

5 Years On:

Citizens' Perspectives on Kenya's Data Protection Act Implementation

OCTOBER 2025



KENYA

**AMNESTY
INTERNATIONAL**



Table of Contents

Acknowledgements	3
County Summaries	4
Mombasa	5
Nairobi	5
Nakuru	5
Tana River	5
Turkana	5
Kisumu	6
Kilifi	6
Taita Taveta	6
Meru	6
Wajir	6
Executive Summary	7
Introduction	9
Jurisprudence on Data Protection in Kenya	12
Methodology	14
Public Awareness of the DPA	15
Personal Data Protection Experiences	17
Awareness of the ODPC	22
Conclusion	24
Recommendations on Effective DPA Implementation	24

Acknowledgements

Amnesty International Kenya is part of Amnesty International's global movement, comprising over 10 million members and supporters, dedicated to creating a future where human rights are enjoyed. United by our shared humanity, we know that the power to create positive change is within all of us.

Amnesty International Kenya extends gratitude to all those who contributed to the successful completion of this perception study report. We are indebted to our dedicated research and writing team, whose expertise and commitment made this evaluation possible. We acknowledge the exceptional efforts of our staff, Victor Ndede, Benta Moige, Joel Maina, Aurelia Miheso, and Sharlene Muthuri, for their meticulous work in data collection, analysis, and synthesis, which was invaluable.

Amnesty International Kenya also extends gratitude to the participants of the focus group discussions (FGDs) and key informants from across Kenya for their candid feedback, thoughtful contributions, and willingness to share their experiences and perspectives that have significantly enhanced the quality of our report.

Except where otherwise noted, all original content in this document is licensed under a Creative Commons license. All users must attribute the contents of this document in the manner specified and do not suggest that we endorse your use of the work. You are free to share this work on a non-commercial basis. <http://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

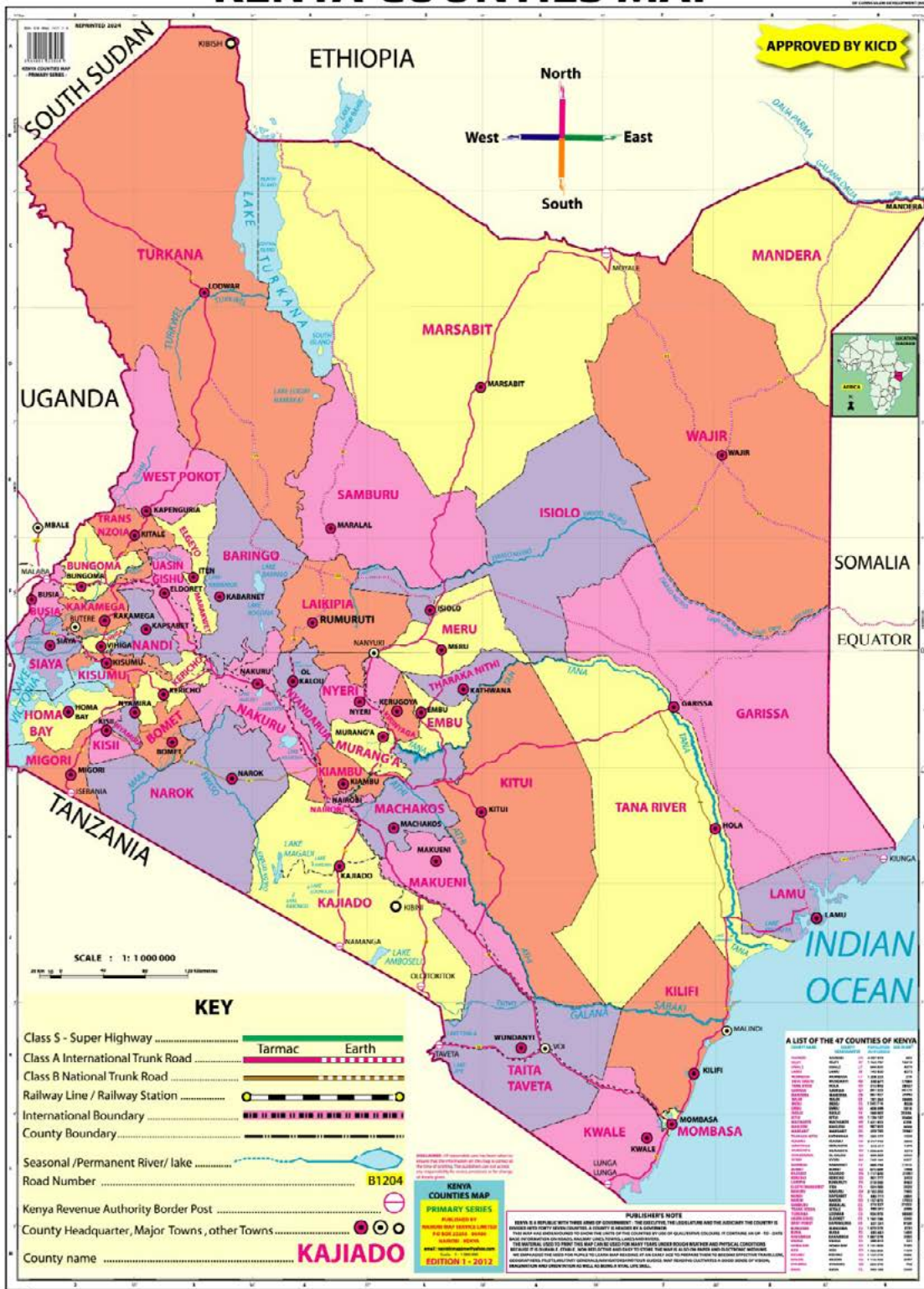
Where material is attributed to a copyright owner other than Amnesty International Kenya this material is not subject to the Creative Commons licence.

First Published September 2025
197 Lenana Road, Lenana Road
P.O. Box 1527-00606 Nairobi, Kenya
Tel: +254 020 – 4283000
Email: amnestykenya@amnesty.org



County Summaries

KENYA COUNTIES MAP



Mombasa

Mombasa County, covering an area of 229.9 Km², is the home of the second-largest city in Kenya and borders Kilifi County to the North, Kwale County to the Southwest and the Indian Ocean to the East. The city serves as the headquarters of Mombasa County.

The county has a population of 1,208,333 people, with the entire population considered an urban population given the size of the county and the population density. 86.3% of the population in Mombasa County has access to electricity. 61.8% of the population own mobile phones, with 29.2% accessing the internet in Mombasa County. The Likoni and Jomvu constituencies have the lowest internet access rates at 19.4% and 23.1%, respectively.

Nairobi

Nairobi is the capital and largest city of Kenya. The city and its surrounding area constitute the Nairobi City County, earmarked as the 47th County in Kenya. The County has a total area of 696.1 Km² and borders Kiambu County to the North and West, Kajiado to the South and Machakos to the East.

The County has a population of 4,397,073 people with the entire population considered an urban population given the size of the county and the population density. 96.7% of Nairobi households have access to electricity. 69.1% of the population in Nairobi own mobile phones with 43% of the population accessing the internet. Mathare constituency and Embakasi record the least populations accessing the internet at 24.8% and 27.7% respectively.

Nakuru

Nakuru County lies within the central parts of Kenya's Great Rift Valley and covers an area of approximately 7,504.9 Km². Nakuru County Borders eight Counties, namely, Laikipia to the North-East, Kericho to the West, Narok to the

South-West, Kajiado and Kiambu to the South-East, Baringo to the North, Nyandarua to the East and Bomet to the West.

Nakuru County has a population of 2,162,202 people with 51.5% of the population classified as rural. 64.3% of Nakuru households have access to electricity. Additionally, 52.7% of the population in Nakuru own mobile phones with 21.4% of the population accessing the internet in the county. Kuresoi North and Kuresoi South have the least populations accessing the internet at 5.6% and 6.5% of the population respectively.

Tana River

Tana River County with a total area of 39,190.6 Km² is one of the six Counties in the Coast region of Kenya. It borders Kitui County to the West, Garissa County to the North East, Isiolo County to the North, Lamu County to the South East and Kilifi County to the South.

The county has a population of 315,943 people with 76.4% (240,221) of the population classified as rural populations. Only 26.1% of the population in Tana River have access to electricity. Mobile phone ownership is low in Tana River with only 31.6% of the population owning mobile phones. Population accessing the internet is also significantly low at 6% of the entire population with Bura and Garsen constituencies reporting 4.1% and 6.0% respectively.

Turkana

Turkana is the largest county (71,597.6 Km²) in Kenya located in the Northwest of Kenya with its headquarters situated at Lodwar Town. It borders Uganda to the west, South Sudan and Ethiopia to the North and Northeast respectively. Internally, it borders West Pokot and Baringo Counties to the South, Samburu County to the Southeast, and Marsabit County to the East.

The county has a population of 926,976 people with 84.8% (786,185) of the population



classified as rural populations. Only 8.8% of the households has access to electricity, with at least 3 constituencies (Loima, Turkana East and Turkana North) having less than 2% of their households accessing electricity. Only 16% of the population owns mobile phones, with only 4.8% of the population accessing the internet. Again, 3 constituencies (Loima, Turkana East and Turkana North) have less than 2% of their populations accessing the internet.

Kisumu

Kisumu County is in western Kenya, on the shores of Lake Victoria. Kisumu County covers approximately 567 km² on water and 2086 km² land area, representing 0.36% of Kenya's total land area. It hosts the third largest city in Kenya which serves as the County's headquarters. The County is bordered by Homa Bay County to the South, Nandi County to the Northeast, Kericho County to the East, Vihiga County to the Northwest, Siaya County to the West and surrounded by the second largest freshwater lake in the World; Lake Victoria.

The county has a population of about 1,155,574 people with a population of 714,668 (61.94%) classified as rural population in Kisumu County. 52.8% of households in Kisumu County have access to electricity. 49.4% of the population owns mobile phones with 20% of the population accessing the internet. Seme and Muhoroni Constituencies have internet access recorded at 7.1% and 9.9% of the population respectively.

Kilifi

Kilifi County in the coastal part of Kenya and covers an area of 12,609.7 Km². It borders Kwale County to the Southwest, Taita Taveta County to the West, Tana River County to the North, the Indian Ocean to the East and Mombasa County to the South. The county has a population of 1,453,787 with a population of 1,059,899 (73.04%) classified as rural population in the county.

38.6% of households in the county have access to electricity. The county has a population of 39.4 owning mobile phones with 12.1% of the population having access to the internet. Constituencies like Ganze and Magarini have internet access recorded as 4.2% and 5.3% of the population respectively.

Taita Taveta

Taita Taveta is situated in the coastal region and has a population of about 340,671 residents. The county headquarters are in Mwatate. Taita Taveta is located within two national parks, namely Tsavo East and Tsavo West. Due to its geographical position, numerous human-wildlife conflicts have been reported in the county. Approximately 48% of its residents have access to electricity, while 54% own mobile phones, which may or may not be smartphones. As of 2019, only 16% of the population has internet access. Around 32% of its residents live below the poverty line.

Meru

Meru County is situated in the former Eastern Province of Kenya, with a population of 987,653 according to the 2019 census. Meru has its headquarters in Meru Town, which is one of the largest urban areas in Kenya. 4.6% of residents have access to electricity in Meru County. 50.3% of the population has access to mobile phones, but only 10.5% have access to electricity.

Wajir

Wajir is one of the counties in Northeastern Kenya and is among the largest counties in Kenya. Wajir has a population of 781,263, with 62.2% living below the poverty line. Only 14.6% of its residents have access to electricity, and just 2% have access to roads. While 27.9% of inhabitants own phones, only 3.9% have internet access.

Executive Summary

This report by Amnesty International Kenya assesses the awareness and implementation of the Data Protection Act (DPA) by evaluating public understanding of privacy rights and the Act's effectiveness. The study, conducted through Focus Group Discussions (FGDs) and Key Informant Interviews in 10 Kenyan counties including Nairobi, Kisumu, Taita Taveta, Mombasa, Turkana, Wajir, Tana River, Nakuru, Meru, and Kilifi found that while the DPA provides a robust legal framework, its practical impact is limited. Specifically, its effectiveness is constrained by low public awareness, a lack of inclusivity, limited regional presence of the regulatory body, and inconsistent enforcement. The findings highlight the critical need for strategic investments in public education, inclusive advocacy, regional institutional development, and proactive enforcement to build a stronger data protection culture in Kenya.

Findings on Public Awareness and Experiences

Awareness of the DPA and Privacy Rights

The research found that awareness of the DPA is moderate. Urban areas such as Nairobi, Kilifi, Nakuru, and Kisumu show a high level of comprehensive understanding of the act and its provisions. In contrast, rural counties show a low understanding, with most residents having heard of the Act but not explicitly understanding its provisions. Nairobi exhibited the highest levels of awareness, with all participants having heard about or engaged with the Act's provisions. Participants learned about the DPA through social media, mainstream media, and, most commonly, through training or activities with Civil Society Organizations (CSOs). Participants demonstrated an admirable understanding of data processing principles and the importance of consent, highly valuing the right to be informed, the right to rectification, and the right to access personal data. While they showed high awareness of what constitutes personal

data, few participants could clearly distinguish between personal and sensitive personal data.

Experiences with Data Breaches and Enforcement

Many participants were hesitant to share personal data, with some admitting they would provide false information, citing a distrust stemming from recent incidents where social media platforms collected and used data without consent. Alarming, some reported that sensitive health information had been disclosed to third parties without their knowledge or permission. While participants exhibited high knowledge of data breaches, defining them as the use of data without consent or for unintended purposes, the majority did not pursue any remedy after experiencing a breach. This was due to a lack of awareness about available legal recourse and a belief that any action would be slow or ineffective, with no consequences for violators. Notably, not one participant reported a breach to the Office of the Data Protection Commissioner (ODPC), underscoring its limited awareness of ODPC as a recourse mechanism. Participants were largely unfamiliar with the ODPC's functions, powers, and reporting mechanisms, which significantly hindered their ability to take appropriate action. Furthermore, exercising the guaranteed rights to access, rectify, or erase personal data remains a challenge, particularly in marginalized and rural areas, due to a lack of awareness, limited capacity to exercise these rights, and weak enforcement mechanisms.

Challenges and Recommendations

Challenges

The findings highlight that awareness and understanding of the DPA remain relatively low, particularly in marginalized counties. Many citizens lack the knowledge and capacity to fully understand their data rights or provide informed consent, leaving them vulnerable to the misuse of their personal information. Furthermore, vulnerable and marginalized groups, including youth, persons with disabilities and low-literacy communities, continue to be excluded from discussions and implementation efforts. Another major challenge is the ODPC's limited regional presence. With limited regional offices and grassroots outreach, the ODPC remains largely inaccessible to many citizens, limiting the DPA's effectiveness in practice. Finally, a perceived lack of consistent enforcement undermines confidence in the DPA. The ODPC's capacity is constrained by limited funding, staffing shortages, and restricted institutional independence, particularly when addressing large-scale violations.

Recommendations

Amnesty International Kenya recommends a multi-pronged approach for effective DPA implementation, beginning with Community Engagement and Education through civic and digital literacy campaigns, utilizing local media, chief's barazas, and social media. Secondly, there must be Intentional Inclusion and Participation of Vulnerable Groups to ensure they benefit from the Act's provisions. Thirdly, the ODPC needs to improve its Institutional Presence & Capacity by deploying officers within police stations to train officers and handle inquiries, and endeavoring to establish

offices in all counties where feasible. Fourthly, the ODPC must enhance its Enforcement and Accountability powers to proactively investigate and make decisions regarding data breaches, especially those involving big Telecom Companies and monopolies, to build public trust and deter violations. Finally, the report calls for Multi-Sectoral Collaboration with stakeholders across government, the private sector, CSOs, and media, and the inclusion of basic data protection concepts within the education curriculum at all levels.

Introduction

The right to privacy is a fundamental human right enshrined in international laws reflecting its universal recognition and significance. Internationally, it is provided under Article 12 of the Universal Declaration of Human Rights and reaffirmed in Article 17 of the International Covenant on Civil and Political Rights, which prohibits arbitrary interference with one's privacy, family, home, or correspondence. This right obligates state parties to respect and ensure the protection of personal autonomy and dignity. Kenya has domesticated these laws under Article 2(5) and (6) of the Constitution, forming part of the laws of Kenya.¹

The promulgation of the Constitution in 2010 bestowed a literal constitutional significance to the right to privacy. Notably, Article 31(c) & (d) states that individuals have the right to privacy, which includes the right not to have information relating to their family or private matters unnecessarily demanded, disclosed, or their communications' privacy infringed upon. Kenya's government plan to implement a digital identification system, Huduma Namba, can be seen as the project that accelerated the enactment of the Data Protection Act. In several legal battles, the courts ruled that a digital identification system was not feasible due to the absence of an adequate data protection framework. In the **Nubian Rights Forum v Attorney General and 2 others**, the court ordered the government to proceed with implementing NIIMS only after establishing a comprehensive data protection framework.

Before the Data Protection Act 2019 was enacted, Kenya lacked a comprehensive legal framework specifically addressing data protection, leaving personal data vulnerable to misuse. However, without dedicated legislation, enforcement relied on a fragmented set of laws.²

and judicial interpretation to operationalise Article 31 of the Constitution. These laws, including the Access to Information Act 2016, the Kenya Information and Communications Act and the Registration of Persons Act, contained limited provisions on data handling but lacked comprehensive safeguards, lacked a dedicated regulator, and left enforcement to sector-specific regulators or courts, which, at the time, lacked expertise in data privacy.

The enactment of the Data Protection Act in 2019 has brought about significant changes to the data protection landscape in Kenya, including the establishment of the rights of data subjects and the creation of the Office of the Data Protection Commissioner, which has played a vital role in enforcing the act's provisions and penalising violators. The Judiciary, through the courts, has been empowered to make influential and well-reasoned decisions. Additionally, registering data processors and data controllers has improved data protection for data subjects. The milestones since the enactment of the DPA include the enactment of several key regulations aimed at ensuring compliance and enforcement with the DPA. These regulations, gazetted under the authority of the Cabinet Secretary for Information, Communication, Technology Digital Economy, are:

The Data Protection (Complaints Handling Procedure & Enforcement) Regulations 2021 outline procedures for lodging complaints and enforcing compliance with the DPA. They specify how the ODPC investigates breaches and imposes penalties for non-compliance, ensuring accountability for data controllers and processors.

The Data Protection (Registration of Data Controllers and Data Processors) Regulations,

¹ Article 2(5) Constitution of Kenya

² Access to Information Act 2016, Kenya Information and Communications Act (KICA) 1998, and Registration of Persons Act (Cap. 107)



2021, require the registration of data controllers and processors with the ODPC. They set thresholds for mandatory registration based on factors such as the volume of data processed or the organisation's nature. This enhances transparency and oversight.

Data Protection (General) Regulations, 2021: These offer detailed guidance on data subject rights (e.g., access, rectification, erasure), restrictions on commercial use of personal data, obligations of data controllers and processors, data protection by design and default, notification of data breaches, cross-border data transfers, and data protection impact assessments (DPIAs).

Data Protection (Civil Registration) Regulations, 2020: These regulations pertain to civil registries that process personal data for registrations such as births, deaths, adoptions, passports, and marriages, ensuring adherence to data protection principles in these sensitive areas. They have been crucial in translating the DPA's broad provisions into practical requirements, promoting a structured approach to data protection in Kenya.

Additionally, the enactment of the DPA led to amendments in legislation, including the Access to Information Act, which was revised to include data protection principles for handling personal data during information disclosure, ensuring lawful processing and security; the Registration of Persons Act, which was amended to incorporate safeguards for national ID data, including NIIMS; and the Kenya Citizenship and Immigration Act, which was amended to ensure that the issuance of immigration documentation, such as passports and visas, complies with the DPA, requiring consent and the protection of personal data for all individuals.

Lessons from Amnesty Kenya's 2021 and 2024 reports

In April 2021, Amnesty International Kenya conducted an opinion poll and published a report on the level of awareness regarding the Data Protection Act and the Right to Privacy in Kenya. The opinion poll showed very low awareness of the Data Protection Act, 2019, with only 33% awareness of the Act, 18% awareness of the Office of the Data Protection Commissioner, and 47% awareness of privacy and related rights. Four years after the report's publication, awareness levels regarding key data protection issues remain a challenge in the country, highlighting the need for additional resources to strengthen awareness in Kenya.

Additionally, the report on Ready or Not? Citizens' Perspectives on Maisha Namba³, published in September 2024, highlighted key concerns regarding personal data issues. In assessing citizens' readiness to transition to the new digital identification system, the findings revealed a high level of scepticism about the measures the government had implemented to protect personal data. This scepticism was largely attributed to incidents of data breaches and a lack of public trust and confidence. As a result, there was a call for the government to enforce stricter measures to safeguard personal data and ensure digital security in the age of technological advancement during the rollout of Maisha Namba. In the current study, while examining personal data experiences, the findings indicated that data breaches continue to be perpetrated by various personnel and institutions, a problem worsened by low awareness of data protection concepts and available recourse mechanisms. These two reports laid the foundation for this research, which highlights the continuing low level of awareness.

³ Ready or Not? Citizens' Perspectives on Maisha Namba. Available at <<https://www.amnestykenya.org/aik-perception-study-report-ready-or-not-citizens-perspectives-on-maisha-namba/>> Accessed on July 10, 2025

ODPC 2025-2029 Strategic Plan

In July 2025, ODPC launched a five-year Strategic Plan to strengthen data governance in Kenya. The data protection authority has identified key social challenges such as low public awareness and knowledge of personal data protection rights, and low trust and transparency in data handling in Kenya. The Strategic Plan includes strategic objectives like improving data protection compliance through advocacy and training. Additionally, the plan outlines ways to achieve this by increasing public awareness campaigns on data protection and privacy issues and leveraging national events and stakeholder collaboration to promote the privacy agenda.

⁴ ODPC 2025-2029 Strategic Plan, Available at < <https://www.odpc.go.ke/wp-content/uploads/2025/06/ODPC-Strategic-Plan-2025-2029.pdf> > Accessed on July 10, 2025



Jurisprudence on Data Protection in Kenyan Courts

Courts and the Office of Data Protection Commissioner have played a crucial role in interpreting the provisions of the Act through their judgments, which have further operationalised the DPA.⁵ Some of the cases include the WorldCoin case, where the High Court ordered World Coin to delete all the data it had collected from subjects in Kenya. The court found that consent for this data was not properly obtained, as the data subjects were not adequately informed of their rights, and WorldCoin exploited their lack of knowledge, inducing them to provide their personal information data.⁶

The Office of the Data Protection Commissioner has also issued key decisions to enforce the provisions of the Data Protection Act. A notable example is the Roma School case, in which the institution was fined KES 4,550,000 (Kenyan Shillings Four Million, Five Hundred and Fifty Thousand) for publishing images of minors without parental consent. This marked the first instance in which an educational institution was penalised by the ODPC for non-compliance with the DPA.⁷ To address the increasing concern over digital lenders unlawfully accessing and using the names and contact details of borrowers' family members and friends to

send threatening messages and calls during debt recovery efforts, the Office of the Data Protection Commissioner (ODPC) imposed a fine of KES 2,975,000 (Kenyan Shillings Two Million, Nine Hundred and Seventy-Five Thousand) on two digital lending companies. This enforcement action aims to ensure that such lenders only cooperate with data subjects who have willingly consented to the processing of their personal data.

In a recent case, Hotel Tobriana (ODPC Complaint No. 1708 of 2024) posted images of the complainant's wedding on its social media platforms (Facebook and Instagram) for advertising purposes. Richard, the complainant, lodged a complaint with the ODPC, arguing that his image, along with those of his ten-year-old son and other family members, was used for commercial gain. The ODPC found Hotel Tobriana in breach of Richard's data rights and that it violated his right to erasure. The hotel was fined Ksh . 750,000 and ordered to remove the wedding images from its social media platforms within 14 days.⁹ This case highlights the importance of obtaining consent before using personal data, specifically images, for commercial activities and emphasises the consequences of failing to comply with data

⁵Nubian Rights Forum & 2 Others v Attorney General & 6 Others [2020] eKLR; Kenya National Commission on Human Rights v Communications Authority of Kenya & 4 Others; Republic v Joe Mucheru & 2 Others Ex Parte Katiba Institute & Another; Mwanzia v Rhodes [2023] KEHC 2688 (KLR)

⁶Republic v Tools for Humanity Corporation (US) & 8 others; Katiba Institute & 4 others (Exparte Applicants); Data Privacy & Governance Society of Kenya (Interested Party) (Judicial Review Application E119 of 2023) [2025] KEHC 5629 (KLR) (Judicial Review) (5 May 2025) (Judgment).

⁷Office Of The Data Protection Commissioner, Office Of The Data Protection Commissioner Issues Three (3) Penalty Notices Totalling To Kenya Shillings 9,375,000, <https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-ISSUES-THREE-PENALTY-NOTICES-TOTALLING-TO-KSHS-9375000> 26 September 2023.

⁹Privacy Breach at Hotel Tobriana: Wedding Photos in Ads cost Sh. 750,000. Available on <<https://theweeklyvisionews.net/2025/04/09/privacy-breach-at-hotel-tobriana-wedding-photos-used-in-ads-cost-sh750000/>> Accessed on July 8, 2025

protection regulations and respecting data subjects' right to erasure. Despite significant progress in policy and legal frameworks related to the Data Protection Act, the hypothesis was that these developments might not reflect the experiences of the public. Therefore, Amnesty International Kenya conducted a study to evaluate public awareness and perceptions of the Data Protection Act across Kenya.

Furthermore, this study examined the level of public awareness regarding data protection and privacy rights, as well as the effectiveness of the DPA's implementation and whether its

objectives have been achieved. Conducted through Focus Group Discussions, the research explored citizens' experiences with managing personal data, including any data breaches, and assessed the public's understanding of the ODPC's mandate and activities. The results aim to support future advocacy efforts, inform policy development under the Data Protection Act, and identify new ways to collaborate with the ODPC and other institutions to achieve DPA's objectives.



Methodology

Amnesty International Kenya held focus group discussions in Nairobi, Kisumu, Taita Taveta, Mombasa, Turkana, Wajir, Tana River, Nakuru, Meru, and Kilifi. These counties included both major cities and rural areas of Kenya. Key Informant Interviews were also conducted in Nakuru, Mombasa, and Kisumu. The information from these two sources was combined and analysed to produce this report.

Participants included representatives from community-based organisations, religious leaders, local administrators, and civil society organisations such as Social Justice Centres, which primarily handle data from multiple data subjects. They were chosen to reflect diverse demographics, including women, youth, urban and rural residents, and vulnerable groups. The research team from Amnesty International Kenya obtained informed consent from all participants at each stage of the study and allowed interviewees to withdraw their consent at any point.

Public Awareness of the DPA

This research aimed to assess the level of awareness of the Data Protection Act among the Kenyan population. The questions explored whether participants had heard of the DPA, where they had come across it, and which concepts within the Act they valued most. Based on our findings, awareness of the DPA Act is moderate, with urban areas such as Nairobi, Kilifi, Nakuru, and Kisumu showing a high level of comprehensive understanding of the Act and its provisions. Rural counties, however, have a low understanding of the Data Protection Act. Most participants from these counties have heard about the Act but did not explicitly understand its provisions. While some participants noted hearing about the Act through social media and mainstream media, most participants reported learning about it through civil society organisation training or by engaging in civil society activities and observing how these organisations uphold data protection standards. Many others interacted with the DPA via social media, where various discussions on data protection have taken place.

“I heard about the action on TV and on TikTok, as well as interactions with other organisations, during the Genz Protests” - Participant, Kilifi.

“I knew it through my cybercafé business, where I log in to people's accounts while offering services. I have supported

someone while registering as a data handler” - Participant, Mombasa

“I am a journalism student who studied the Act under the Media Law and Ethics course” - Participant, Tana.

Some of the participants have heard about the law when in operation than reading or being trained about the law.

“I knew about the Act when I heard that a school and a nightclub had been fined for violating someone's privacy” - Participant, Taita Taveta.

In Meru, notably, the awareness level was relatively low, with only one participant out of 12 having prior knowledge of the Act through television news. Nairobi exhibited the highest levels of awareness of the Data Protection Act, with all participants having heard about or engaged with its provisions.

Generally, participants who interacted with the act seemed well-versed in the concept of consent and the importance of obtaining it from data subjects before processing any data or information.

"I heard it from a friend in our community whose child's photo was taken without their consent. The parent sued the photographer and received compensation"- Participant, Nairobi.

"We are not permitted to share children's information without consent" - Participant, Wajir County

This research highlighted a moderate level of awareness of data subject rights. Additionally, participants indicated that their personal data is private and should not be accessed without permission, nor stored longer than necessary. This demonstrates an admirable understanding of data processing principles and rights.

The following rights were recorded to be the most important to most participants:

- Right to be informed
- Right to rectification
- Right to access

Finally, this objective aimed to examine citizens' awareness of the meaning of personal data. Findings from this research indicated a high level of awareness of personal data and sensitive personal data. However, few participants could clearly distinguish between them.

"It is that information which belongs to a person and should

not be accessed unlawfully — includes ID Number, my KRA Pin" - Nakuru FGD Participant.

"It is any data that can trace you and includes biometrics, KRA pin, passwords, date of birth" - Kilifi FGD participant.

"Anything that relates to me, including my name and information I give during online engagements" - Mombasa FGD Participants

"It includes that info that belongs to me, given out for a specific use and once given out should be taken good care of" - Nakuru FGD participant

Given Kenya's social, economic, and internet exposure, a lack of knowledge of the law can lead to non-compliance. This means that the Office of the Data Protection Commissioner needs to put in more effort to create awareness about the DPA.

Personal Data Protection Experiences

This objective aimed to explore participants' experiences with sharing personal data and to determine whether they had encountered any data breaches. The majority of the participants said they would share their personal data only if they trusted the person requesting it. Some added that they would be willing to share if the collector clearly explained why the data was needed. A small number of participants, however, expressed deep skepticism and said they would not share their information at all. Many attributed this distrust to recent incidents where social media platforms collected and used people's data without their consent.

"I don't readily share because I fear impersonation" - Participant, Nairobi.

A few participants admitted they would resort to providing false information rather than sharing their personal details, an action that could compromise data quality. Alarming, some reported that sensitive data, including health information, had been disclosed to third parties without their knowledge or permission.

"I use wrong details mostly" – Participants, Meru

"A friend sought medical services, and the nurse realised that he was ill, The nurse went to reveal the information to the

girlfriend" - Participant Nakuru

Participants in the 10 Counties exhibited high knowledge levels of data breaches. It was broadly defined as the use of data without consent or for unintended purposes, or using data collected for reasons other than its intended use.

"I participated in a survey where they asked how many youth are willing to participate in the 2027 elections as aspirants. E gave out information, but then we ended up being enrolled as members of political parties to give the 'owners' political mileage." - Participant, Nairobi

"I cannot share because I receive messages from financial institutions, I am not a party to" - Participant, Mombasa

Most participants did not pursue any remedy after experiencing data breaches, citing a lack of awareness about available legal recourse. Even among those aware, many believed action

would be slow or ineffective, with little to no consequences for violators. A minority reported incidents primarily to the police and Safaricom but noted inadequate support, as officers often lacked understanding of data protection issues. Notably, no participants reported breaches to the ODPC, highlighting its limited visibility as a redress mechanism.

Information gathered from focus group discussions revealed that the related provision of the Act is not being consistently followed, despite its clear legal requirements. Furthermore, representatives from community-based organisations that manage personal data reported that their organisations lack clear protocols for identifying, preventing, and responding to data breaches. This situation not only puts the affected individuals at risk but also undermines the credibility and legal compliance of the organisations involved.

Information collated from the focus group discussions indicated that this provision of the Act was not being adhered to, despite the existence of legal provisions to the contrary. Additionally, representatives of community-based organisations, which handle data, indicated that their organisations lack clear pathways to assess, prevent, and contain data breaches within their organisations. This position is not only prejudiced against the affected organisations.

Requesting access or deletion

While the Data Protection Act guarantees individuals the right to access their personal information and request its correction or deletion, the reality for many citizens tells a different story. Across the counties visited, especially in marginalized and rural areas, there is a significant lack of awareness and capacity to exercise these rights, compounded by weak enforcement mechanisms. As a result, many Kenyans face challenges when trying to rectify or erase data collected without proper consent:

“I requested a political party to deregister my membership, which they had signed me up for illegally” - Participant, Meru.

“An organisation in Nakuru collected my information and asked them to correct my name as it was misspelt when they collected it” - Nakuru FGD participant

A media organisation misrepresented me during a PWD conference and I requested they correct it. They didn't delete or rectify the mistake, and the only apology they offered was to say they were working on it. They also claimed they have no control over information already appearing on the digital platform — Nakuru FGD Participant. These first-hand experiences underscore the gap between data subject rights and lived experiences of many Kenyans. Many institutions either lack the capacity or the willingness

to uphold data subjects' rights. Worse, they sometimes hide behind technical excuses or bureaucratic processes. The right to access and deletion isn't just a legal formality but about accountability and dignity of a data subject. As digital footprints expand, the urgency to operationalize these rights in real and responsive ways becomes even more pressing.

Amnesty International Kenya conducted key informant interviews with informants in Kisumu, Nakuru, Mombasa, and Nairobi. The responses below show that awareness and compliance with the Data Protection Act (DPA) have significantly improved among civil society organisations (CSOs) across Kenya. Many CSOs have developed internal privacy policies, established data protection mechanisms, and now seek informed consent before collecting or sharing community data. This shift has strengthened trust between CSOs and the communities they serve.

However, challenges remain, especially in areas such as limited resources, staff and volunteer awareness, and community understanding of data subject rights and the role of the Office of the Data Protection Commissioner (ODPC). Regions such as Kisumu, Kakamega, and Nakuru continue to face challenges in raising grassroots awareness and promoting attitudinal change towards data privacy.

“These days, we understand the impact of data protection as a CSO. We typically contact our communities before sharing their data, and they are aware of the need for their consent” -

Participant, Mombasa.

“We have now successfully embedded these regulations within our organisations.

We know how to collect data from communities effectively. Internally, we've also ensured that each of our staff members gains knowledge on data protection” - Participant,

Mombasa.

“Success with the DPA has been promoting locally-led awareness of data protection and digital rights within Kisumu and Kakamega counties. We've been able to cascade this awareness within communities. One major challenge remains: general awareness in this region and shifting community attitudes around data rights. Many people still don't know their rights, nor the mandate of the ODPC.

Now, with the emergence of new technologies, this raises even more concerns about data protection” - Participant- Kisumu

“At WeCare, we now obtain informed consent when collecting data. We also have a Data Protection Officer (DPO) and mechanisms in place to prevent breaches. This has helped us build trust with the communities we serve” - Participant, Kisumu.

“Our main challenge has been the inadequate resources to maintain strong data protection systems. Another challenge is the lack of awareness among our staff and volunteers; for many people in Kisumu, data protection is still not a priority” - Participant Kisumu.

“Since the implementation of the Data Protection Act, CSOs,

especially those operating in Nakuru, have become very intentional about how they collect and share data. We now seek consent from the people we work with and limit access to personal data to specific personnel, to ensure everyone's data is safeguarded. This has become embedded in CSO culture as good working practice since the DPA 2019 came into effect”

- Participant, Nakuru

out there, somewhere in that organisation” - Participant, Nairobi

“Before I learned about data protection, I used to give out my data casually. There was a friend who was doing a promotion, and he asked for my details so he could earn his daily wages. As a good friend, I said, ‘Go ahead,’ and gave him whatever he needed. Years later, I still don’t know what that information was used for, but I know my data is



Awareness of the ODPC

Public awareness of the Office of the Data Protection Commissioner (ODPC) was found to be generally low in the rural counties as compared to the urban counties. Most participants reported that they were unfamiliar with the Office and had not heard of its functions, powers, duties, and obligations.

Furthermore, participants indicated a lack of knowledge regarding the reporting mechanisms and procedures established by the ODPC. This lack of awareness significantly hindered their capacity to take appropriate action in instances where their personal data had been breached or otherwise violated. The low awareness of ODPC is due to most regions not having a physical ODPC office. However, in counties with offices such as Nakuru and Kisumu, very few participants knew about or had interacted with the office.

When asked what could be done to ensure that the ODPC was visible, the participant recommended the following:

1. ODPC to utilise creative art to educate the public about the office's functions-

This can be done by using means which communities can easily relate to, including creating and sharing short explainer videos, producing brief animated or live-action clips that outline the ODPC's role, how to access its services, and where to file complaints, posting these videos on various platforms where they can reach a wider audience. The office of the ODPC can also partner with local influencers and youth digital advocates to increase visibility.

2. Expand physical presence-

Participants, especially those from underserved counties (Wajir, Tana River, Turkana), recommended that the office create offices in their respective counties

to increase visibility. Participants proposed that while the office awaits allocation of resources for expansion, they could work towards having the offices co-located with Huduma centres. They also proposed stationing ODPC officers in police stations to handle inquiries, offer guidance on filing complaints with the office of the ODPC, and aid in referrals to ODPC.

3. Community-Level Sensitization-

Participants recommended that ODPC undertakes baraza-style engagements, community dialogues, and roadshows especially in under-represented areas to raise awareness about rights under the DPA. These were recommended because in the marginalised areas, they are the most related ways of raising awareness about various topics.

It was also recommended that the ODPC doubles its efforts in working with local CSOs, Chiefs, county teams, and community radio stations to disseminate messages and gather feedback.

4. Use Social Media for Education Campaigns-

ODPC should launch coordinated campaigns on mainstream and social media platform frequented by Kenyans to share educational content, success stories, tips for personal data protection, and the rights of data subject

5. Partner with Grassroots and Youth Networks-

Participants recommended that ODPC doubles its efforts in partnering with local youth groups, student unions, women's and PWD associations, and queer/non-binary networks to co-design and deliver outreach. This was proposed because the said groups

experience data breaches in a unique way and therefore requiring unique approaches to reach them and have the DPA make sense to their unique situations.

Additionally, this could also be achieved through forming multi-Stakeholder Working Groups and use those groups working groups for regular updates, feedback loops, and co-create community-friendly materials about ODPC.

6. Secure a dedicated budget for awareness programs-

It was recommended that ODPC secure an annual budget dedicated to grassroots campaigns, digital outreach, and community participation initiatives to raise awareness amongst communities on the duties of ODPC.



Conclusion

The findings of this study highlight several challenges that must be addressed to ensure the effective implementation of the Data Protection Act (DPA) in Kenya. Awareness and understanding of the DPA remains relatively low, particularly in marginalised counties, especially those visited by Amnesty International Kenya. Many citizens lack the knowledge and capacity to fully understand their data rights or provide informed consent, leaving them vulnerable to the misuse of their personal information.

In contrast, awareness levels are notably higher in urban areas, where outreach efforts appear to have had a greater impact. Despite efforts by the Office of the Data Protection Commissioner and its partners, civic and digital education initiatives have not reached a substantial portion of the population. This gap is particularly evident in rural and underserved regions, where public education on data rights remains inadequate. Furthermore, vulnerable and marginalised groups, including youth, persons with disabilities, gender minorities, and low-literacy communities, continue to be excluded from discussions around data protection and the implementation of the DPA. This lack of representation risks reinforcing systemic inequities in the protection of data privacy and access to remedies. Another major challenge is the limited local presence of the ODPC. Without decentralised offices or effective grassroots outreach mechanisms, the ODPC remains largely inaccessible to many citizens. This disconnect reduces public trust and limits the DPA's effectiveness in practice. Lastly, a perceived lack of consistent enforcement undermines confidence in the DPA.

Although the ODPC has taken enforcement actions in some cases, its capacity is constrained by limited funding, staffing shortages, and restricted institutional independence, particularly when addressing large-scale violations.

In conclusion, while Kenya's DPA provides a robust legal framework, its practical impact is significantly weakened by low public awareness, limited inclusivity, insufficient regional presence, and enforcement. To build a stronger data protection culture, Kenya must prioritise strategic investments in public education, inclusive advocacy, regional institutional development, and proactive enforcement.

Addressing these challenges is essential for ensuring that data protection rights are fully realised by all citizens across all parts of the country.

Recommendations on Effective DPA Implementation

Based on the findings of this study, Amnesty International Kenya makes the following recommendations:

1. Community Engagement & Education-

This will include conducting civic and digital literacy campaigns focused on data protection and sensitising communities through local media, especially community radio, chief's barazas, and social media platforms. This will ensure that communities are aware of the ODPC and its functions so that they can effectively utilise its processes to ensure effective implementation of the Data Protection Act.

2. Intentional Inclusion and Participation of Vulnerable Groups-

Participants noted that vulnerable groups were left out in the implementation of the act and subsequent policies, which have been developed to ensure effective implementation of the Act. Effectively, it is proposed that for the act to achieve its intended purpose, these groups must be included and involved to ensure that they also benefit from the provisions of the Act.

3. Institutional Presence & Capacity-

ODPC should widen its engagement and form working groups comprising ODPC personnel, police representatives, and community members to coordinate implementation. Additionally, ODPC should deploy ODPC officers within police stations, with dedicated desks to train officers on data-protection standards and reporting procedures and address citizen complaints and inquiries directly.

4. **Enforcement and Accountability** - ODPC should enhance its enforcement powers, particularly those that enable it to investigate and make decisions regarding data breaches, especially sui moto investigations. These cases, especially those involving telecom companies and other big tech companies that collect and process personal data. This will build public trust, demonstrate credibility, and deter violations.
5. **Multi-Sectoral Collaboration** ODPC should engage diverse stakeholders across the government, private sector, CSOs, and media in multi-sectoral forums, especially in rural counties, such as counties (Wajir, Turkana) outside of Nairobi, to address issues preventing the effective implementation of the DPA.
6. **Inclusion of basic data protection concepts within the education curriculum at all levels.**





Amnesty International Kenya

Ground Floor, 197 Lenana Place

Lenana Road, Kilimani

P.O Box 1527-00606

Nairobi, Kenya



AmnestyKenya



amnesty_kenya



Amnesty International Kenya