KICTANet
The Power of Communities

Five Years of Kenya's Data Protection Act

Reflections and Considerations for the Future

Published by:
Kenya ICT Action Network (KICTANet)
Email: info@kictanet.or.ke
Web: www.kictanet.or.ke
Twitter: @kictanet
Facebook: @kictanet
Instagram: @kictanet
LinkedIn: @KICTANet
Youtube: @kictanet8886
tiktok: @KICTANet

Lead Researcher:
Sigi Waigumo Mwanzia

Research Assistant:
Linda Gichohi

Editors:
Dr. Grace Githaiga
Victor Kapiyo

Acknowledgements:
KICTANet is grateful to our funders and the following for providing invaluable contributions to this publication: the Commission on Administrative Justice, Sarah Wesonga, Ivy Kinuthia, Florence Ogonjo, Barrack Otieno, Benard Matu, Benson Muite, John Gathii, Kamochi Ombiro, Levine Njau, Mildred Achoch, Ochieng' Odaro, Wambui Wamunyu, among others.

Design & Layout:
Stanley K. Murage - stanmuus@gmail.com

Year of publication:
Policy Brief No. 19, May 2024

Photo (Title):
www.freepik.com

Table of Contents

Executive Summary 4
1.0 Introduction and Background 7
1.1 Overview of Key Concepts 7
1.1.1 Data Protection 7
1.1.2 Digital Sovereignty 7
1.1.3 Data Flows 8
1.2 Overview of Policy and Legal Framework 10
1.2.1 Data Protection Act, 2019 10
1.2.2 Regulations and Guidelines 11
1.2.3 ODPC Strategy 12
2.0 Analysis of the Implementation and Enforcement of the Data Protection Act, 2019 13
2.1 Registration of Data Processors and Controllers 13
2.1.1 Low Registration of Data Handlers 13
2.1.2 Collaboration of ODPC with Sector Regulators in Licensing is Essential 14
2.2 DPA Impact on Data Protection Practices by Data Handlers 14
2.2.1 Effective Enforcement Incentivises Compliance 14
2.2.2 Compliance Is Costly for Small Organizations 15
2.2.3 Business Practices are Changing 15
2.3 Awareness Raising 16
2.4 Data Breaches and Enforcement by ODPC 17
2.4.1 Financial Services Sector is Notorious for DPA violations 18
2.4.2 Failure to Obtain Consent Remains a Central Complaint 18
2.4.3 Consent and the Commercial Use of Data 19
2.4.4 Collection of Sensitive Personal Data 20
2.4.5 Emphasis on Data Subjects' Rights 22
3.0 Challenges and Opportunities in Data Protection Implementation 24
3.1 SWOT of ODPC/Data Protection in Kenya 24
3.2 Opportunities in DPA Implementation 25
3.2.1 Adequacy Framework and Cross-Border Data Transfers 25
3.2.2 Integrate and Monitor Impact of Emerging Technologies 26
3.2.3 Promoting Cross-Border Collaboration 26
3.2.4 Promoting Innovation and Investment in Data Protection Technologies and Services 26
3.2.5 Data Protection as an Intersectional Gateway Requiring Multistakeholder Collaboration 27
3.2.6 Strict Enforcement of Unregulated Data Handlers 28
3.2.7 Internalisation of Data Protection by Design/Default by Data Handlers 28
3.2.8 Legislative Clarity to Address Overlapping Mandates 28
4.0 Conclusion and Key Considerations for the Future 30

Executive Summary

Kenya is on the cusp of celebrating five years since the enactment of the Data Protection Act, (DPA) on 25th November 2019. The enactment of this law represents 15 years of domestic and international advocacy efforts towards establishing a comprehensive privacy and data protection framework for the country.

The objective of this policy brief is to review the robustness of Kenya's policy and legal framework for the protection of privacy and personal data. It also presents an opportunity to reflect on Kenya's progress, challenges and opportunities in its journey towards the implementation of the DPA, and also identify areas for enhancement and reform.

The methodology for this brief included desk review of relevant literature, online focus group discussions on the KICTANet mailing[1] list, and key informant interviews.

The key findings in the report include:

Progressive Trends:

1. Broad policy and regulatory framework to promote privacy and data protection, such as the establishment of the Office of the Data Protection Commissioner (ODPC) and enactment of policies, laws, regulations and guidelines.

2. Commendable steps by the ODPC to implement and enforce the DPA, 2019, enhance its capacity to discharge its mandate through staff recruitment, increase its funding and budgetary allocations, utilise technology, decentralise its functions to regional offices, and collaborate with stakeholders.

3. Increasing public awareness and stakeholder engagement interventions by ODPC and key stakeholders on privacy and data protection.

4. Increasing compliance by non-state entities evidenced through registration, appointment of Data Protection Officers (DPOs), updating/publication of data protection policies, change of internal practices e.g., data minimisation, accountability principle, consent for marketing operations.

5. Existence of a robust dispute resolution mechanism that integrates voluntary Alternative Dispute Resolution (ADR) mechanism and evolving jurisprudence by ODPC and courts that are reinforcing data subject rights, promoting data protection principles, and clarifying the roles of data collectors and processors.

6. Willingness by other jurisdictions to offer Kenya equivalency status which can enhance trade and cooperation.

Problematic Trends:

1. Threats to the independence of the ODPC due to limited funding, low staffing, legal structure, political interference, recommendations for a Board appointment, and the existence of competing data protection roles/responsibilities with other sector regulators.

2. Poor enforcement of the DPA against state actors, entities in the financial sector, and Big Tech giants who continue to process vast amounts of personal data.

1. These discussions were held between 22nd May and 2nd of April 2024.

3 Lack of a holistic national data governance framework. Low registration levels of data handlers, with at least 90% of potentially registrable business or corporate entities remaining unregistered.

4 Legislative gaps include the lack of a data-sharing framework for state entities, guidelines on the commercial use of data, a data protection code of practice for journalism, literature and art, and an adequacy framework for cross-border data transfers.

5 Low public awareness and poor compliance levels among registrable small and medium-sized (SMEs) organisations.

6 Weak inter-agency coordination and cooperation amongst sector regulators and ministries (e.g., the Communications Authority of Kenya, the Central Bank of Kenya, the Ministry of Health, the Ministry of Trade and Industry, the Companies Registry, the Competition Authority of Kenya, the Kenya Revenue Authority) leading to oversight and enforcement gaps.

7 Pressure from other jurisdictions for alternative data protection regimes (e.g., the Cross Border Privacy Rules (CBPR)) which could affect the sovereignty of ODPC and the effectiveness of the DPA.

8 Entities are deploying and harnessing emerging and automated technologies, such as AI, to process personal data without effective intervention or oversight from the ODPC.

Recommendations to Kenyan Stakeholders:

1 Parliament should strengthen the independence of the ODPC by amending the DPA to make the ODPC autonomous and separate it from the ICT Ministry, and increase the ODPCs budgetary allocation to enable it to effectively discharge its mandate across the country.

2 ICT Cabinet Secretary to formulate a comprehensive national data governance framework to holistically address complimentary data protection issues, including interoperability, data classification, and data security.

3 ICT Cabinet Secretary/ODPC should issue relevant guidelines, codes, and frameworks to fully operationalize the DPA, including publishing guidance for lawful data-sharing between state agencies, and adequacy rules to facilitate lawful cross-border data transfers.

4 ODPC should obtain equivalency status with other jurisdictions and collaborate with other government agencies to reap economic benefits.

5 ODPC should intensify efforts to regulate and oversee the data processing operations of all data handlers, especially state entities, Big Tech, and the financial sector. Further, it should engage, coordinate and cooperate with relevant sector regulators/ministries to address the emerging compliance, oversight and enforcement gaps.

6 ODPC should build its internal capacity to understand and respond to the potential risks and impact of emerging technologies, such as artificial intelligence (AI), blockchain, the Internet of Things (IoTs), digital asset management, robotics, fintech, cloud computing, virtual reality, big data analytics, genomics and biometric technologies, amongst others.

7 ODPC should enhance greater transparency and accountability in their compliance, complaints and risk management systems by publishing all decisions, enforcement and penalty notices. Further, the ODPC should publish all pending registers, including an updated register of noncompliance, an updated register of complaints, a register

of suspended/deregistered data handlers, and a data protection risk register.

Recommendation to African Data Protection Authorities (ADPAs):

1 Prioritise critical issues within their jurisdiction to ensure a strategic, consistent, responsive, and tailored response to data protection concerns. Governments are encouraged to provide ADPAs with the requisite resources to effectively exercise their mandate.

2 Develop sector- and issue-specific guidelines to facilitate the conduct of impact assessments, due diligence and compliance by data controllers and processors in critical sectors including education, elections, emerging technologies, finance, identity management, health, national security, transport, and telecommunications.

3 Review and assess data localisation requirements in national data protection legal frameworks and consider these against human rights implications, domestic digital agenda and economy priorities, and citizens' privacy and security concerns about data residency.

4 Be proactive in adopting adequacy decisions as part of the operationalisation of legal frameworks on cross-border data transfers and establish proof of appropriate safeguards from data handlers prior to personal data transfers to other jurisdictions. Publish guidance notes on Cross Border Privacy Rules (CBPR) and other international mechanisms to determine if they are compatible with their national data protection legal frameworks.

5 Promote transparency in regulatory activities, given the mutually-reinforcing relationship between data protection, access to information, transparency, and open data and the need to maintain trust in data ecosystems.

1.0 Introduction and Background

1.1 Overview of Key Concepts

1.1.1 Data Protection

The term 'data protection' refers to the holistic "combination of legal, administrative and technical safeguards,"[2] e.g., practices, measures, laws, and policies, aimed at safeguarding personal data from various risks, threats, or unauthorised access, ensuring its availability, integrity, and confidentiality.

The term 'data protection' comprises two constituent parts, namely
(1) Data, and
(2) Protection. Data protection laws exclusively deal with 'personal data', to the exclusion of 'non-personal data.'[3] In jurisdictions that have internalised the European Union's (EU) GDPR definition, personal data is founded on four (4) building blocks.

These include "
(i) any information
(ii) relating to
(iii) an identified or identifiable
(iv) natural person.[4]

Sensitive personal data and pseudonymous data are also protected under data protection laws.

The exclusion of non-personal data is mandatory for purposes of defining the scope of application of data protection legal frameworks.[5]

However, the distinction between personal and non-personal data (e.g., anonymous data) is extremely difficult to maintain in practice given the risk of re-identification.

This is attributed to the emerging and sophisticated technologies, such as data analysis algorithms, that enable the use of varied data sets to re-identify an individual through "inferences, singling out and linkability."[6]

The 'protection' element of data protection refers to the strategic act of safeguarding, securing, or preserving personal information from unauthorised access, damage, loss, or harm.[7]

1.1.2 Digital Sovereignty

The term 'digital sovereignty' refers to the need for state control and ownership of key technology assets, including data and infrastructure.[8]

---

2. World Bank (2019) ID4D Practitioner's Guide.
3. Non-personal data refers to de-personalised data, i.e., data that does not permit the identification of an identified or identifiable natural person due to the removal of personal identifiers. One example of non-personal data is anonymous data. See: Michèle Finck, Frank Pallas (2020) They who must not be identified—distinguishing personal from non-personal data under the GDPR; Section 2, Data Protection Act, 2019.
4. See: IAPP (2023) European Data Protection Law and Practice.
5. Section 2 of Kenya's DPA defines personal data as "any information relating to an identified or identifiable natural person."
6. Michèle Finck & Frank Pallas (2020) They who must not be identified—distinguishing personal from non-personal data under the GDPR.
7. The protection of personal data is necessary for the 'empowerment of individuals, restraining harmful data practices, and limiting data exploitation by companies and governments.' See: Privacy International (2018) A Guide for Policy Engagement on Data Protection.
8. World Economic Forum (2021) What is digital sovereignty and why is Europe so interested in it?

Digital sovereignty intersects with data protection as a critical component of any country's evolving digital transformation and digital governance landscapes, and in response to an escalating geopolitical battle for digital dominance.[9]

Nation states exert their digital sovereignty in the data protection sphere through the development and implementation of legal and policy frameworks that specify how personal data can be processed and transferred by local and foreign entities.

1.1.3 Data Flows

The term 'data flows' in relation to data protection refers to the movement or transfer of personal data from one location or entity to another, using automated or non-automated means.

The regulated flow of personal data is integral given technological advancements that have magnified the increased value of personal data and the associated privacy and security risks of unregulated data flows.

The inclusion of localisation provisions in data protection legal frameworks is designed to domesticate data and encourage investments in local data infrastructure as part of data protectionism efforts by nation states.[10]

These localisation provisions have been the topic of debate given their impact on trade and digital economies.

GUIDING NOTE: DIGITAL SOVEREIGNTY AND CROSS-BORDER DATA TRANSFERS

Digital sovereignty is, at its core, a timeless jurisdiction question invoking the concept of the sovereign nation state. It requires African Data Protection Authorities (ADPAs) to collaboratively establish holistic data governance mechanisms, and address specific data protection queries such as cross-border data flows, data ownership, and data localisation.

Domestically and regionally, ADPAs are encouraged to work collaboratively with other regulatory agencies to ascertain the impact of cross-cutting issues such as trade, competition, taxation, and consumer protection. The African Union's (AU) Digital Transformation Strategy for Africa (2020 - 2030) and the AU's Data Protection Framework provide ADPAs with guiding frameworks.[11]

A Global CBPR Forum has been established to "promote interoperability and help bridge different regulatory approaches to data protection and privacy", implementing the Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems.[12]

However some stakeholders have raised concerns about CBPR's impact on the sovereignty of a government's laws and regulators for varied reasons. First, the CBPR takes away the power of rule-setting from national governments to other bodies, such as industry bodies.

Secondly, the CBPR takes away DPAs regulatory powers and proposes to bestow them upon Accountability Agents, and lastly takes away the power of a government to imple-

9. Litha Mzinyati (2023) How to Achieve African Digital Sovereignty.
10. Data localisation is facilitated through data residency or compulsory local data storage requirements in legal frameworks.
11. African Union (2020) Digital Transformation Strategy for Africa (2020-2030); African Union (2022) Data Policy Framework.
12. US Department of Commerce, Global Cross-Border Privacy Rules Declaration.

ment enforcement mechanisms.[13]
In April 2024, the US Department of Commerce and the Kenyan Ministry of ICT issued a statement indicating that Kenya will engage with the Global CBPR Forum whilst also recognizing "the need to incorporate African countries' perspectives in the development of international mechanisms."

1.2 Overview of Policy and Legal Framework

The journey to protect individuals' personal data in Kenya has been marked by a series of concerted multi-stakeholder efforts spanning a period of fifteen (15) years to modernise the nation's legal and policy framework[14].

To a large extent, the enactment of the Data Protection Act was a critical milestone spurred by growing digitisation drives, increased use and threats to personal data, foreign and domestic pressures and renewed political will.

Moreover, its enactment was catalysed by strategic litigation contesting the unregulated collection of personal and sensitive personal data for digital identity purposes by the State under the 'Huduma Namba' drive.[15]

Kenya has a robust legal, policy and institutional framework for privacy and data protection. This framework comprises the Constitution of Kenya, 2010, the DPA, various sector-specific legislation,[16] three (3) regulations, eight (8) guidelines, case law (from the Kenyan courts and determinations by the ODPC), and the Privacy and Data Protection Policy, 2018.[17]

The constitution provides for the right to privacy under Article 31 and a framework for the development of specific laws and regulations aimed at protecting personal data, such as the Access to Information Act, 2016 and the DPA.[18] However, it does not provide for a stand-alone right to data protection.

Kenya is also party to various international treaties and conventions and adheres to the general rules of international law, which form part of the data protection legal framework.[19]

Notably, despite the Malabo Convention coming into force on 8 June 2023, Kenya is yet to sign or ratify the instrument. This hierarchical framework sets out the rules, rights and obligations of individuals, private sector and state entities in respect to data protection and privacy.

The key data protection institutions include the ODPC, the Judiciary, and various sector regulators and licensing entities.

13. US Department of Commerce (2024) Joint Statement on Harnessing Artificial Intelligence, Facilitating Data Flows and Empowering Digital Upskilling Between the United States Department of Commerce and the Kenyan Ministry of Information, 14.
14. Communication and the Digital Economy.
KICTANet (2021) Public participation: An Assessment of Recent ICT Policy Making Processes in Kenya.
15. Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR.
16. Examples include the National Payment System Act (2011), the Consumer Protection Act (2012), the Kenya Information and Communications Act (KICA) (2012), the Access to Information Act (2016), the Computer Misuse and Cybercrimes Act (2018), HIV Prevention and Control Act, among others.
17. The PDPP, 2018 is a policy document that lays the foundation for enforcing Article 31 of the CoK, 2010, informed by global practices in data protection. This policy informed the development of the DPA, 2019, and supports the ODPC's effective application of, and compliance with, the DPA, 2019 to guard against personal data misuse. Commendably, the PDPP, 2018 highlighted the need to safeguard the rights of data subjects, underscoring the special protection that should be provided to children and vulnerable groups.
18. Under Article 31 of the CoK, 2010, individuals have the right not to have: (a) "their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; (d) or the privacy of their communications infringed." See: The Constitution of Kenya, 2010.

1.2.1 Data Protection Act, 2019

The DPA largely mirrors the evolving standard of data protection legislation influenced by the European Union's General Data Protection Regulation (GDPR), with a few notable framing differences. The notable deviations in the DPA include

(a) the establishment of the ODPC as a state office operating within the ICT Ministry, rather than as an independent authority;

(b) the optional rather than mandatory requirement for entities to appoint data protection officers (DPOs); and

(c) the provision of alternative dispute resolution (ADR) mechanisms.

Generally, the DPA outlines the material and territorial scope of its application, defines key terms and outlines the powers, roles and responsibilities of the ODPC and the ICT Cabinet Secretary.

Further, it provides for eight (8) standard data protection principles, outlines data subjects' rights and remedies, imposes restrictions on sensitive personal data processing, regulates data transfers and data localisation, and stipulates the enforcement measures (penalties, fines, compensation, right of appeal).

OBJECTIVES OF THE DPA

The DPA, 2019 regulates personal and sensitive personal data processing by natural or legal persons, referred to as 'data controllers' and 'data processors' (data handlers) in the public and private sectors, guided by five objectives.

These include
(1) Upholding constitutional privacy rights,
(2) Establishing the ODPC for oversight, compliance, and enforcement;
(3) Regulating the processing of personal data via an enforcement of eight (8) data protection principles;
(4) Defining data subjects' rights and remedies;
(5) specifying obligations for data controllers and processors in the public and private sectors; and
(6) providing for ancillary data protection purposes.[20]

In terms of material scope, the DPA applies to personal data, which is defined as "any information relating to an identified or identifiable natural person (i.e., a data subject).[21]"

The DPA also applies to sensitive personal data. Additionally, it covers all data processing operations which broadly includes "any operation performed on personal data or sets of personal data"[22] using automated or manual means.

Two riders are important to note here. Firstly, personal data processed by individuals in the "course of a purely personal or household activity" is excluded by virtue of Section 51 (2)

19. Kenya Law. Kenya Law Treaties and Agreements Database. See: Chatham House (2024) The AU took important action on cybersecurity at its 2024 summit – but more is needed.
20. Section 3 of the DPA, 2019.
21. Sections 2 and 4 of the DPA, 2019.
22. Examples of such operations include collection, storage, retrieval, disclosure by transmission, erasure, destruction, amongst others. See: Section 4 of the DPA, 2019.

of the DPA. In 2024, the ODPC reaffirmed this exemption by dismissing a complaint regarding the processing of personal data using CCTV cameras within the private setting of one's premises.[23] Secondly, any personal data processed by non-automated means must form whole or part of a filing system.

In terms of territorial scope, the DPA applies to all natural or legal persons processing personal data, irrespective of establishment or local residency in Kenya. Similar to the GDPR, the DPA introduced extra-territorial scope for data controllers or processors outside of Kenya processing the personal data of data subjects in Kenya.

The effectiveness of the ODPCs governance structure in the DPA has come under scrutiny by stakeholders in the recent past especially after the Worldcoin project, yet opinion remains divided on the best approach to ensure the independence and effectiveness of the ODPC.

For example, there are proponents for the ODPC to remain as currently structured albeit with enhancements to its enforcement capacity and independence from its parent ministry.

However, an Ad hoc Committee of Parliament recently recommended the establishment of a Board to oversee the ODPCs daily functions.[24] Stakeholders observed that if this proposal was adopted, then it needs to be composed of multi-stakeholder representatives.

A government-only board would risk further weakening the ODPCs governance structures, with implications for Kenya's ability to obtain an EU adequacy decision as part of ongoing discussions between Kenya and the EU.[25]

1.2.2 Regulations and Guidelines

Section 71 of the DPA grants the ICT Cabinet Secretary delegated legislative powers, which have borne three (3) data protection regulations.

These regulations provided much-needed legal clarity to various aspects of the data protection legal framework. They also aid compliance efforts by data handlers and empower data subjects with tools to control and assert ownership over their personal data.

The Data Protection (General Regulations), 2021 elaborate on the provisions in the DPA[26] by expounding on data subjects' rights, data handlers' obligations, restrictions on the commercial use of personal data, and elements of implementing data protection by design or default.
Additionally, it clarifies the categories of notifiable breaches and the legal basis for data transfers, introducing Binding Corporate Rules as a mechanism for data transfers within groups (e.g., parent-subsidiary undertakings) and multinational entities.

Lastly, it also elaborates on the processing activities that require Data Protection Impact Assessments (DPIAs) and the exemptions under the DPA on national security and public interest. Notably, civil registration entities are exempt from these regulations, by virtue of the Data Protection (Civil Registration) Regu-

23. *ODPC (2024) ODPC Complaint No. 2431 of 2023 Determination.*
24. *KICTANet (2023) Why the Data Commissioner Should or Shouldn't Report to a Board.*
25. *Key informant interview (Anon), 03 May 2024.*
26. *The Data Protection (General Regulations), 2021.*

lations, 2021, a move criticised by civil society organisations.[27]

The Data Protection (Registration of Data Controllers and Processors) Regulations, 2021 establishes the framework for registering data controllers and processors, defines the registration criteria and threshold, and provides for the maintenance of a data handlers' register.[28]

Lastly, the Data Protection (Complaints Handling and Enforcement Regulations), 2021 outlines procedures for lodging and determining complaints, and elaborates enforcement mechanisms, including penalties and fines in the event of non-compliance.[29]
To date, the ODPC has issued eight (8) guidance notes[30] aimed at 'fostering a compliance and accountability culture in Kenya and assisting entities to align with the data protection legal framework.[31]

These guidance notes reinforce the ODPC's targeted efforts to promote compliance, particularly in sectors where large personal data sets are amassed for varied purposes, such as communications, finance, education, and healthcare.[32] The remaining four (4) guidance notes provide clarity on consent, data protection impact assessments, the registration of data controllers and processors, and operationalising the ADR mechanisms.

1.2.3 ODPC Strategy

In October 2021, the ODPC published its inaugural Strategic Plan for the 2021-2024 period[33]. The plan outlines its approach to protect personal data in Kenya. It prioritises three (3) key result areas:

(1) The institutional capacity development pillar, which focuses on fully operationalising the ODPC through capacity building,
(2) The regulatory services pillar, and
(3) The awareness creation pillar.

The Strategic Plan heavily emphasises the need for a fully operationalised ODPC to enable an effective regulation of personal data processing operations by data handlers.

Further, the plan magnifies the need to promote self-regulation among data handlers, receive, investigate and resolve complaints, and promote international cooperation.[34]

To date, the ODPC has issued eight (8) guidance notes aimed at 'fostering a compliance and accountability culture in Kenya and assisting entities to align with the data protection legal framework.'

28. The Data Protection (Civil Registration) Regulations, 2021.
29. The Data Protection (Registration of Data Controllers and Processors) Regulations, 2021
30. The Data Protection (Complaints Handling and Enforcement Regulations), 2021
These include: Guidance Note on Registration of Data Controllers and Data Processors; ODPC Guidance Note on Data Protection Impact Assessment; Guidance Note on Consent; Alternative Dispute Resolution (ADR) Framework/Guidelines; Guidance Note For Digital Credit Providers; ODPC Guidance Note on the Processing of Health Data; Guidance Note for the Education Sector; Guidance Note for the Communication Sector. The ODPC has published guidance notes on electoral purposes, but this is not available on the website.
31. ODPC (2024) ODPC Releases Sector-Specific Guidance Notes for Compliance.
32. ODPC (2024) Guidance Note For Digital Credit Providers; ODPC Guidance Note on the Processing of Health Data; Guidance Note for the Education Sector; Guidance Note for the Communication Sector.
34. ODPC (2021) Strategic Plan, FY 2022/3 - 2024/5.

2.0 Analysis of the Implementation and Enforcement of the Data Protection Act, 2019

Kenya's implementation of the DPA commenced in earnest in November 2020, following the appointment of Kenya's inaugural data protection commissioner and the subsequent establishment of the office. Thereafter, it developed and issued three (3) regulations in 2021.

This intervening period granted data controllers and processors an implicit grace period of one (1) year to integrate the data protection principles delineated in Section 25 of the DPA into their operational processes, frameworks, products and services.

Additionally, it enabled the operationalisation of the functions, roles and responsibilities of the ODPC, while affording data subjects an opportunity to understand the implications of the DPA on their personal data.

2.1 Registration of Data Processors and Controllers

The DPA mandates the ODPC to keep and maintain an updated public register of all data handlers in Kenya which can be accessed on the ODPCs website.[35] ODPC (2024) Registered data handlers.

This register enables stakeholders, such as researchers and data subjects, to identify the number of data controllers vis-a-vis data processors with active registration certificates, and the key counties where data processing activities are being undertaken.

2.1.1 Low Registration of Data Handlers

As of April 2024, the ODPC had issued "5,195 registration certificates to entities.[36] According to the register, there are 5,312 registered entities in Kenya which is commendable given that registration officially commenced less than two years ago.[39] Out of these 5,312 entities, KICTANet was able to map out 34 registered state entities on the publicly accessible register, although accordi ng to the ODPC, there are "over 85 registered state entities."[38]

These figures are concerning for various reasons. Firstly, the Registrar of Companies has registered 105,531 business/corporate entities between 2023/2024.[39] Consequently, at least 90% of potentially registrable business or corporate entities remain unregistered, which demonstrates the need for continued efforts to promote awareness and compliance by data handlers.[40]

Secondly, whereas some state agencies are exempted from the DPA, the registration of 85 state entities out of an estimated "526 state corporations".[41] underscores

35. *Ibid.*
36. *ODPC (2024) Registered data handlers.*
37. *Ibid, n.33.*
38. *Respondent, ODPC, 07 May 2024*
39. *These include the Tana Water Works Development Agency, the Anti-Doping Agency of Kenya, and the County Governments*
40. *BRS (Registrar of Companies) (2024) Summary of Registered Entities - In 2023/2024. Leeway has been given here noting the registration threshold in the Registration Regulations.*
41. *Business Daily (2024) President Ruto goes for State corporations' cash surpluses in fresh mop-up.*

the government's lackadaisical approach towards compliance with the data protection legal framework. This serves as evidence that despite the efforts of the ODPC, there are still implementation and compliance challenges reigning in state-led data processing operations.

Moreover, the ODPC is yet to implement Section 55 of the DPA, which requires the development of a data-sharing code specifying the lawful exchange of data between government departments or public sector agencies.[42] Additionally, the absence of approved Guidance Notes for County Governments perpetuates the lack of regulation among state entities at the county level.

2.1.2 Collaboration of ODPC with Sector Regulators in Licensing is Essential

During the Worldcoin saga (explored below), the ODPC clarified that registration does not amount to licensing, i.e., that it does not have the mandate to grant data handlers permission to operate in Kenya.[43]

This clarification between registration and licensing has introduced a novel distinction in Kenya's data protection regulatory framework with implications for data handlers.

It reinforces the notion that compliance with the DPA is an 'ongoing obligation' imposed on data handlers, as magnified in KICTANet's submissions to the National Assembly Ad-Hoc Committee,[44] With a certificate of registration merely serving as prima facie evidence of compliance with registration requirements only.

Additionally, it underscored the principle of accountability in data protection, affirming that data handlers bear the primary responsibility for ensuring that their data processing activities adhere to prescribed legal obligations.

Lastly, it clarified the ODPC's regulatory role as being one of compliance rather than sanctioning data handlers operations through operational licences, which mandate vests with other state entities.

While this latter point has been disputed by some respondents, it buttresses the pressing need for inter-entity collaboration to create an effective privacy and data protection implementation and compliance environment.

2.2 DPA Impact on Data Protection Practices by Data Handlers

2.2.1 Effective Enforcement Incentivises Compliance

The DPA has had a demonstrable impact on non-state data handlers' data protection practices. This brief concludes that two factors have incentivised registrable and registered non-state data handlers in Kenya to internalise compliance as a "continuous obligation" into their business operations.[46]

The first is the material risk of non-compliance on entities' business operations, and particularly the negative impact of penalties, enforcement notices, and deregistration on profit and reputational considerations.

42. Key informant interview (Anon), 03 May 2024. 43. MMS Advocates (2023) Lessons on Data Privacy from the Worldcoin Project in Kenya.
44. KICTANet (2023) Technical Brief on the ODPC registration process and independence of data protection authorities.
45. Bowmans (2022) Kenya: Data Protection – Let's Talk Compliance, Enforcement and Penalties.
46. ODPC. Directorates. See also: Bowmans (2022) Kenya: Data Protection – Let's Talk Compliance, Enforcement and Penalties.

In comparison, a similar impact was not observed in the data protection practices of a majority of state entities who still consider themselves 'custodians of personal data,' with the exception of the seven (7) state data handlers who have registered with the ODPC (see above). Their compliance with the DPA was not assessed in this brief.

The second factor that is driving compliant data protection practices by non-state entities is the operationalisation of the ODPCs Compliance and Complaints, Investigations, and Enforcement directorates, coupled with the ODPCs shift from voluntary compliance to strict enforcement.

This has been facilitated by the provision of monetary and staffing resources to the directorates and the taking effect of the Complaints Handling and Enforcement Procedures Regulations in February 2022.[47]

Moreover, the implementation of the DPA has specifically impacted private entities' adherence to (1) the data minimisation and accountability principles, (2) the integration of consent into business operations where this is used as the legal basis for processing or data transfers,[48] and (3) the promotion of data subjects' accuracy and erasure rights under Section 40 of the DPA.

2.2.2 Compliance Is Costly for Small Organizations

The implementation of the law has had a differentiated Impact on multinational and local entities. Large multinational corporations reported a lower financial compliance burden in comparison to smaller entities with monetary constraints.

Data handlers specifically observed that the cost of compliance rises where an entity falls within the threshold of processing activities where DPIAs are mandated.

Conversely, registrable/registered local entities inevitably face a relatively higher cost, given the introduction of a new regulatory requirement mandating an alignment of their data processing operations with the data protection legal framework.

2.2.3 Business Practices are Changing

2.2.3.1 Marketing Operations

Two key informants working for multinational entities commented that the implementation of the DPA has materially altered their marketing operations, with anonymisation carrying significant risks from a cost and a re-identification perspective.

These alterations sought to align business operations with the provisions on lawful processing, consent, the commercial use of data, and domestic and cross-border data transfers.

One key challenge that was reported is the ongoing failure by the ICT Cabinet Secretary to prescribe practical guidelines for commercial personal data use, as encouraged under Section 37 (3) of the DPA.

2.2.3.2 Internal/External Changes

The study found that both multinational and local entities reported taking steps to update

47. This has enabled the practical implementation of various provisions, including Sections 25, 28, 30, 32, 33, 37, 39, 45, 48, and 49 of the DPA, 2019.
48. Key informant interviews, 30 April 2024.

or develop existing/new data protection internal and external procedures.

Multinational corporations reported material alterations in contractual agreements governing employer-employee, business-to-business relationships, the deletion of unnecessary personal data contained in internal databases, and data-sharing agreements with third-parties.[49] Entities have also recruited data protection officers (DPO), outsourced the DPO role, or integrated the privacy and data protection functions within their legal, audit and risk departments.

Notably, the demand for privacy and data protection services by entities has spurred the creation of employment opportunities and the development of an industry and community of researchers, auditors, lawyers, public policy personnel, innovators and ICT practitioners offering various services in the field of privacy and data protection.

Due to ongoing cross-jurisdictional compliance efforts of multinational entities with data protection laws, such as the EU's GDPR, respondents from these entities noted that the DPA did not have a material impact on their existing data protection policies.

This was attributed to established efforts to comply with the GDPR, consequently allowing these entities to simply update their policies to reflect the provisions of the DPA. Additionally, positions or roles such as in-house data protection officers were already mandated and established roles required in other jurisdictions making DPA compliance at this level comparatively easier.
This is because they were able to simply update them to reflect the DPA provisions while positions or roles such as in-house data protection officers were already established roles required in other jurisdictions.

Locally based organisations which did not have prior engagement with the EU GDPR, have had to put in place various measures to ensure compliance with the DPA.

2.2.3.3 Data Storage and Data Minimisation

Local entities reported material changes to their data storage processes, particularly the storage of sensitive personal data. Further, local entities observed an active integration of data minimisation into business practices, and reported taking steps to delete or erase unnecessary personal data.

2.3 Awareness Raising

The implementation of the DPA has led to a notable increase in awareness levels on privacy rights and data protection among individuals and organisations in Kenya.

This heightened awareness is crucial for fostering a culture of data protection and ensuring that stakeholders understand their rights and obligations under the law.

In March 2021, the ODPC embarked on a spirited campaign targeting key stakeholders to protect personal data by instituting "appropriate privacy awareness[50] The ODPC prioritised capacity building before embarking on capacity strengthening for significantly impacted stakeholders.
This approach considered the varying stakeholder capacities and prioritised their continuing improvement to facilitate implementation efforts.

49. ODPC (2021) Strategic Plan FY 2022/3 - 2024/5, pp. 23.
50. ODPC. Data Handler Registration. ODPC. Report a Data Breach. ODPC. File/Lodge a Complaint.

Central to these awareness-raising efforts is the ODPCs provision of information and knowledge to stakeholders for purposes of providing legal clarity on compliance requirements and enforcement procedures, and safeguarding data subjects' privacy rights.

To achieve this, the ODPC has used a combination of digital (print, online, website, social media) and physical awareness-creation measures.

Few notable examples of these include:

- The establishment of various online portals digitising
- (a) the registration process for data handlers,
- (b) the reporting of data breaches, and (c) the filing/lodging of complaints,[51]

  The provision of regular external communication on ongoing regulatory activities on its online platforms,[These include the ODPC website and social media platforms,[52]

- The hosting of multiple, in-person, awareness creation and consultation trainings/forums,[53]

- The publication of guiding material both clarifying and simplifying the DPA for data handlers in the private and public sectors and data subjects.[54]

  The sensitisation and training of state entities through an ongoing multi-agency awareness campaign in partnership with the Kenya School of Government,[55]

- The sensitisation of the public and data handlers at the grassroots level through the launch of a country-wide awareness campaign, commencing in Machakos, Tana River, Garissa and Nyeri counties,[56]

- The establishment of six (6) regional offices in Nakuru, Mombasa, Kisumu, Garissa, Eldoret, Kisumu, and Nyeri counties, including at Huduma Centres,[57] to cascade ODPC operations and access to ODPC services to the county level.[58]

Strategically, the ODPC is supported in its awareness-raising and capacity building efforts with financial and non-financial support from stakeholders, such as civil society, businesses and development partners.

This support has accelerated the operationalisation of the office and enabled the ODPC's ongoing countrywide public outreach and education campaigns.

51.These include the ODPC website and social media platforms, including LinkedIn, Facebook, Twitter and YouTube.
52.In April 2024, the ODPC partnered with Mastercard Foundation and Amnesty International to provide training to 120 Data Protection Officers on Data Protection Impact Assessments. This training supports the practical dissemination of the ODPCs Guidance Note on Data Protection Impact Assessments. See: ODPC (2024) Data Commissioner Inaugurates Training For Data Protection Officers On Data Protection Impact Assessment.
53. ODPC. Guidelines. ODPC (2023) Data Protection Handbook. ODPC. Data Protection Z Card. ODPC Newsletters. ODPC and Kenya School of Government (2023). Data Protection Curriculum.
54. Kenya News Agency (2023) ODPC Unveils Data Protection Act 2019 Curriculum. This curriculum is not publicly accessible.
55. ODPC (2024) ODPC Launches Country-Wide Awareness Campaign. ODPC (2024). Data Protection Awareness Campaign. Kenya News Agency (2024) Kenyans Told To Be Wary Of Personal Data Protection.
56. These are public service delivery centres deployed under the Huduma Kenya Service Delivery Programme (HKSDP), a Kenya Vision 2030 Flagship Project established vide the Kenya Gazette Notice No. 2177 of 4th April, 2014. See: Huduma Kenya, About Us.
57. ODPC (2024) ODPC's Regional Offices (Nakuru, Mombasa)
58. See: Federal Ministry for Economic Cooperation and Development (BMZ) (2024) Digital Transformation Center Kenya.

Illustratively, the ODPC has successfully partnered with a number of non-profit and development partners, such as the KICTANet, Amnesty International, the Open Institute and the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)[59] to enhance stakeholder awareness and capacity building efforts.

Notably, the GIZ through the Digital Transformation Centre (DTC) has provided extensive resources and support to the ODPC, both from an operational and implementation perspective.

A key informant noted that only 'non-financial, bilateral support' has been provided to the ODPC.[60]

While the receipt of resources from international development partners to implement the DPA is permissible under Section 67 of the DPA, the ODPC must remain alive to the potential influence of these resources on the fulfilment of its mandate.

This challenge is further compounded by the fact that currently, no information is publicly accessible regarding the ODPCs receipt of any grants, gifts, donations or other endowments from partners.[61]

These partnerships, in the context of awareness raising and capacity building, reinforce the importance of the ODPCs national control over the data protection regulatory framework as it pursues collaborations with international entities.

2.4 Data Breaches and Enforcement by ODPC

This section outlines essential ODPC determinations, offering African DPAs valuable jurisprudential guidance for shaping their regulatory authority concerning determinations.

2.4.1 Financial Services Sector is Notorious for DPA violations

As of April 2024, the ODPC had received "5,315 complaints [and issued] 106 determinations, 60 enforcement notices, and 9 penalty notices."[ODPC (2024) ODPC Hosts Media Breakfast Meeting As Kenya Gears Up For NADPA AGM & Conference.

As part of the study, 72 out of the 106 determinations issued by the ODPC were analysed with the majority of the determinations pitting private individuals against private companies.

Some of these determinations involved consolidated complaints. nations, offering African DPAs valuable jurisprudential guidance for shaping their regulatory authority concerning determinations.

59. Examples of this support include: awareness raising based on the ODPCs requests; the operationalisation of the ODPC strategic plan and development of standard operating procedures; connecting ODPC with other DPAs at the international level to provide implementation guidance; the provision of ICT equipment to capacitate the ODPCs office; support to develop the AI Chatbot; support to the ODPC regarding its case management system (internal structuring); support to acquire observer status for Convention 108 (pending), amongst others.

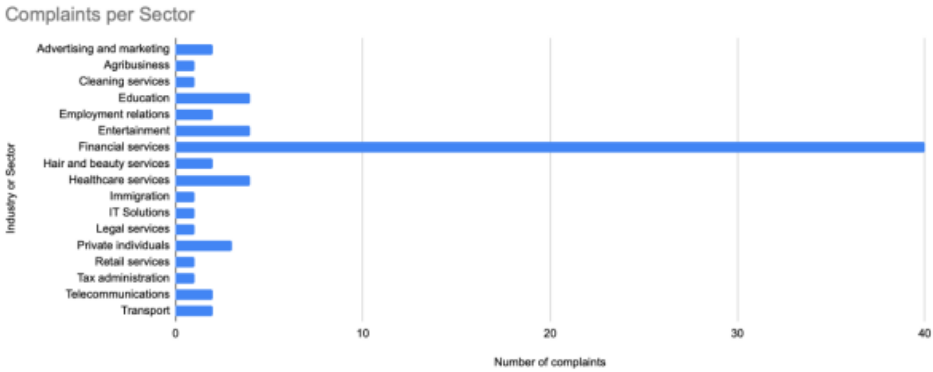
60. Despite a reporting requirement under the DPA, 2019, only one (1) Annual Report to the National Assembly is publicly accessible online. This report does not detail the ODPCs receipt of non-state funding. See: ODPC (2021) First Annual Report for the 2021/21 Financial Year.

61. ODPC (2024) ODPC Hosts Media Breakfast Meeting As Kenya Gears Up For NADPA AGM & Conference.

2.4.1 Financial Services Sector is Notorious for DPA violations

As of April 2024, the ODPC had received "5,315 complaints [and issued] 106 determinations, 60 enforcement notices, and 9 penalty notices."[62]

As part of the study, 72 out of the 106 determinations issued by the ODPC were analysed with the majority of the determinations pitting private individuals against private companies.[63]



62. *Some of these determinations involved consolidated complaints.*
63. *ODPC (2022) ODPC to Audit 40 Digital Lenders and Issues Enforcement Notice Against a Health Service Provider.*

As shown in the chart above, the financial sector, particularly digital credit providers, were the single-largest category of persons complained against by data subjects with 40 determinations made. Local and foreign digital credit providers (DCPs) have earned the reputation of being repeat violators of the provisions of the DPA.

In response to the 1,030 complaints received by September 2022, the ODPC instituted an audit of digital lenders in line with Section 23 of the DPA.[64]

The findings of this audit process have not yet been released for public consumption. However, a key interviewee observed that the audit is viewed by DCPs as an 'ongoing compliance process' that informed the ODPCs Guidance Note for DCPs.[65]

The next category was on sectors with 3-5 determinations which included education (private and public institutions), entertainment, healthcare services (private and public) and private individuals.[66] The sectors with the least number of determinations were agri-business, advertisement and marketing, cleaning services, hair and beauty services, IT solutions, legal services, immigration and resettlement, employment, taxation, and travel.

2.4.2 Failure to Obtain Consent Remains a Central Complaint

As shown in the table below, out of the 72 determinations sampled, more than 70% were complaints related to consent violations. Other complaints related to erasure, rectification and updating of personal data, requests for personal data, data relating to minors, and processing in the course of personal activities.

Table 1: Summary of Sampled Complaints

Nature of Complaints	Number
The unlawful or irregular collection of personal data without consent, insistent and unnecessary communications without consent.	19
The non-consensual publishing of a data subject's image for commercial purposes	14
The sharing of personal data with a third party without consent	12
The collection and processing of complainant's personal data without consent	12
The sending of promotional messages without consent	8
Failure to erase, rectify or update data subject's personal data	3
Request for personal data held by a data controller or processor	2
The unlawful disclosure of a minor's sensitive personal data (name and address)	1
Processing of personal data through use of CCTV (video & sound) in the course of personal / household activity	1
Total	**72**

64. ODPC (2023) Guidance Note for Digital Credit Providers.
65. ODPC. Determinations.
66. Section 2 of the DPA.

This illustrates that consent is one of the most frequently relied on legal bases for the processing of personal data but is also the most common reason for the violation of data subjects rights under the DPA.

Under the DPA, consent is defined as "any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject."[67]

This demonstrates that during the transition period (2019 - 2021), data handlers who had not implemented appropriate consent protocols in accordance with the DPA are increasingly facing the consequence of their non-compliance.

2.4.3 Consent and the Commercial Use of Data[68]

This case study explores the non-consensual publishing of data subject's publicly available images (including two minors) on social media for commercial purposes.

It raises various data protection issues relating to consent for personal data obtained indirectly for marketing purposes, transparency in data processing, and the need for data handlers to incorporate appropriate technical and organisational measures.

ODPC DETERMINATION 1973 OF 2023

On 6th January 2024, the ODPC found Bold Decisive Digital Lab (BDDL), a marketing agency, liable for using the images of Mercy Wambua and her two children, N.R and K.W, for commercial gain without her consent or knowledge, thereby violating her and her children's rights under the DPA. In her complaint, Ms. Wambua stated that she came across images of herself and her two children in a pamphlet bearing the logo of Equity Afia, the 2nd Respondent, at one of the 2nd Respondent's branches. Ms. Wambua noted that she has posted these images on her social media page.

BDDL claimed that the document was a proposal document presented during a private pitch to Equity Afia. BDDL further claimed that this document was not meant for public consumption nor intended to be used for marketing purposes.

In this instance, BDDL was ordered to compensate the complainants a sum totalling Kenya Shillings one million and nine hundred thousand (KShs. 1,900,000/=), computed as follows: 1st Complainant (KES 500,000), 2nd Complainant (KES 700,000), and 3rd Complainant (KES 700,000).

The key developments from this case study are that:

a) Consent is still required for collection of personal data whether directly or indirectly collected even where the information is in the public domain or social media.

b) Data handlers must obtain consent prior to the processing of a child's personal data from a person who has parental authority or by a guardian.[69]

67. *ODPC (2024) Determination No. 1973 of 2023.*
68. *Section 27 (a) of the DPA.*
69. *Section 30(a) and 32 of the DPA.*

c) Data handlers bear the burden of proving that consent was obtained from the data subject, including for personal data in the public domain.[70]

d) Organisations should prioritise transparent data collection practices, including for publicly available data, and put in place appropriate and consistent technical and organisational measures for the processing of personal data.

e)Specific damages must be pleaded in complaints for compensation to be awarded. Comparatively, the ODPC has declined to make orders for compensation where a complainant failed to pray for specific damages.

This brief highlights that before December 2023, the ODPC allowed certain data handlers to internalise the data protection by design/default principles as means of addressing complaints instead of granting compensation to complainants, even where these were pleaded.

2.4.4 Collection of Sensitive Personal Data

This case study explores the impact of biometric and emerging technologies used in the unlawful collection, processing, and cross-border transfer of personal and sensitive personal data.

It also highlights the use of economic incentives to obtain consent, underscored the need for an approved DPIA prior to the processing of personal data, and magnified the gaps in the ODPC enforcement mechanism.

DETERMINATION ON THE SUO MOTU INVESTIGATION BY THE ODPC ON THE OPERATIONS OF THE WORLDCOIN PROJECT IN KENYA BY TFH, THG, AND WH.[71]

The Worldcoin project by Tools for Humanity Corporation (THF), Tools for Humanity GmbH (THG) and Worldcoin Foundation (WF) (also, 'Worldcoin entities') has generated immense global interest.[71]
On or about the 21st of May 2021, TFH collected and processed personal data in Kenya for purposes of developing a machine learning algorithm to establish a "Proof of Personhood" protocol. In 2022, the ODPC contacted Worldcoin for additional information on the lawfulness of their activities in Kenya.

The ODPC and TFH exchanged various correspondence, including a review of a Data Protection Impact Assessment (DPIA) between 17 June 2022 and 15 July 2023. Certificates of registration as data controllers were issued to THG and THF on 15 September 2022 and 18 April 2023, respectively.

TFH continued collecting sensitive personal data until 30 May 2023, when the ODPC raised concerns on the processing of sensitive personal data by TFH and directed TFH to cease the processing of personal data.

TFH clarified the ODPC concerns and confirmed that they suspended the collection of facial and iris images from Kenyans for 14 days. TFH subsequently transferred controller responsibilities to Worldcoin Foundation.

In July 2023, the Worldcoin Token WLD (ECR-20) on Ethereum Mainnet was launched resulting in an upsurge in the Worldcoin

70. Out of these entities, only THC and THG were registered by the ODPC as data controllers. WF was unregistered.
71. ODPC (2023) Determination on the Suo Motu Investigation by the ODPC on the Operations of the Worldcoin Project in Kenya by TFH, THG, and WH.

Project activities in Kenya. In the same month, the ODPC issued a cautionary statement to the public on disclosing any personal or sensitive data.

In August 2023, the ODPC directed TFH to immediately cease the collection and processing of personal data, ensure the safe restriction of further processing of the collected data, and securely store all collected data. On 2 August 2023, the Ministry of Interior and National Administration suspended the operation of the Worldcoin project in Kenya.

Subsequently, a multi-agency committee was formed and it took the following remedial actions:

1. Ordering TFH to cease its operations in Kenya for 12-months, until TFH, inter alia

a). Grants the multi agency team access to its systems for purposes of conducting a Security Systems Audit,

b. Conducts a DPIA for phase 2 of its data collection activities.

The ODPC also took a number of remedial action including:

2. Issuing a cease-and-desist notice to TFH to cease its operations in Kenya, which was ignored;
3. Conducting an investigation on the ODPCs own initiative into the project in October 2023,[72]
4. Cancelling registration certificates for TFH and THG,
5. Applied to the High Court of Kenya seeking preservation order of the personal and traffic data handled by TFH

The key developments from this case study are that:

a) Economic incentives given to data subjects in exchange for their consent to data processing activities undermines the validity of consent.

b) Prior consent is a prerequisite for data transfers outside of Kenya.[74]

c) Data controllers cannot transfer their DPA responsibilities to third parties.

d) Data handlers are mandated to conduct DPIA prior to the processing or transfer of sensitive personal data.

e) The enforcement of the cross-border data transfer provisions in the DPA remains a key challenge to the ODPC and the Cabinet Secretary, and regulatory vigilance by the ODPC on the data processing operations of foreign entities is critical.

f) The ODPC has an extensive mandate in oversight and enforcement of the DPA and thus it should neither see nor constrain itself to the role of a registration-only entity.[74]

72. Section 9 (1) (a) of the DPA, 2019 and Regulation 14 (Complaints Handling Procedure and Enforcement) Regulations, 2021.
73. One Trust Data Guidance (2023) Kenya: ODPC finds Worldcoin, Tools For Humanity Corporation and Tools For Humanity GmbH liable for data protection violations.
74. Key informant interview (Anon), 30 April 2024.

2.4.5 Emphasis on Data Subjects' Rights

The case studies below reinforce the protection and promotion of data subjects' rights under Section 26 of the DPA. Specifically, the ODPC has issued positive determinations relating to the right to correction of false or misleading data, the right to deletion of false or misleading data, and the right of data subjects to access their personal data in the custody of a data controller or data processor.

In the following cases, the ODPC arrived at a violation finding but applied different enforcement penalties to each, demonstrating that admitted complaints will be dealt with on a case-by-case basis.

Further, each case highlights the need for organisations to fully internalise the data protection by design/default provisions in the DPA by implementing appropriate technical and organisational measures.

ODPC DETERMINATION NO. 0796 OF 2023

In August 2023, the ODPC dealt with a complaint relating to unnecessary communications from a data handler resulting from inaccurate records.[75] The complainant, Teresiah Karungari alleged that Branch Microfinance Bank had infringed her rights under the DPA after the bank spammed her email with messages claiming that she had not cleared payment on a century microfinance loan.

Teresia noted that the Respondent sent her three messages daily for several months. Further, the complainant noted that she had cleared her payment in 2022, but her name was still included on the list of default borrowers resulting in the unintended communication.

In this instance, the Bank took steps to rectify the complainant's loan information and further ceased all communication to the complainant. Additionally, the Bank reinforced their review and quality assurance procedures by conducting a comprehensive review of their borrower records, addressing inaccuracies and discrepancies, and ensuring that information is both accurate and appropriate. Lastly, the Bank committed to limit their data collection to what is strictly necessary to provide the required services and comply with regulatory requirements. Consequently, the ODPC closed the complaint without any finding of a violation.

75. *Key informant interview (Anon), 30 April 2024.*

The determination above demonstrates a lenient approach by the ODPC with respect to some data handlers that take steps to redress rights infringements under the DPA through the strengthening of technical and organisational safeguards.

However, it also magnifies the inconsistency of the ODPCs approach towards dispute resolution where similar violations are alleged by complainants.

ODPC DETERMINATION NO. 0781 OF 2023

In May 2023, the ODPC dealt with a complaint relating to a data handler's failure/neglect to update the complainant's records, infringing on their right to correct false/misleading data.[76] The complainant, Koros Kiprotich, complained that the respondent, the Higher Education Loans Board (HELB), had listed the complainant as being in default despite them clearing their HELB loan.

The complainant noted that they had been in default of their loan but later cleared this. As a result of HELB's failure to update his records and making reference to a default history, third parties continued to make reference to this inaccurate default history, which negatively impacted him. In arriving at a violation finding of Section 26 of the DPA, the ODPC held that the respondent failed to adhere to the principle of accuracy by failing to update the complainant's personal data and, where necessary, rectify or erase inaccurate data.[77]

The ODPC directed the HELB to rectify and/or update its records to ensure the complainant's personal data shared with third parties is accurate within seven (7) days. HELB noted that they were taking remedial measures by engaging relevant third parties with whom they share personal data to integrate HELB's systems through APIs for seamless updates.

The determination above clearly outlines the burden placed on data controllers to provide accurate data to reliant third parties.

76. ODPC (2023) Teresiah Karungari v Branch Microfinance Bank.
77. ODPC (2023) Jeremy Obano v Kenya Airways PLC.

ODPC DETERMINATION NO. 1775 OF 2023

In December 2023, the ODPC dealt with a complaint relating to a data handler's failure to adhere to a data subjects' request for access to personal data held by a data handler, infringing on his right to access his personal data.[78]

The complainant, Jeremy Obano, complained that the respondent, the Kenya Airways PLC (KQ), had failed to provide a copy of a telephone conversation recording between himself and a customer care agent where he sought provision of a wheelchair for his mother ahead of their planned travel. Mr. Obano noted that KQ's failure to provide him with the recording resulted in inconvenience suffered by his mother and himself, contrary to health, safety and disability laws.

The ODPC arrived at a violation finding of Section 26 (b) of the DPA as read together with Regulation 9 (1) of the General Regulations, 2021, and issued a compensation order of Kenya Shillings Two Hundred and Fifty Thousand (KShs. 250, 000/=). Further, the ODPC held that the KQ could not refuse to provide the complainant access to his personal data on grounds that granting access would infringe on the customer service agent's own personal data.

This ruling emphasises data handlers' obligation to facilitate data subject access requests, regardless of potential challenges related to other individuals' personal data. In this regard, data handlers should implement appropriate technical and organisational measures to anonymise and conceal the personal data of their staff, to be able to give effect to data subjects' right to access.

78. *ODPC (2024) ODPC Launches AI Chatbot as Kenya Marks Data Privacy Day 2024.*

3.0 Challenges and Opportunities in Data Protection Implementation

This section highlights key challenges and opportunities in data protection implementation. This is canvassed through a SWOT analysis and a brief discussion on observed implementation opportunities, as informed by key respondents drawn from KICTANet members' informative feedback.

3.1 SWOT of ODPC/Data Protection in Kenya

OPPORTUNITIES	WEAKNESSES
1. Strong collaboration and partnerships with various stakeholders on privacy and data protection. 2. Sectoral focus on private data handlers' with large jurisdictional/population scope (education, health, telecommunications, and finance). 3. Functional online portals facilitating access to information, registration and complaints, and awareness raising. 4. Introduction of voluntary data dispute mechanism (ADR) to reduce adversarial administration action/litigation. 5. Decentralisation of data protection (public awareness campaigns, establishment of regional offices). 6. Continued integration of eme rging technologies in service delivery (e.g., online complaints and registration, and AI-powered chatbot, LindaData).[79]	1. Ongoing delay by the ODPC/ICT Cabinet Secretary to fully actualise the DPA.[80] 2. Constrained ODPC independence. 3. Lax enforcement against state entities' data collection and processing operations. 4. Lack of national data protection certification standards, resulting in reliance on international accreditation (e.g., IAPP). 5. Non-holistic national data governance framework resulting in data governance gaps (e.g., lack of data classification guidelines).

79. Issues noted include the failure to establish an adequacy framework; the delayed publication of guidelines on the commercial use of data, guidelines on the localised processing of data; the failure to publish a data-sharing code for the exchange of personal data between government departments/public sector, certification codes/mechanisms).
80. KICTANet (2023) How to Engage With Data Protection Authorities as an SME.

STRENGTHS	THREATS
1. Strong multi-stakeholder goodwill, interest and collaboration to support ODPC to promote privacy and data protection. 2. Strength of DPA and ODPC can be used to obtain equivalency status with other jurisdictions and generate economic benefits for the country. 3. Directed focus on state entities to shatter perception of data ownership vesting in the state rather than data subjects. 4. Promotion of transparency in regulatory activities through publication of additional registers (updated register of noncompliance; an updated register of complaints; a data protection risk register). 5. Collaboration with other regulatory, licensing and ministerial entities to support holistic data governance (e.g., introduction of data protection registration as a licensing prerequisite for financial entities with the Central Bank of Kenya). 6.Active participation in the development of the AI Strategy to ensure infusion of data protection considerations. 7.Sustained development of internal and external stakeholder capacities and capabilities (e.g., dissemination of privacy and data protection resources, staff expansion). 8. Directed compliance support to registrable SMEs.[81] 9. Stricter adherence by ODPC to <90 day complaints resolution window (Section 56(5), DPA).[82]	1. Broad claw-back clauses in the DPA (e.g., national security, public interest). 2. Poor self-reporting of data breaches by data collection and processing entities. 3. Steep rise in cyberattacks with increased risks for automated databases containing personal/sensitive personal data. 4. ICT Ministry consideration of Cross Border Privacy Rules threatening digital sovereignty and domestic position on cross-border data transfers 5. Foreign pressure to alter provisions of the data protection legal framework (e.g., renewed calls by the World Bank to water down localisation requirements). 6. Growing use of unregulated emerging technologies (e.g., AI, digital assets). 7.Inadequate staffing and technical capacity at data handlers' level. 8.Conflation of data protection and privacy, with limited focus on other privacy values. 9.Low public awareness. 10. Differentiated protection of sexual orientation and gender identity rights.

81. Gichuhi & 2 others v Data Protection Commissioner; Mathenge & another (Interested Parties) (Judicial Review E028 of 2023) [2023] KEHC 17321 (KLR) (Judicial Review) (12 May 2023) (Judgement). See also: Paul Ogendi (2023) The effect of the 90-day period for deciding on complaints submitted to the Office of the Data Protection Commissioner in Kenya.
82. A key informant noted that the ODPC is in the process of operationalizing cross-border mechanisms. This is pending. See: Key informant interview (Anon), 03 May 2024.

10. Development of additional guidelines/ frameworks (e.g., user guide outlining integration of fairness and justice in complaints mechanism, guidelines on data localisation to support digital sovereignty efforts). Provision of legal clarity on meta consent.	11. Unregulated secondary use of data. Lack of regulatory clarity regarding the data protection roles/responsibilities of the ODPC and the Commission on Administrative Justice.

3.2 Opportunities in DPA Implementation

The implementation of the DPA presents several opportunities for stakeholders in Kenya, by positioning Kenya as a responsible and sustainable digital ecosystem that prioritises privacy, security, and trust. This section highlights eight core opportunities for varied stakeholders.

3.2.1 Adequacy Framework and Cross-Border Data Transfers

Given growing data demands for international trade and cooperation and noting the international remit of data protection, it is imperative for the ODPC to establish Kenya as a secure country with a suitable level of data protection to be able to obtain adequacy decisions with international

and regional countries. Further, the ODPC is encouraged to develop a national adequacy framework and proactively seek equivalency status with other jurisdictions to facilitate cross-border data transfers and align with the domestic agenda on global trade and e-commerce.[83]

This alignment with best practices is critical for enhancing Kenya's reputation as a reliable and trustworthy destination for digital trade and data-driven businesses and will demonstrate Kenya's commitment to upholding high standards of data protection, data privacy and data security, thereby attracting foreign investment and partnerships.

3.2.2 Integrate and Monitor Impact of Emerging Technologies

Emerging technologies such as Artificial Intelligence bring new challenges to data protection, as they require large amounts of data, and can bring tremendous economic and social value to those who utilise that data to develop solutions.

Thus there is pressure for making data available, but also pressure for domestic entities to capture the value from that data. These pressures can further test DPA implementation, and specifically test registered data handlers' ongoing compliance. One key informant recommended the use of

AI to support audit and compliance processes through the integration of AI tools into data handlers systems/processes. However, this recommendation raises legal challenges that need to be explored prior to the finalisation of Kenya's AI Strategy.

The ODPC and ADPAs, are encouraged to adopt a proactive rather than a reactive approach to emerging data protection issues. Some respondents called on the ODPC and ADPAs to build their internal capacity to understand and respond to the potential opportunities, risks, and impact of other key emerging technologies with an impact on data protection. These include blockchain, the Internet of Things (IoTs), digital asset management, robotics, fintech, cloud computing, virtual reality, big data analytics, genomics and biometric technologies, amongst others.

3.2.3 Promoting Cross-Border Collaboration

The ODPC and ADPAs, are encouraged to address cross-jurisdictional data protection challenges in collaboration with regional and international DPAs. Some respondents urged ADPAs to identify actionable areas of collaboration on emerging areas such as the regulation of personal data, cross-border data transfers, and technological advancements such as AI, blockchain, and the Internet of Things.[84]

By sharing best practices, resources, and expertise along with establishing Equivalency or Adequacy statuses and related mechanisms for cooperation, DPAs can enhance their capacity to address these complex challenges and protect the privacy rights of individuals across jurisdictions whilst maintaining digital sovereignty.

83. ODPC. Conference Theme.
84. Boniface Abudho & Stephen Beard (2023) Africa's Data Centre Boom.

3.2.4 Promoting Innovation and Investment in Data Protection Technologies and Services

The implementation of the DPA presents a fantastic opportunity for innovation and investment in data protection technologies and services by technology companies.

As organisations entrench their compliance with the requirements of the DPA, there is a growing demand for solutions such as data encryption, anonymization techniques, and data breach detection tools.

This presents an opportunity for technology companies to develop and offer innovative solutions to address these needs, stimulating growth and job creation in the digital sector. In the same breath, Kenya's migration of IT infrastructure onto the cloud by public and private entities is catalysing Kenya's growth of the data centre industry, leveraging renewable power.[85]

Boniface Abudho & Stephen Beard (2023) Africa's Data Centre Boom.] While this migration is still in its nascent stages, this presents a novel opportunity for the development of robust data protection infrastructure and services.

The ODPC is encouraged to proactively engage data centre entities to invest in secure and compliant data storage solutions by building data protection by design and default into their products and services prior to deployment.

3.2.5 Data Protection as an Intersectional Gateway Requiring Multistakeholder Collaboration

Some respondents noted that the protection of personal data goes hand in hand with efforts to bridge technology gaps to ensure that individuals have meaningful, safe, and secure access to digital products and services.

Given the cross-cutting scope of data protection, the continuing implementation of the DPA presents an opportunity for interentity collaboration at the state level and the prioritisation of collaborative awareness raising on intersectional issues, such as cybersecurity.

DIGITALISATION TRENDS IMPACTING DATA PROTECTION

The COVID-19 pandemic spurred the rapid adoption of ICTs and increased digitalisation efforts across various sectors. Illustratively, Kenya's mobile (SIM) penetration rate stood at 130.5 percent against a population of 56,203,030.[86]

Communication Authority of Kenya (2023) Third Quarter Sector Statistics Report for the Financial Year 2022/2023 (1st January – 31st March 2023); Macrotrends (2024) Kenya Population 1950-2024.] Mobile data subscriptions stood at 51 million and the number of smartphone devices was recorded as 33.6 million.[87]

As of February 2024, the Central Bank of Kenya reported 77.33 million mobile money

85. Communication Authority of Kenya (2023) Third Quarter Sector Statistics Report for the Financial Year 2022/2023 (1st January – 31st March 2023); Macrotrends (2024) Kenya Population 1950-2024.
86. Ibid.
87. Central Bank of Kenya, Mobile Payments.

accounts transacting a total of KES 790.8 billion[88] and Safaricom's M-Pesa's 30 million active monthly users made 21.6 billion transactions valued at KES 35.86 trillion in 2022.[89]

To leverage these ICT dividends, the government has prioritised service delivery through its digital platform, eCitizen and introduced a biometric digital identity (Maisha Namba) for all citizens.[90]

These developments have progressively heightened cyber risks and data breaches. In the period between September and December 2023, the total cyber threats detected increased by 943% from 123.9 million to 1.29 billion, of which 98.2% comprised system vulnerabilities.[91]

Other threats noted included mobile application attacks, malware, brute force attacks (DDOS/Botnets) and web application attacks.

The Worldcoin saga cemented the pressing need for the ODPC and other sector regulators and licensing entities to collaborate in scrutinising the deployment of emerging technologies given their impact on sensitive personal data.

To this end, respondents recommended heightened inter-entity collaboration between the ODPC with critical regulators/ ministries at the domestic level for purposes of shattering "siloed conversations between state entities.[92]

A few critical entities highlighted included:

- The National Computer and Cybercrimes Coordination Committee (NC4), where an ODPC representative sits as a member, to address growing cybersecurity threats.
- Relevant licensing authorities, such as the Central Bank of Kenya, Communications Authority, and relevant agencies within the Office of the Attorney General, Ministry of Health and Trade, to integrate data protection registration as a prerequisite for licensing for non-state entities.
- Trade and taxation entities, such as the Ministry of Trade, Investments and Industry and the Kenya Revenue Authority to ensure that data protection considerations are internalised into trade discussions, both regionally and internationally, and at the local tax level, noting the powers wielded by tax authorities.

3.2.6 Strict Enforcement of Unregulated Data Handlers

Respondents queried the ODPC's capacity to effectively regulate both state entities and technology giants, such as social media platforms, which process large data sets but remain largely unregulated.

Two areas where implementation/ enforcement gaps were observed relates

88. Safaricom PLC (2024) Annual Report and Financial Statements.
89. KICANet (2023) Understanding Maisha Namba, Kenya's New Identity System.
90. Communications Authority of Kenya (2023) Sector Statistics Report September - December 2023 91. Key informant interview (Anon), 03 May 2024.
91. Communications Authority of Kenya (2023) Sector Statistics Report September - December 2023
92. Kaplan and Stratton (2024) Emerging Development and Challenges in Complying with the Data Protection Act.

to social media and data mining/scraping companies, which operate across borders, making it challenging to enforce data protection regulations effectively.

3.2.7 Internalisation of Data Protection by Design/Default by Data Handlers

Data handlers are reminded about the need to "rethink and perhaps even redesign their processes, products and services in order to factor in data protection principles throughout the lifecycle of their operations."[93]

One interviewee emphasised their proactive approach, which includes the regular conducting of compliance audits and risk assessments on their data processing activities to ensure compliance with ODPC determinations, evolving case law, guidelines, and other relevant factors.[94]

3.2.8 Legislative Clarity to Address Overlapping Mandates

Prior to enactment of the DPA, there were several laws and institutions implementing various sectoral functions relating to privacy and data protection. For example, some respondents observed that the Commission on Administrative Justice (CAJ) was Kenya's first data protection authority under the Access to Information Act, 2016 (ATI Act, 2016).

This is attributed to the data protection powers, roles and responsibilities, specifically targeting public entities and regulatory bodies, possessed by the CAJ.[95]

The CAJ's data protection functions include: 'assessing and evaluate the protection of personal data processed and stored by public entities; engaging the public on the right to the protection of personal data; ensuring public entities' and regulatory bodies' compliance with data protection measures; monitoring state compliance with international treaty obligations relating to the protection of personal data, and promoting the protection of data.'

Other relevant institutions with functions relating to privacy and data protection include the Central Bank of Kenya, the Communications Authority, the ICT Authority, Insurance Regulatory Authority, Kenya National Commission on Human Rights, amongst others.

Noting that privacy and data protection is a cross-cutting issue, it is imperative for Parliament to address potential mandate overlaps. In the interim, ODPC should consider entering into a working regulatory arrangement with other agencies or regulators that have a role that affects or complements their mandate.

93. Key informant interview (Anon), 02 May 2024.
94. Key informant interview (Anon), 02 May 2024.
95. The CAJ's data protection functions include: 'assessing and evaluate the protection of personal data processed and stored by public entities; engaging the public on the right to the protection of personal data; ensuring public entities' and regulatory bodies' compliance with data protection measures; monitoring state compliance with international treaty obligations relating to the protection of personal data, and promoting the protection of data.

4.0 Conclusion and Key Considerations for the Future

In the five years since the enactment of the DPA, the protection of personal data has transitioned from a peripheral concern to occupying legal and normative primacy, with significant progress being made towards implementing and enforcing its provisions.

Particularly noteworthy are the commendable efforts of the ODPC to bolster its internal implementation and enforcement mechanisms, heighten awareness among stakeholders, and fortify its ability to implement and uphold the DPA. These efforts stand out as key drivers of Kenya's notable progress in this domain.

However, looking back, stakeholders noted the existence of key implementation and enforcement gaps and issues in Kenya's data protection environment that require urgent redress. A few key issues noted in this brief include:

1 **Independence:** The ODPCs independence remains a key issue, with Parliament's recommendation for a Board to oversee the daily operations of the ODPC remaining a contested solution.

2 **Gaps in Enforcement against State Entities and Technology Giants:** The ODPC's capacity to effectively regulate both state entities and large technology giants, such as social media platforms, has not yet been fully tested. This is attributed to an ongoing delay by the ODPC/ICT Cabinet Secretary to fully actualise the DPA, 2019.

3 **Low Registration Levels of Data Handlers:** At least 90% of potentially registrable business or corporate entities remain unregistered.

4.Foreign Pressure: Kenya's ICT Ministry and the ODPC are facing immense pressure to adopt rules (e.g., CBPR) and water down localisation provisions with an impact on the nation's digital sovereignty and the domestic position on cross-border data transfers.

5 **Unregulated emerging technologies:** entities are deploying and harnessing emerging and automated technologies, such as AI, to process personal data without effective intervention from the ODPC.

It is against this background that this policy brief makes critical recommendations to data protection stakeholders, including the ODPC, Parliament, the ICT Cabinet Secretary to:

6 **Strengthen the independence of the ODPC:** this can be by amending the DPA to make the ODPC autonomous and separate it from the ICT Ministry, and increase the ODPCs budgetary allocation to enable it to effectively discharge its mandate across the country.

7 **Adopt Proactive and Collaborative Approach to Emerging Technologies and Key Data Protection Threats:** the ODPC is reminded about the need to be alive to emerging tech and to build its internal capacity to understand and respond to the potential risks and impact of emerging technologies, with calls for collaborative inter-agency efforts geared towards risk mitigation from existing and emerging technologies.

8 **Regulation of Unregulated Data Handlers:** the ODPC is urged to intensify its efforts to regulate the data processing operations of all data handlers, especially state entities, Big Tech, and the financial sector.

The policy brief also makes critical recommendations to ADPAs and African governments, given the need to collaboratively secure an effective regional data protection environment in Africa, which include:

1 **Prioritise Transparency in Regulatory Activities:** ADPAs are reminded about the need to promote transparency in their regulatory activities, given the mutually-reinforcing relationship between data protection, access to information, transparency, and open data and the need to maintain trust in data ecosystems.

2 **Prioritise Critical Issues at the Domestic Level:** ADPAs are encouraged to prioritise critical issues within their jurisdiction to ensure a strategic, consistent, responsive, and tailored response to data protection concerns. Governments are encouraged to provide ADPAs with the requisite resources to effectively exercise their mandate.

KICTANet
The Power of Communities

About KICTANet

The Kenya ICT Action Network (KICTANet) is a multi-stakeholder think tank for ICT policy and regulation whose guiding philosophy encourages synergies for ICT policy-related activities and initiatives. The network provides mechanisms and a framework for continuing cooperation and collaboration in ICT matters among industry, technical community, academia, media, development partners, and Government.

KICTANet
The Power of Communities

KICTANet.or.ke | Twitter | LinkedIn | Facebook | Instagram | Youtube | TikTok

KICTANet: Transformed communities through the power of ICTs