Kenya over the past year; and examines the achievements and shortcomings experienced as a result of the enactment and implementation of the Act.

[1] AYAKO, D., 2022. *How Banks Can Handle Data Protection Hurdles.* [online] Available at: <https://www.businessdailyafrica.com/bd/opinion-analysis/ideas-debate/how-banks-handle-data-protection-hurdles-3606912> [Accessed 24 January 2022].
[2] Ibid

Chapter 1: 2021 In Review

Introduction

In 2019, Kenya sought to give effect to the constitutional right to privacy,[3] by enacting Data Protection legislation.[4] This Chapter provides an overview of the activities and defining moments in the quest for policies, laws, determinations and philosophies sensitive to the dynamic digital and technological advancements which are capable of impacting the right to privacy.

a. Courts and Enforcement of the Right to Privacy in Kenya: Case Law

The following cases have been consequential in reshaping the direction of the Government and other institutions in implementing programs with far-reaching effects on the right to privacy:

- **Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR** (read full case here)

Briefly, the High Court held that processing of data collected pursuant to the amendment of the Registration of Persons Act should not be undertaken before the Data Protection Act was operationalised and a regulatory framework put in place.

In the ground-breaking decision, the Court expressly stated that the regulatory framework was to address the concerns raised relating to the constitutional right to privacy in view of the somewhat intrusive nature of the National Integrated Identity Management System ("NIIMS").

The effect of the decision, although subject of a live Appeal was that there is a need for an effective framework that is keen on enhancing privacy protections.

The decision put both private and public institutions on notice to comply with privacy requirements regarding various data processing activities without requisite safeguards.

- **Republic v. Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others Ex Parte Katiba Institute & another; Immaculate Kasait, Data Commissioner (Interested Party) [2021] eKLR** (read full case here)

In this instance, the Court addressed the question of whether the DPA applied retrospectively to such an extent or to such a time as to cover any action that could be deemed to affect the right to privacy, and further whether the collection and processing of personal data under the NIIMS was subject to the Act.

[3] Constitution of Kenya 2010, Article 31.
[4] Data Protection Act, 2019.

The Applicants, who were aggrieved by the rollout or the launch of the Huduma Card, filed a Judicial Review Application for orders of certiorari, mandamus and prohibition to challenge the roll out of Kenya's digital ID on grounds that the State had not carried out a data protection impact assessment,[5] before rolling out the digital ID system.

In his judgement, Justice Jairus Ngaah quashed the decision to roll out Huduma Cards for being ultra vires Section 31 of the Data Protection Act. The section[6] requires that where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, the data controller or processor must carry out a Data Protection Impact Assessment ('DPIA'). The DPA does not specifically set out the types of processing subject to DPIA but generally provides that the assessment would apply to any processing that by its nature, scope, context, or purposes would result in high risk to the rights and freedoms of the data subject.

From the decision of the Court, it is clear that the collection of personal data for purposes of rolling out the Huduma Namba can be categorised as one such process. The Court further issued an order of mandamus compelling the Respondents to conduct a Data Protection Impact Assessment in accordance with Section 31 before processing of data and rolling out the Huduma Cards.[7]

From the two cases above, it is clear that even though there are yet very few decisions made under the DPA, an analysis of the reasoning of the Court establishes that there is a level of appreciation to put data processors and data controllers in check, by evaluating data processing activities, and measuring the impact of processing.

b. Law Reform

Since the enactment of the Data Protection Act, considerable strides have been made towards its implementation and ensuring privacy and data protection is upheld, some of which we discuss below:

- *Task Force on Implementation of the Data Protection Act*

On 15 January 2021, the Cabinet Secretary responsible for Information Communications and Technology, Hon. CS Mucheru, appointed a 14-member Task Force chaired by Data Commissioner, Immaculate Kassait, to audit the data protection law.

Among the Terms of Reference, was conducting a comprehensive audit of the DPA to identify gaps or inconsistencies; develop Data Protection Regulations; propose

[5] Data Protection Act 2019, Section 31.
[6] Section 31 Data Protection Act 2019 Laws of Kenya
[7] Kenyalaw.org. 2022. *Judicial Review Application E1138 of 2020 - Kenya Law*. [online] Available at: http://kenyalaw.org/caselaw/cases/view/220495/ [Accessed 21 January 2022].

any new policy or legal and institutional framework that may be needed to implement the Act; and other tasks related to its full implementation.

The Taskforce set out to deliver on their mandate, and as a result drafted three (3) sets of Regulations aimed at enforcing the substantive and procedural provisions of the DPA:

- ➔ Data Protection (General) Regulations, 2021 - which outline the procedures for the enforcement of data subject rights, as well as expand upon the duties and obligations of data controllers and data processors;
- ➔ Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 - which define the procedure that will be adopted by the Office of the Data Protection Commissioner ("ODPC") when registering data controllers and data processors; and
- ➔ Data Protection (Compliance and Enforcement) Regulations, 2021 - which outline the compliance and enforcement provisions for the Commissioner, data controllers, and data processors.

Lawyers Hub notes that the Regulations have since been published and are awaiting the approval of the National Assembly.

- *Guidance Notes by The Office Of The Data Protection Commissioner*

In January 2021, Kenya's Data Protection Commissioner issued a draft ''Guidance Note on Access to Personal Data During COVID-19 Pandemic.'' The note offers policy guidance to any person processing personal data of individuals to actualize responses and research on the pandemic, including data requests by innovators and any other use, so as to give effect to the right to privacy as it relates to the protection of personal information.[8]

Among its key principles, the note proposed that: Personal data must be collected for the specific purpose of ''contain[ing] and prevent[ing] the spread of COVID- 19,'' and that it ''shall only be that which is adequate, relevant and limited to what is necessary in relation to the purpose for which the personal data is requested.'' Further, it states that data should not be retained ''for longer periods than is necessary to achieve the purpose'' for which it was collected and after that purpose is achieved ''it shall be destroyed.''[9]

The Data Commissioner issued two additional Guidance Notes: the Guidance Note on Consent and the Guidance Note on Data Protection Impact Assessment.

The Guidance Note on Consent provides guidance on the processing of personal data on the basis of consent whereas the Guidance Note on Data Protection Impact

[8] Icnl.org. 2022. *Impact of technology during the COVID-19 pandemic*. [online] Available at: https://www.icnl.org/wp-content/uploads/Africa-COVID-Briefer-Technology-2.pdf [Accessed 21 January 2022].
[9] Ibid

Assessment provides guidance to data controllers and data processors on when and how to conduct Data Protection Impact Assessments.

The ODPC published a Guidance Note for Electoral Purposes whose key mandate is to: assist data controllers and data processors in dealing with voters' personal data, including sensitive personal data, and members of political parties' personal data in order to understand their obligations under the DPA. This Guidance Note applies solely to the processing of personal data on voters (or potential voters) and the processing of personal data for the purposes of creation and maintenance of member registers.

The ODPC has also developed three manuals and standard operating procedures on Lodging Data Breach Complaints; the Procedure on Complaints Handling; and the Procedure on Carrying Out Inspection (the ODPC Complaints Management Manual).

Lastly, through a Stakeholder Validation Workshop, the ODPC published and validated its Draft Strategic Plan Financial Year 2021-2023 designed to take note of ongoing technological and societal changes.[10]

The Plan adopts an inclusive approach and has the vision of enhancing trust and building transparency of data protection in Kenya. It is expected to provide a roadmap to improve institutional effectiveness and efficiency as relates to personal data protection, in light of Kenya's Digital economy BluePrint.[11]

The overall aim is to ensure that the law gains grounding and for Kenyans to conceptualise the right to privacy as one that is realisable. [12]

c. Institutional Governance

The DPA establishes the Office of the Data Protection Commissioner which is mandated with overseeing the implementation of the Act. The Office is tasked with establishing and maintaining a register of data controllers and data processors; receiving and investigating any complaints on infringements of the rights under the Act; carrying out inspections of public and private entities with a view to evaluating the processing of personal data; and imposing administrative fines for failures to comply with the Act.

The Act gives the Commissioner wide powers on investigation of data breaches including powers of entry and search, and issuing administrative fines. This is

[10] https://twitter.com/ODPC_KE/status/1453248589522771973?cxt=HHwWioC9zY_5_KooAAAA

[11] Weekly, V., 2022. *Stakeholders Add Their Voice to Draft Strategic Plan by Office of the Data Protection Commissioner during Public Participation Forum | Vellum Kenya*. [online] Vellum Kenya. Available at: https://vellum.co.ke/stakeholders-add-their-voice-to-draft-strategic-plan-by-office-of-the-data-protection-commissioner-during-public-participation-forum/ [Accessed 24 January 2022].

[12] ARTICLE 19. 2022. *Kenya: New data protection strategy must support other key rights - ARTICLE 19*. [online] Available at: <https://www.article19.org/resources/kenya-new-data-protection-strategy-must-support-other-key-rights/> [Accessed 24 January 2022].

witnessed in instances such as where a data controller is required to notify the Commissioner when personal data in their control has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access. The Commissioner ought to be notified without delay, within seventy-two hours of becoming aware of such breach.[13]

Additionally, the provisions of various sectoral laws enforced by the respective sectoral regulatory bodies are also now increasingly requiring compliance with the Data Protection Act. Case in point is the financial sector which is regulated by the Central Bank of Kenya.

The regulator, through The Central Bank of Kenya (Amendment) Act, 2021 is now empowered to oversee the digital lending space to curb unethical or illegal practises such as debt shaming, predatory lending, charging exorbitant interest rates, and illegal sharing of defaulters' data. The regulator presently has the mandate to revoke permits of operators who breach customer confidentiality or breach the conditions of the Data Protection Act or the Consumer Protection Act. [14]

In light of the foregoing, it is prudent for organisations to assess the impact of the existing framework on their day to day activities, as the minimum thresholds in advancing and promoting the right to privacy are taking shape.

d. Capacity Building

The Data Protection Act provides for the appointment of a Data Protection Officer (DPO)[15], who is a natural or legal person appointed by a Data Controller or Processor to assist with compliance of provisions outlined under the Act for the duties and responsibilities of the Controller or Processor. The overarching obligation of the DPO, to their contracting Data Controller or Processor, is to possess a thorough comprehension of the processing activities and an understanding of the possible risks arising from said processing activities.[16]

Further, an appointed DPO is tasked with the responsibility of identifying all members of staff who engage and interact with various forms of data collected, and their level of interaction with the same and consequently, adequately inform them of the

[13] Mondaq.com. 2022. *Data Protection In Kenya – What You Need To Know - Privacy - Kenya.* [online] Available at: <https://www.mondaq.com/data-protection/867010/data-protection-in-kenya-what-you-need-to-know> [Accessed 24 January 2022].

[14] Njanja, A., 2022.*TechCrunch is part of the Yahoo family of brands.* [online] Techcrunch.com. Available at: <https://techcrunch.com/2021/10/25/kenya-cracks-down-on-digital-lenders-over-data-privacy-issues/> [Accessed 25 January 2022].

[15] Section 24 of the Data Protection Act 2019

[16] Interactive, S., 2022. *DATA PROTECTION OFFICER APPOINTMENT IN KENYA - Sentinel Africa Consulting.* [online] Sentinel Africa Consulting. Available at: <https://sentinelafrica.co.ke/data-protection-officer-appointment-in-kenya/> [Accessed 24 January 2022].

potential risks and threats to the data, as well as their obligations and duties in relation to ensuring data privacy and preservation of the Data Subjects' rights.[17]

In a more general sense, the ODPC, civic societies and private organisations have championed for awareness creation on privacy matters in a bid to build capacity, in terms of knowledge, skillset and goodwill. This has been done through public engagements and multistakeholder convenings that have interrogated digital rights and safety, data protection concerns, and cyber security measures.

Capacity building workshops on data regulations, data protection laws and privacy cannot be overstated. Key areas of focus should include: the issue of trust in the digital economy, the evolution of data privacy law, practice and enforcement, cross-border data flows, localisation, the importance of international cooperation and the role of data protection supervisory authorities.

e. Policy Dialogues

- **Kenya Data Protection Regulations 2021 Discussion hosted by The Lawyers Hub**

The Lawyers Hub, in partnership with the ODPC held a public participation forum on the Draft Data Protection Regulations and obtained multiple comments to improve the framework.
Some of the recommendations made included: That there be a revision of the stipulated fees for certification from Kshs. 250,000 (approximately. USD 2500) to 25000 (approximately. USD 25); alternatively a clarification that certification is for accredited institutions offering certification as a service; that there be provision for accredited certification bodies to undertake certification of data controllers and data processors; that the period for renewal of a certificate of registration is lengthened to more than a year; that consideration is given to the issuing of electronic certificates which are easily retrievable to avoid the cost of replacement and that as regards the automated decision making provisions; the explain-ability on algorithms should be sufficient to allow data subjects informed consent while balancing between proprietary rights and privacy.

- **Stakeholders' Consultation Workshop on the Draft 2022 - 2025 Strategic Plan for the Office of the Data Protection Commissioner**

The ODPC and the UK Embassy held a day's workshop during which the ODPC Draft Strategic Plan (FY 2021/2022- 2023/2024) was subjected to stakeholders' validation in a hybrid workshop.[18]

The workshop, which was held in October 2021, brought together various stakeholders participating in the privacy and data protection sphere including

[17] Ibid
[18] Weekly, V., 2022. *Stakeholders Add Their Voice to Draft Strategic Plan by Office of the Data Protection Commissioner during Public Participation Forum | Vellum Kenya.* [online] Vellum Kenya. Available at: https://vellum.co.ke/stakeholders-add-their-voice-to-draft-strategic-plan-by-office-of-the-data-protection-commissioner-during-public-participation-forum/ [Accessed 24 January 2022].

government institutions, NGOs, private entities and civic activists to provide valuable input to the Strategic Plan, whose implementation will determine the policy direction in the regulation of personal data in the country.

Through the discussions held, stakeholders encouraged the ODPC to ensure the Plan specifies the ways in which the Office would encourage capacity building, not just for staff as had been highlighted in the Plan, but also for the general public, more specifically vulnerable persons and communities.

The Office was also encouraged to consider including timelines or structures for shared solutions actions for the benefit of all agencies which they could leverage such as a data ethics framework, data protection toolkit, a curriculum and a data standards repository and in consultation with relevant regulatory stakeholders, specify the schedule or plan for review of various relevant policies and regulations to ensure integration across board and avoid duplication or overlapping roles.

Further, stakeholders raised the critical need to ensure the provision of adequate human and financial resources to the ODPC to facilitate and promote data protection laws as well as obtain the necessary budget for the 3 year strategic plan through various proposed funding sources.[19]

f. Research/Articles to Note

The following resources are important in reviewing the status of the right to privacy in Kenya:

1. The African Union Convention on Cyber Security and Personal Data Protection

2. The African Declaration on Internet Rights and Freedoms

3. A Study On (Sub) National Data Practices In Kenya - Gaps and Opportunities By Open Institute

4. Amnesty International Kenya Data Protection Report 2021 – A Comparative Study on Data Protection Regimes

5. Privacy & Data Protection Practices of Digital Lending Apps In Kenya

6. DATA PROTECTION IN THE KENYAN BANKING SECTOR: A study of Publicly Available Data Policies of Commercial Banks operating in Kenya in Relation to a Set Data Protection Standard: A report by the Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University, Nairobi, Kenya

7. Biometric Technology, Elections, And Privacy Investigating Privacy Implications of Biometric Voter Registration In Kenya's 2017 Election Process

[19] Ibid.

8. Data Protection Regulations And International Data Flows: Implications For Trade And Development (Unctad)

9. Resources by LAWYERS HUB

Chapter 2: Tech, Trends and Insights from 2021

Kenya is facing a significant increase in data privacy trends, just like other jurisdictions the world over, which reflects a growing consumer expectation that the organisations they entrust with their data will be accountable.

There has thus been an urgent call to prioritise technology that is centred on streamlining and automating tools that protect data. There is a further need to create visible audit trails to ease compliance related tasks while governments need to ensure the implementation and enforcement of privacy and data protection laws and compliance regulations.

The following are some of the data privacy trends witnessed in 2021:

a. An Increase in Privacy Laws and Regulation

The past year has seen the drafting, publishing and enactment of more laws and guidelines that relate to privacy and data protection in Kenya. This included: Publishing of the Draft Data Protection Regulations; the Guidance Note on Access to Personal Data During COVID-19 Pandemic commonly known as 'COVID-19 Guidelines'; the ODPC Guidance Notes on Data Protection Impact Assessment and Consent; and the ODPC Complaints Management Manual (Procedure for Lodging Data Breach Complaints; Complaints Handling; Carrying Out Inspection).

b. An Increase in Reported Cases of Breach of Personal Data

The establishment of the ODPC led to more individuals lodging complaints for breach of their personal data, a trend that is likely to continue in 2022. Examples are such as:

- **A Subscriber Data Breach Complaint Against Safaricom Plc**

In February of 2021, a Safaricom subscriber, Adrian Kamotho Njenga, through his lawyers, lodged a complaint,[20] with the ODPC citing that the telco had failed to secure the confidentiality, privacy and security of subscribers' data which had been lawfully entrusted to them.

[20] https://twitter.com/KinyanBoy/status/1358395467462279175?t=WdlHgz-krXlaXqzpfP2NIw&s=08

The subscriber argued that the personal data of millions of Safaricom PLC subscribers had been variously transferred from Safaricom servers to publicly accessible google drive repositories as well as other devices outside Safaricom's control. This situation exposed the data to irregular analytical and data mining scripts in a manner contrary to the law and the express contractual and statutory duty to keep the data confidential, private and secure.

He sought the intervention of the ODPC in offering reprieve as per their mandate to implement and enforce the Data Protection Act.

- **Radisson Blu Hotel Data Breach Complaint**

Prow & Company Advocates, lodged a complaint,[21] with the ODPC on a possible data breach involving the records of hotel guests at the Radisson Blu Hotel & Residence, Nairobi Arboretum where the complainant alleged a guest list from the hotel had been leaked to the public.

The Firm sought investigations to hold the hotel accountable for violating guests' privacy, contending that Radisson Blu Hotel committed a serious data breach and violated the privacy rights of all Radisson guests whose personal information was illegally published/leaked.

- **Illegal Registration of Voters to Political Parties**

In June of 2021, a large number of Kenyans discovered—through the Office of the Registrar of Political Parties' (ORPP) online portal—that they were registered as members of political parties without their knowledge or consent.[22]

Consequently, hundreds of Kenyans took to social media platforms to protest and complain about being registered into political parties they do not subscribe to without their knowledge or consent.[23] Some went ahead to accuse the Registrar of Political Parties of allowing political parties to infringe on their privacy and forge their signatures.[24] After receiving over 200 complaints, the Data Commissioner held a meeting with the ORPP to arrange for the deregistration of those individuals.

---

[21] Data-policy-centre. 2022. *data-policy-centre*. [online] Available at: https://dpccipit.org/detail/?id=3 [Accessed 20 January 2022].

[22] Rutenberg, A., 2022. *Securing Kenya's Electoral Integrity: Regulating Personal Data Use*. [online] The Elephant. Available at: https://www.theelephant.info/op-eds/2021/10/01/securing-kenyas-electoral-integrity-regulating-personal-data-use/ [Accessed 24 January 2022].

[23] Oyugi, C., 2022. *Kenyans Can Sue Political Parties For Illegal Registrations - RoGGKenya*. [online] RoGGKenya. Available at: https://roggkenya.org/2021/06/28/kenyans-can-sue-political-parties-for-illegally-registration/ [Accessed 20 January 2022].

[24] Ibid

This conduct raised issues pertaining to certain fundamental rights and freedoms such as the right to privacy and data protection, the right to make political choices including joining a political party, and the right to correct and delete untrue or misleading information as stipulated in articles 31, 38 and 35 of the Constitution of Kenya 2010.[25]

- **Digital Lenders Illegal Use of Borrowers' Personal Data**

There are currently more than 100 digital lenders in Kenya, taking the form of digital mobile applications or websites.[26] It is in public record that some lenders have faced claims of using predatory lending tactics, including sharing of personal data of loan defaulters with third parties. It has become the practice for digital lenders to use common debt shaming in a bid to recover their loans through scraping data from borrowers' phones and using it to shame those who have failed to pay up.[27]

The Central Bank of Kenya (Amendment) Act 2021 was thus enacted to resolve a raft of issues, including developing Regulations to govern digital lending. The Act gives the Central Bank of Kenya the power to suspend or revoke the licence of digital lenders that breach the conditions of the Data Protection Act or the Consumer Protection Act. As such, digital lenders who breach the confidentiality of personal information risk permanent ban and revocation of their permits.

These reports and complaints serve to create awareness on possible areas of exposure by organisations, and put to test the kind of interventions that the ODPC pursues against data controllers and processors held to be in breach of the DPA.

c. Adoption of Tools/Mechanisms Built as Privacy Preserving

The world transitioning into becoming a completely data-dependent landscape where individuals, agencies, and businesses depend on data for the vast majority of their decisions, has led to conversations around adoption of systems and practises designed to be in line with principles of privacy protection and safety of the data.[28]

Businesses and organisations are now required to implement data protection by design and by default[29] which has resulted in the incorporation of design safeguards

---

[25] Amnesty International Kenya. 2022. *Illegal Registration of Voters To Political Parties Endangers Democracy - Amnesty International Kenya*. [online] Available at: https://www.amnestykenya.org/illegal-registration-of-voters-to-political-parties-endangers-democracy/ [Accessed 20 January 2022].

[26] AFP, F., 2022. *Public humiliation follows Kenyans opting for easy credit*. [online] Daily Sabah. Available at: https://www.dailysabah.com/business/finance/public-humiliation-follows-kenyans-opting-for-easy-credit [Accessed 20 January 2022].

[27] Ibid

[28] Iredale, G., 2022. *What are Privacy-Enhancing Technologies (PETs)?*. [online] 101 Blockchains. Available at: <https://101blockchains.com/privacy-enhancing-technologies/> [Accessed 25 January 2022].

[29] Data Protection Act 2019.

while prototyping and developing various products as developers are now increasingly using a data centric approach for security and privacy.[30]

Kenya's existing legislation champions the use of law as a device for preservation, and to achieve this, it empowers the Data Commissioner to apply to a court for a preservation order for the expeditious preservation of personal data including traffic data, where there is reasonable ground to believe that the data is vulnerable to loss or modification.[31]

This rise in priority for data privacy and security as well as the digital shift is one of the reasons for a focus towards privacy enhancing technologies (PETs).

PETs are a category of technologies capable of enabling, enhancing, and preserving data privacy concerns throughout the data lifecycle.[32] Some of the tools and solutions organisations are increasingly adopting are:

i. Personal Data Stores (PDS)

Personal Data Stores (PDS) are consumer-facing apps, services and systems which enable individuals to access and control data about them, and decide what information they want to share and with whom. The system provides transparency and agency to individuals over the data they generate and can be used to empower citizens with the managing and processing of data about them.[33]

ii. Homomorphic Encryption

Homomorphic encryption is a form of encryption that allows certain computations on encrypted data, that then generates an encrypted result which, when decrypted, matches the result of the same operations performed on the data before encryption. It might be used in particular to securely outsource certain specific operations on sensitive data to the cloud, or to another third party organisation. It can also be used in combination with other PETs to safely share data.[34] It provides confidentiality and is viable for use while addressing problems of 'insecurity' and 'exposure' and the risk of revealing sensitive attributes related to individuals or organisations, in a dataset or output.

---

[30] Privacy Enhancing Technologies, available at <https://101blockchains.com/privacy-enhancing-technologies/>- [Accessed 23 January 2022].
[31] Section 66
[32] Iredale, G., 2022. *What are Privacy-Enhancing Technologies (PETs)?.* [online] 101 Blockchains. Available at: <https://101blockchains.com/privacy-enhancing-technologies/> [Accessed 25 January 2022].
[33] The Royal Society, *Protecting privacy in practice- The current use, development and limits of Privacy Enhancing Technologies in data analysis,* March 2019 -<https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf>- on 12 September 2021.
[34] Ibid

However, some of the concerns raised about this method include it being extremely computationally expensive, having a lower throughput and entailing a substantial increase in data size, which can cause a major bandwidth problem.

iii. Trusted Execution Environment (TEE)

A Trusted Execution Environment (TEE) is a secure area inside a main processor. It is isolated from the rest of the system, such that the operating system cannot read the code in the TEE. However, TEEs can access memory outside and can also protect data 'at rest', when it is not being analysed, through encryption. Similar to homomorphic encryption, TEEs can be used to securely outsource computations on sensitive data to the cloud.[35]

As witnessed in other existing cryptographic technology, protecting secure keys in TEEs remains a challenge and it is thus important particularly to protect the system that generates secure crypto functions.

iv. Secure Multi-Party Computation (MPC)

A subfield of cryptography, secure multi-party computation (MPC) is concerned with enabling private distributed computations. MPC protocols allow computation or analysis on combined data without the different parties revealing their own private input. Specifically, it may be used when two or more parties want to carry out analyses on their combined data but, for legal or other reasons, they cannot share data with one another. A good example would be that MPC can allow bidders to identify who has won an auction without revealing anything about the actual bids.[36]

v. The Differential Privacy

The differential privacy security means that, when a dataset or result is released, it should not give much more information about a particular individual than if that individual had not been included in the dataset. As opposed to the previous three PETs which address privacy during computation, differential privacy addresses privacy in disclosure.[37] This mechanism can, in particular, provide secure public access to private datasets and protect data whilst disclosing derived information.

Policymakers have considered PETs as technical tools or methods for achieving compliance with data protection requirements or legislations. Generally, the functionality of PETs is implied in unison with different organisational measures, which includes personnel management and access controls, audits, information security policies, and procedures.[38]

---

[35] Ibid
[36] Ibid
[37] Ibid
[38] Labhuram, A., 2022. *Privacy Enhancing Technologies (PETs) and championing their utilisation in the Kenyan data protection environment* - Centre for Intellectual Property and Information Technology law.

While this field is rapidly evolving, with many of the most promising tools having a rich research heritage, they are currently still relatively new to real-world applications.[39]

However, it is safe to conclude that with the advances in underlying techniques, PETs have started to be deployed in real-life scenarios – with national intelligence and healthcare as key sectors of early adoption, as well as anti-money laundering and financial crime prevention.[40]

There is therefore a need to ensure the acceleration of research and development of PETs, promote expertise and assurance for implementation of technological applications in both the public and private sectors, and create a skilled workforce needed to develop and implement PETs.[41]

d. Public Participation with ODPC

The ODPC and the Ministry of ICT published three draft regulations and consequently invited public consultation on 13 April 2021 with comments accepted until 11 May 2021. In relation to the same, the Ministry also extended an invitation to interested parties to attend virtual public hearings on the draft regulations.

The Office also held a validation forum by stakeholders under public participation which invited stakeholders to offer comments on the ODPC Draft Strategic Plan (FY 2021/2022- 2023/2024). Consequently, the Office also received written submissions from the public on the draft Strategic Plan.

Since beginning its operations, the ODPC has participated in multiple consultations including webinars hosted by civic societies, private and government entities both locally and internationally, to create awareness and champion for data protection in Kenya.

Chapter 3: Priority and Agenda Setting for 2022

a. Privacy and Elections

With the entire election cycle growing increasingly data dependent, and democratic engagement becoming increasingly mediated by digital technology, there have been

---

[online] Centre for Intellectual Property and Information Technology law. Available at: <https://cipit.strathmore.edu/privacy-enhancing-technologies-pets-and-championing-their-utilisation-in-the-kenyan-data-protection-environment/> [Accessed 25 January 2022].

[39] The Royal Society, *Protecting privacy in practice- The current use, development and limits of Privacy Enhancing Technologies in data analysis,* March 2019 -<https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf>- on 12 September 2021.

[40] Future-fis.com. 2022. *Case Studies Of The Use Of Privacy Preserving Analysis To Tackle Financial Crime.* [online] Available at: <https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_innovation_and_discussion_paper_-_case_studies_of_the_use_of_privacy_preserving_analysis_-_v.1.3.pdf> [Accessed 25 January 2022].

[41] Ibid

novel issues and challenges for all electoral stakeholders on how to protect citizens' data from exploitation.[42]

Personal data has become central to this emerging way of seeking to influence democratic processes. This has been witnessed through the amassing and processing of vast amounts of data, and thereafter profiling of individuals based on their stated or inferred political views, preferences, and characteristics. Through these profiles, individuals are then targeted with news, disinformation, political messages, and many other forms of content aimed at influencing and potentially manipulating their views.[43]

In Kenya, the 2007/8 elections saw some local language radio stations used to fan the flames of ethnic violence by exploiting the homogeneity of their respective listeners to disseminate messages of hate.[44] Bulk text messages were also used to target specific communities so as to divide Kenyans along tribal lines to the extent that the then Safaricom CEO, Michael Joseph, considered blocking text messaging services.[45]

The nuance applied to targeting had considerably developed by the 2013 and 2017 election cycles, especially due to the growth of social media use and the large-scale collection of personal data taking place on such platforms.[46] The sheer volume and scope of personal data available to political actors through these platforms meant that the precision of targeting could be infinitely refined.

In both cycles, it is widely reported that Cambridge Analytica rendered its services to various political actors in the country. Cambridge Analytica's involvement in Kenya—which it has described as "the largest political research project ever conducted in East Africa "—entailed a large-scale gathering of Kenyans' data through participant surveys. Coupled with the personal data it had already improperly acquired through Facebook, it was ostensibly able to carry out micro targeting. It further claimed to be able to craft messages specific to individuals as opposed to broad demographics. In particular, it admitted to developing messaging to leverage voters' fears of tribal violence.[47]

Effectively, the enactment of the Data Protection Act translates to several obligations for political actors seeking to make use of personal data. For example, the Act introduces mandates that would invariably hamper political actors' ordinary collection and use of personal data. Since it provides prescriptions at each stage of the data lifecycle (collection, storage, use, analysis, and destruction), political actors have to

---

[42] Privacyinternational.org. 2022. *Data and Elections | Privacy International.* [online] Available at: https://privacyinternational.org/learn/data-and-elections [Accessed 24 January 2022].
[43] Ibid
[44] Rutenberg, A., 2022. *Securing Kenya's Electoral Integrity: Regulating Personal Data Use.* [online] The Elephant. Available at: https://www.theelephant.info/op-eds/2021/10/01/securing-kenyas-electoral-integrity-regulating-personal-data-use/ [Accessed 24 January 2022].
[45] Ibid
[46] Ibid
[47] Ibid

be more careful. Case in point is such as, while it was previously easy to collect personal data indirectly and indiscriminately, political actors now have to do so directly seeking the consent of the individuals to whom the data relates (data subjects).[48]

The principles underpinning the Act also operate to restrict some of the micro targeting practises political actors engage in. i.e. the requirement that political actors only collect and make use of the minimum amount of data required for the lawful purpose they are engaged in, aids to foreclose to a given extent, the issue of micro targeting which heavily relies on a wide scope of personal data.[49]

The Data Protection Act brings the practises around personal data collection and use under the supervision of the Data Commissioner, creating an oversight mechanism with whom these political actors would be required to register.

It is the expectation that this recent enforcement and implementation of data protection law in Kenya and the appointment of the Data Protection Commissioner offers positive material change and plays a fundamental role in covering any loopholes that can be exploited by political campaigns through issuing binding enforceable guidance on the use of data in political campaigning in the upcoming elections.

With the 2022 general elections quickly making way, synergistic collaborations with academics, civil society, and private and public sectors will greatly contribute to a better understanding of data protection concepts, and how various actors are to conduct themselves. These efforts may also increase the electorate's understanding of how micro targeting works, the steps they can take to reduce their susceptibility to targeted messaging and the efforts to improve the culture around personal data use in campaigns.

b. Regional Engagement on Continental Data Policy

The African Union Commission (AUC) has been in the process of developing a Data Policy Framework for Africa. To this end, AUC has sought to curate a Policy that respects, protects and fulfils human rights and provides a shared vision of a data realm that is achieved in a just and fair manner, whilst creating the safe and trusted digital environment necessary for the development of a sustainable and inclusive African digital economy and society.[50]

Taking into consideration the fact that data is used in everyday life across the continent, it is imperative that States and stakeholders champion for consistent regional consultation engagement to ensure the framework will provide

[48] Ibid
[49] Ibid
[50] Weekly, V., 2022. *Data Policy Framework for Africa – Vellum Kenya*. [online] Vellum.co.ke. Available at: https://vellum.co.ke/data-policy-framework-for-africa/ [Accessed 21 January 2022].

principle-based guidance to the member states in their domestication of the continental data policy appropriate to their conditions.[51]

c. Digital Lending

The widespread use of mobile phones, high demand for credit and a fairly lax regulatory environment has contributed greatly to Kenya's unprecedented growth in the digital lending ecosystem. This practice, which is particularly attractive to first-time borrowers who would otherwise be locked out of the lending process due to a lack of a credit history, adopts the use of AI, machine learning and automation technologies to derive the customer's credit score.[52]

The programs run both traditional customer data and alternative data including data that has been generated by a customer through digital interactions such as their browsing history, call logs, messages and GPS data.[53]

This continued transfer of personal data through digital channels has raised many privacy concerns. A good example has been the public outcry against digital lenders' use of non-financial data in the past year, where they were accused of using mined phone data to engage in debt shaming practises and predatory lending tactics.

As a result of a lack of regulation in the sector, customer privacy was never guaranteed as digital lenders arbitrarily shared user data with third parties. Customers defaulting on loan repayments faced unending reminder calls from debt collectors, who also used shaming tactics like calling friends and family to compel defaulters to pay.[54]

In its mandate to protect Kenyans against such unscrupulous practises, the Central Bank of Kenya (Amendment) Act, 2021 serves to ensure better regulation of the sector and weeding out unscrupulous dealers as well as borrowers in the digital lending space. The amendment Act gives authority to the Central Bank of Kenya to license digital lenders in the country as well as ensure the existence of fair and non-discriminatory practices in the credit market.[55]

The enactment of the DPA is expected to revolutionise the way in which these firms handle data and the various aspects of their involvement with the customer's data. It

---

[51] Ibid

[52] Mutheu, A., 2022. *Digital Lending and Data Privacy in Kenya - Mutie Advocates*. [online] Mutie Advocates. Available at: https://www.mutie-advocates.com/how-the-data-protection-act-will-impact-digital-lending-in-kenya/ [Accessed 24 January 2022].

[53] Ibid

[54] Njanja, A., 2022. TechCrunch is part of the Yahoo family of brands. [online] Techcrunch.com. Available at: https://techcrunch.com/2021/12/07/kenyas-president-signs-new-law-to-police-digital-lenders-apps-have-six-months-to-apply-for-licenses/ [Accessed 24 January 2022].

[55] Ibid

introduces stringent compliance obligations and standards to curtail the rampant misuse of data.

Among the expected changes, is registration of digital lenders with the Data Commissioner, transparency and fairness in the collection and processing of personal data, transparency and fairness in credit scoring, requirements for compliance with privacy by design and default before rolling out a system or process, use of appropriate mechanisms while conducting direct marketing including clear affirmative action on the part of the data subject, personal data breach management, and the introduction of data protection impact assessments in instances where a digital lender seeks to introduce a process or technology which impacts the privacy of its customers.

d. Huduma Namba

Kenya's Huduma Namba, meaning service number in Swahili, is a biometric digital identity program which is intended to be the 'single source of truth' about a person's identity. Kenya established the National Integrated Identity Management System ("**NIIMS**") in 2019 to administer the collection and storage of personal data for the Huduma Namba program.[56]

To this end, there have been released the Huduma Bill ("Huduma Bill ") as a standalone statute intended to provide firm legal backing to the NIIMS and govern its functioning. However, the previous drafts of the Bill, i.e. 2019 and 2020 both failed to address key issues of inclusivity which were raised in court petitions, and memorandums submitted by the public.

The most recent draft, the Huduma Bill 2021 proposes a primary law on civil registration and legal identity management and would effectively repeal and replace the Registration of Persons Act, the Births and Deaths Registration Act, and the Kenya Citizens and Foreign Nationals Management Act.[57] It proposes fines of up to Sh10,000 (approximately US$88.35) for those who fail to show up for digital ID registration or to include their children in the NIIMS databases which Huduma Namba is built on.[58]

The Bill seeks to comply with the provisions of Data Protection Act of 2019 by providing for various safeguards on data collection, processing, restrictions, access,

[56] Macdonald, A., 2022. *Kenya pushes on with Huduma Namba as compulsory digital ID amid controversy | Biometric Update*. [online] Biometric Update |. Available at: https://www.biometricupdate.com/202201/kenya-pushes-on-with-huduma-namba-as-compulsory-digital-id-amid-controversy [Accessed 24 January 2022].
[57] Citizenshiprightsafrica.org. 2022. *Kenya: Huduma Bill, 2021 : Citizenship Rights in Africa Initiative*. [online] Available at: https://citizenshiprightsafrica.org/kenya-huduma-bill-2021/ [Accessed 24 January 2022].
[58] Macdonald, A., 2022. *Kenya pushes on with Huduma Namba as compulsory digital ID amid controversy | Biometric Update*. [online] Biometric Update |. Available at: https://www.biometricupdate.com/202201/kenya-pushes-on-with-huduma-namba-as-compulsory-digital-id-amid-controversy [Accessed 24 January 2022].

technical security, right of rectification, confidentiality, location of data servers and designation of a data protection officer.[59]

This is particularly relevant given Kenya has already collected extensive information about its citizens and residents, including biometric information such as fingerprints, hand geometry, retina and iris patterns, voice waves, as well as DNA and GPS data. The Bill curbs unlawful use of information like names, date of birth, postcode and residences, it restricts the sharing of personal data and prohibits publication, display or public posting of biometric data collected.

In roping in the provisions of the Data Protection Act in the processing of personal data, the Bill seeks to unlock an impasse in the roll-out of Huduma Namba cards to Kenyans after the High Court declared the process of rolling out Huduma Cards illegal for being in conflict with the Data Protection Act.[60] Justice Jairus Ngaah found that the government had started collecting personal data from Kenyans without first determining how it would protect that data and that it had not appreciated the import and the extent of the application of the Data Protection Act with respect to the collection and processing of data under the NIIMS.

As a result, the court compelled the Government to complete a data protection impact assessment, as required by the Data Protection Act (2019), prior to processing of data or rolling out Huduma Cards.

Challenges and Recommendations: Moving The Data Protection Act Forward

Lawyers Hub in its various forums noted the following challenges in privacy developments and consequently makes recommendations to this effect:

a. Slow response to compliance since the DPA came into force in 2019

According to a poll run by Amnesty International, 14% of telecommunication/mobile service providers, 13% of mobile money agents and 9% of police officers are ranked as the greatest violators of personal information and people's right to privacy.[61] These figures demonstrate a lax approach to compliance with the Act, especially due to a lack of regulations being in place.

We recommend that data controllers and data processors take immediate steps to ensure compliance with the DPA including undertaking audits on how they process personal data, putting in place data privacy policies, data privacy notices, data

[59] Part 6 of the Huduma Bill 2021.
[60] MUTAI, E., 2022. *Leaking Huduma Namba data to attract Sh5m fine*. [online] Available at: https://www.businessdailyafrica.com/bd/economy/leaking-huduma-namba-data-to-attract-sh5m-fine-3666040 [Accessed 24 January 2022].
[61] Amnesty International Kenya. 2022. *Kenyans Still Unaware of Data Protection and Right to Privacy - Amnesty International Kenya.* [online] Available at: <https://www.amnestykenya.org/kenyans-still-unaware-of-data-protection-and-right-to-privacy/> [Accessed 27 January 2022].

transfer/sharing agreements and data storage policies and reviewing/inserting data protection clauses in standard form contracts.

b. Lack of a Sectoral Approach to Compliance

The enactment of the Data Protection Act directly affects the operation of several institutions, sectors and the laws that govern them. Sectors such as finance and health, processes involving electorates, births and death registration, immigration to mention but a few are now directly affected by the Data Protection Act and need to come into compliance with it in so far as their activities are concerned.

c. Financial and Institutional Handicap of the ODPC

One of the greatest threats to the Office of The Data Protection Commissioner is a lack of funding. Just like any other new statutory body in Kenya, funding is hardly provided for in advance.[62] The Office has already taken months to get funding for operations from the exchequer, and the release of such funding remains unknown to the general public.

Even with funding, an analysis of data protection authorities across the world indicates that they are generally underfunded and are not able to effectively carry out their mandates and are constrained in attracting good personnel.[63]

As was recommended during the ODPC's Strategic Plan validation exercise, it is crucial for the Office to explore additional funding options and income generating activities in order to ensure self-sustenance and further cement its independence as an office.

d. There is No Coordinated Approach to Creation of Awareness.

Many Kenyans are still unaware of data protection and the right to privacy. According to the poll run by Amnesty International, only 54% of Kenyans are aware they have the right to privacy, while 70% remain unaware of the data protection act nearly 2 years since its commencement.[64]

It is imperative for comprehensive public education to be conducted across the nation and for swift enforcement of the data protection act to be intensified.

---

[62] Laibuta, M., 2022. *What awaits the Data Protection Commissioner - Mugambi Laibuta.* [online] Mugambi Laibuta. Available at: <https://www.laibuta.com/data-protection/what-awaits-the-data-protection-commissioner/> [Accessed 27 January 2022].
[63] Ibid
[64] Ibid

Conclusion

Two years into the application of the Data Protection Act, everyone is cognisant of challenges related to enforcing this legislation. However, the Office of The Data Protection Commissioner is strategically positioned to continue identifying core issues arising from the operationalisation of various enforcement mechanisms.

From the harmonisation of sectoral laws, to lack of sufficient resources, to a lack of coordinated approach, to the creation of awareness, the issues raised offer a clear path forward to significantly improve the enforcement of the Data Protection Act.

The relevant parties are well capable of making these improvements, by illuminating certain provisions and providing the ODPC with appropriate tools and resources to fulfil its mandate.

Much still remains at stake and getting the Act enforcement right is of paramount importance for effectively guaranteeing the right to data protection.

We therefore urge the Government, the Office of The Data Protection Commissioner, civic societies, private entities and all relevant stakeholders to work together to address these issues and unlock the full potential of the Data Protection Act to improve people's lives.

Happy Data Privacy day 2022 from the Lawyers Hub Team.

Email: info@lawyershub.ke | Location: 6th Floor, ACK Garden House, Upper Hill on 1st Ngong Avenue| Phone: +254207840228 +254784840228 | P.O Box 2468-00621 Nairobi, Kenya | www.lawyershub.org