



DPGSK

Data Privacy
and Governance
Society of Kenya

2026 ANNUAL PROFESSIONALS' PERCEPTION SURVEY

ANALYSIS AND FINDINGS REPORT

The state of data protection practice, AI governance, state surveillance,
and electoral data risk in Kenya, as seen by the profession

Contents

1. Executive Summary	4
Key findings.....	5
2. About the Survey.....	6
Purpose	8
Method and respondents	8
Limitations	8
3. Respondent Profile	9
4. AI Governance and the DPO Function	12
Capability and exposure.....	13
What practitioners agree on	13
What practitioners need	14
5. ODPC Enforcement	16
Does enforcement change behaviour?.....	17
Perceived effectiveness	17
Which levers work best	17
Where to enforce	18
6. The DPO's Organisational Standing	19
Seat at the table	20
Reporting lines and management attitude	20
Workload.....	20
7. Sectoral Compliance Assessment	22
A public-sector compliance deficit.....	23
Most and least compliant — the forced choice	23
Why organisations fail to comply	24
Most-breached obligations and the private-sector verdict.....	25
8. State Surveillance and the Telcos.....	26
The activities that concern practitioners most	27
Is the DPA adequate against surveillance?	28
The telcos	28
9. Actor Responsibility and Risk	30
Who poses the greatest risk to individuals	31
Who is most responsible	31
OSINT, data brokers, essential services and MSMEs	31
The individual's own role.....	32
10. The 2027 General Election.....	33
The scale of concern.....	34
Which risks rank highest	34
What the profession wants done	35
11. Jurisprudence and ODPC Determinations	36
Determinations are changing practice	37
The cases that shape practice.....	37

12. Conclusions and Recommendations	38
For the Office of the Data Protection Commissioner	39
For Parliament and law reform	39
For the IEBC and the 2027 election.....	39
For DPGSK and the profession.....	39

01

SECTION 1

EXECUTIVE SUMMARY



This report presents the findings of the 2026 Annual DPGSK Professionals' Perception Survey, completed by 62 data governance professionals practising in Kenya between June and July 2026. The instrument canvassed practitioner opinion across the full arc of the discipline:

- a. the changing role of the Data Protection Officer (DPO),
- b. readiness to govern artificial intelligence,
- c. the Office of the Data Protection Commissioner's (ODPC) enforcement posture,
- d. sector-by-sector compliance,
- e. state surveillance and the position of telecommunications companies, and
- f. the data and AI risks facing the 2027 General Election.

The picture that emerges is of a profession that is confident in its mandate, deeply concerned about the state's handling of personal data, and convinced that both the law and the regulator ought to move further and faster.



Key findings

- **The DPO role is expanding beyond its statutory responsibilities.** Three-quarters of respondents agree the DPO function should be formally extended to cover AI governance, and an even stronger majority hold that AI responsibilities should attract additional remuneration. Only a minority accept that the Data Protection Act, 2019 (DPA) already provides a sufficient framework for AI-related processing, a clear signal that practitioners see a legislative gap.
- **AI capability is moderate and unevenly distributed.** Half of respondents rate their own AI-governance capability as no better than “moderate,” and only 26% describe themselves as “strong.” The most-requested supports are practical DPIA templates for AI systems and a structured course on AI ethics and risk, followed closely by a dedicated DPGSK CPD session on the AI Regulation.
- **Enforcement is felt but judged incomplete.** Many consider the ODPC's enforcement approach only “moderately effective.” Practitioners would prioritise ODPC-mandated compliance audits, administrative penalties and published enforcement notices that name data handlers as the levers most likely to drive compliance.
- **Compliance is a public-sector problem above all.** Of 28 sectors rated, county governments, security and intelligence agencies and national government ministries sit at the very bottom, while banks sit at the top. The sectors most frequently named as non-compliant include digital lenders, government and county governments. These map almost exactly onto where respondents want the ODPC to concentrate its 2026–2027 enforcement.
- **State actors dominate the risk register.** Asked to rate the data-governance risk each actor poses to individuals, respondents place the National Police Service/DCI, the National Intelligence Service, the Kenya Revenue Authority and the telcos at the top, all well into “high-to-critical” territory. Fully 97% are concerned

about state surveillance, and only a minority believe the DPA as it stands adequately protects citizens against it.

- **Telcos are seen as complicit, and transparency is demanded.** A clear majority characterise telcos as at least being partially complicit in unlawful state access to subscriber data and support a legal or voluntary annual transparency-reporting obligation.
- **The 2027 election is viewed as a data-protection emergency.** Ninety per cent regard the threat of data misuse and AI-generated content in the 2027 campaign as “existential” or “extremely” serious. Deep-fake video and manipulated audio of candidates top the list of AI risks, and strong majorities support requiring political parties to register as data controllers and treating unlawful electoral data use as an electoral offence.
- **Jurisprudence shapes practice.** Practitioners follow ODPC determinations closely and credit them with materially changing consent, data-sharing and data-subject-rights practices. The cases most often cited as influential include the *Huduma Namba litigation*, *Katiba Institute v Communications Authority*, the *LSK v Safaricom petition*, the *Worldcoin/Tools for Humanity matter* and the *Cleanshelf privacy case*. This indicates that Kenyan courts are now a primary driver of compliance behaviour.

02

SECTION 2

ABOUT THE SURVEY





Purpose

The Annual DPGSK Professionals' Perception Survey is the Society's flagship instrument for capturing how Kenya's data governance community reads the state of the field. The 2026 edition was structured around three developments shaping practice this year: the emergence of a dedicated AI regulatory agenda (including the AI Bill, 2026), the maturing enforcement record of the ODPC, and the approach of the 2027 General Election.

Method and respondents

The questionnaire comprised 125 items across thirteen thematic sections, combining single- and multiple-choice questions, Likert-type rating scales, forced-ranking items and open text. It was administered online and completed by 62 respondents during fieldwork between 5 June and 31 July 2026. Respondents are experienced: 74% hold a postgraduate qualification, 56% have eleven or more years of overall professional experience, and half have practised data protection specifically for four years or more.

Limitations

The findings represent the considered opinion of an engaged, self-selecting community of practitioners; they are a barometer of professional perception rather than a nationally representative survey of organisations or the public. With a sample of 62, sub-group figures should be read as indicative.

03

SECTION 3

RESPONDENT PROFILE



Respondents are evenly split by gender (32 women, 28 men, two preferring not to say) and concentrated in the mid-career band: 39% are aged 36–45 and a further third are 31–35. The sample is highly qualified, 45% hold a master’s degree and a further quarter a postgraduate diploma. Law is the dominant professional background (31 of 62), followed by information technology and cybersecurity (15), reflecting the discipline’s twin roots in legal and technical practice.



Figure 1. Respondent demographics (N = 62).

Most respondents work in the private sector, in corporate roles and in legal practice or consulting, with meaningful representation from national government, academia and civil society.

Notably, over half report that they **perform data protection functions without formally holding the DPO title**, while others are internal DPOs employed by the data controller. This under-titling of the function is itself a governance finding: it suggests that in many organisations the DPO role, as envisaged by section 24 of the DPA and the Data Protection (General) Regulations, 2021, is being discharged informally rather than through a designated, empowered office.



Primary place of work

Distribution of 61 recorded responses

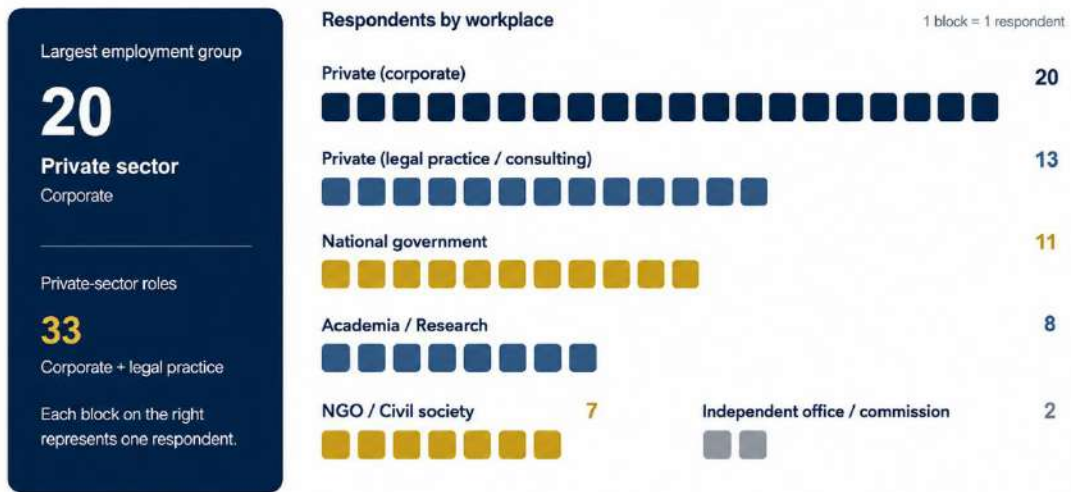


Figure 2. Primary place of work.

04

SECTION 4

AI GOVERNANCE & THE DPO FUNCTION



If a single theme runs through the 2026 survey, it is that artificial intelligence has arrived faster than the profession’s mandate, tools and remuneration have adjusted to meet it. Practitioners are being pulled into AI governance in practice while the formal architecture around them lags.

Capability and exposure

Only 26% rate themselves as “strong” and confident advising on AI-specific obligations. The largest group (30) describe their capability as “moderate, able to navigate the basics but in need of specialised training,” and 16 more are “limited” or would defer to a specialist.

Exposure to AI-specific casework is still nascent: only 19 of 62 have led or contributed to a Data Protection Impact Assessment (DPIA) for an AI or automated decision-making system in the past two years, though many of the remainder expect to within twelve months.

Involvement in AI decisions is the weakest of all decision types tested: for the adoption of AI or automated tools, more respondents report being “not involved” than involved before the decision.



Figure 3. Self-rated capability to advise on AI governance.

What practitioners agree on

Respondents endorse extending the DPO role to AI governance, agree that most Kenyan DPOs currently lack the technical knowledge to govern AI, and strongly agree that AI responsibilities should be separately remunerated. Crucially, they do not accept that the DPA 2019 already suffices for AI: at a mean of 2.64 this is the only statement to fall below the neutral midpoint. Read together, these results articulate a coherent professional position, expand the mandate, resource it, and give it a firmer legislative footing.

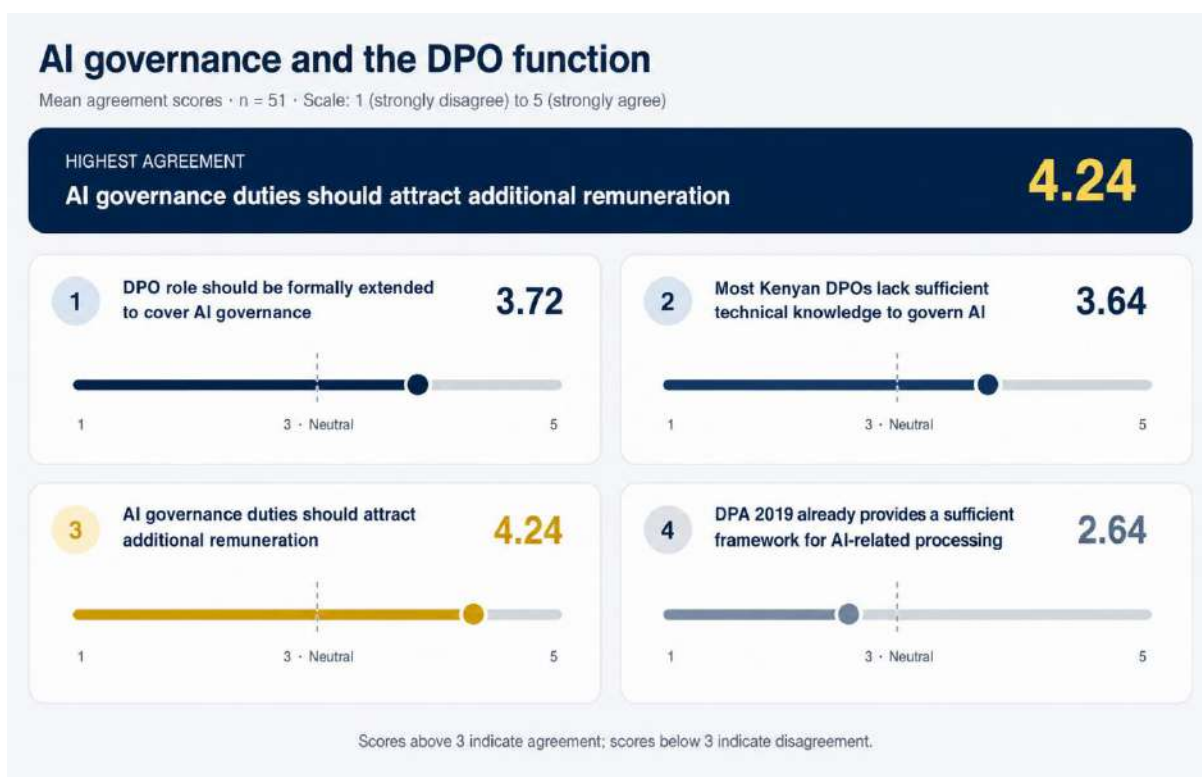


Figure 4. Mean agreement with statements on AI governance and the DPO function (1 = Strongly Disagree, 5 = Strongly Agree; n = 51).

What practitioners need

Asked to select the resources that would most improve their AI-governance capability, respondents prioritised the practical over the theoretical:

- DPIA templates and guidance tailored to AI systems,
- a structured course on AI ethics and risk assessment, and
- a DPGSK CPD session dedicated to the AI Regulation.

Demand for mentorship and comparative regulatory material, the EU AI Act, Singapore and others round out a clear brief for the Society's capacity-building programme.

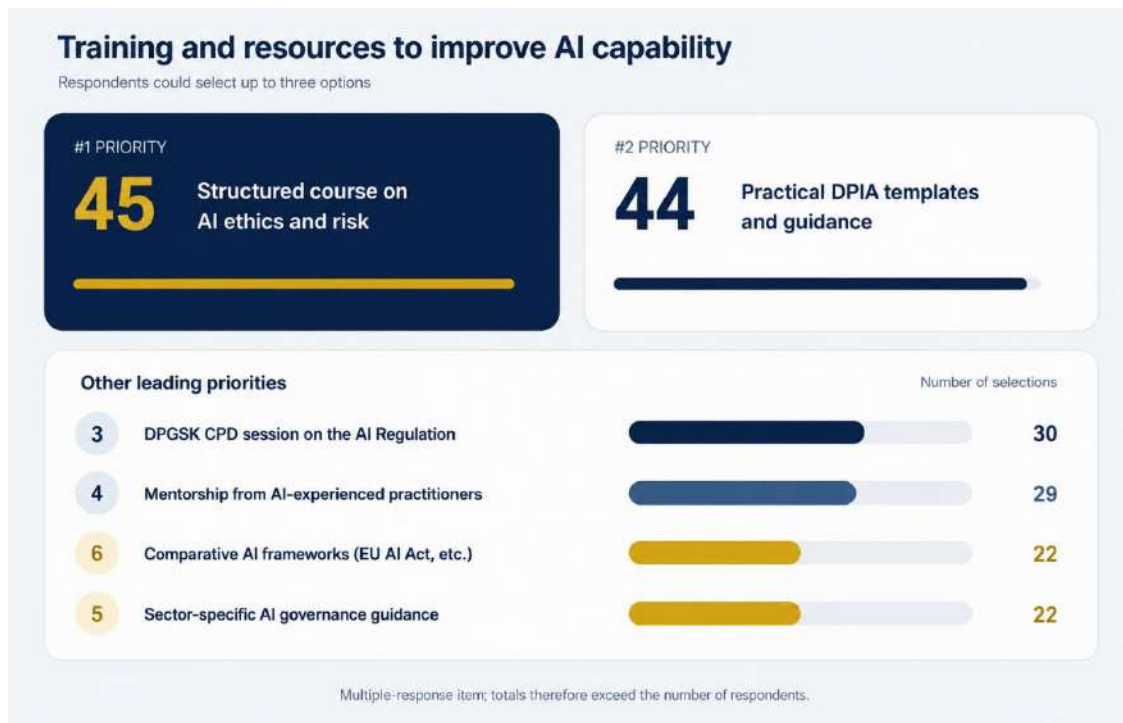


Figure 5. Training and resources that would most improve AI-governance capability (up to three).

“The DPO role should be formally extended to cover AI governance, and AI governance responsibilities should attract additional remuneration.”

~ THE TWO MOST STRONGLY ENDORSED POSITIONS IN THE SURVEY

05

SECTION 5

ODPC ENFORCEMENT



Direct experience of enforcement remains the exception rather than the rule: half of respondents report no involvement in any ODPC enforcement process in the past two years. Where there has been contact, it has most often taken the form of an ODPC investigation or audit, voluntary engagement on a compliance matter, or a complaint filed against the organisation. Enforcement notices and penalty notices remain comparatively rare in respondents' direct experience.

Does enforcement change behaviour?

Where enforcement has occurred, the organisational response is mixed. The most common outcome was significant investment in data protection infrastructure, staffing and training, but many organisations updated policies without committing new resources or responded only minimally to the specific finding.

Enforcement does appear to raise the DPO's internal standing: 30 of the respondents who had a view said the DPO is now taken more seriously, or that enforcement opened budget and executive attention.

Perceived effectiveness

About half the respondents judge the ODPC's current enforcement approach only "moderately effective, creating some incentive but inconsistent." A meaningful group consider it "very effective," while others see limited effect and think it too early to assess.

Enforcement exists, but it is not yet consistent or visible enough to drive compliance.

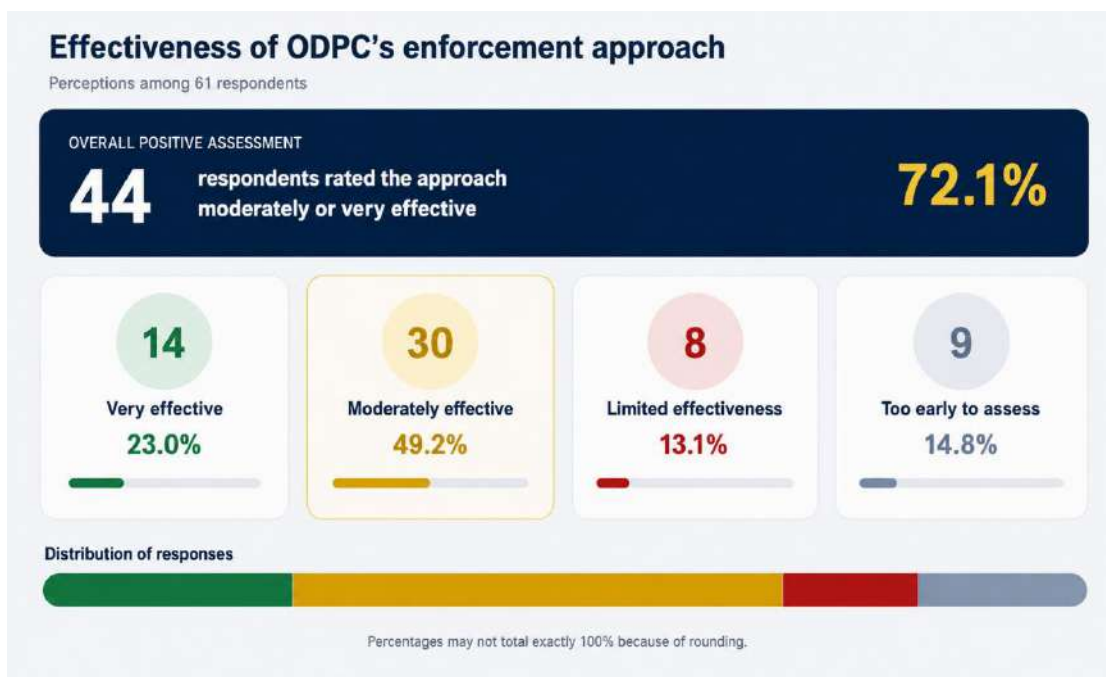


Figure 6. Perceived effectiveness of the ODPC's current enforcement approach.

Which levers work best

Practitioners are clear about what would sharpen enforcement. ODPC-mandated compliance audits lead decisively, ahead of administrative penalties and published enforcement notices that name data handlers. Reputational transparency ranks alongside financial penalty in the professional mind. Mandatory DPO designation enforced through registration conditions and sector-specific enforcement campaigns complete the toolkit.



Figure 7. Enforcement actions considered most effective at driving compliance (up to three).

Where to enforce

Asked where the ODPC should prioritise enforcement in 2026–2027, respondents pointed to the health sector, AI and algorithmic systems, the public sector and government agencies, social media and digital platforms, financial services and telecommunications.

06

SECTION 6

THE DPO'S ORGANISATIONAL STANDING



The survey probes where the DPO sits in organisational decision-making, a proxy for whether the function operates as the independent, early-warning role the DPA contemplates or as a downstream compliance check. The results show a function consulted reasonably early on core data transactions but marginalised on precisely the decisions that now matter most.

Seat at the table

Involvement is strongest for entry into data-sharing or processing agreements (21 involved before the decision) and for marketing/customer-data programmes (18). It is weakest for the adoption of AI and automated tools, organisational restructuring, and cross-border expansion; for each of these, “not involved” is the single most common answer. That the DPO is least present for AI adoption, restructuring and cross-border moves is a governance blind spot, since these are among the highest-risk processing decisions an organisation makes.



DPO involvement across organisational decisions (n = 62).

Reporting lines and management attitude

Board-level visibility is partial. Only 18 of 62 report to the Board quarterly or more often; 16 have no formal reporting line to senior management at all, and 13 report only when an incident arises.

On management attitude, the dominant view is that data protection is treated as a regulatory compliance requirement but not a business priority; more say management shows minimal interest absent enforcement risk.

Just 10 report that data protection is viewed as a strategic priority. One respondent’s plea captures the mood: **DPGSK should convene CEO round tables to “drive engagement and buy-in from the top.”**

Workload

The function is under strain. A majority report that their workload has increased over the past year, and only 20 describe their current workload as “manageable” and the rest are “stretched” (24), “overloaded” (8) or “severely



overloaded” (7). The primary drivers are AI and new-technology adoption creating fresh obligations (39), growth in ODPC enforcement activity (35), and new regulatory requirements (29). Capacity, in short, is not keeping pace with mandate.

07

SECTION 7

SECTORAL COMPLIANCE ASSESSMENT



Respondents rated the 2026 compliance of 28 sectors on a five-point scale (1 = very poor, 5 = exemplary), scoring only sectors in which they had direct experience. The resulting league table is one of the report’s most actionable outputs: it identifies, from the vantage point of practitioners who work across these sectors, exactly where the DPA is and is not being honoured.



Figure 8. Mean sectoral data-protection compliance, 2026 (1 = Very Poor, 5 = Exemplary). Red < 2.3; gold 2.3–3.0; green ≥ 3.0.

A public-sector compliance deficit

Only banks and deposit-taking institutions (3.69) score clearly above the “adequate” line of 3.0, with mobile money (3.10) and private hospitals (3.08) just at it. Everything else falls below. The floor of the table is occupied almost entirely by the state: county governments (1.71), security/intelligence/law-enforcement agencies (2.03), national government ministries (2.08), water and sewerage companies (2.15) and MSMEs (2.17). Digital lenders (2.45) and the SHA/NHIF (2.39) also score poorly, both areas of intense public sensitivity. The pattern is unambiguous: the sectors that hold the most sensitive data and wield the most power over citizens are perceived to be the least compliant.

Most and least compliant: the forced choice

Asked to name the three most non-compliant sectors outright, respondents pointed to digital lenders and credit-scoring platforms, national government ministries, county governments and social-media/global platforms. The

mirror question produced a striking consensus at the top: 46 of 62 named banks as among the most compliant, well ahead of legal and professional services firms and mobile money.

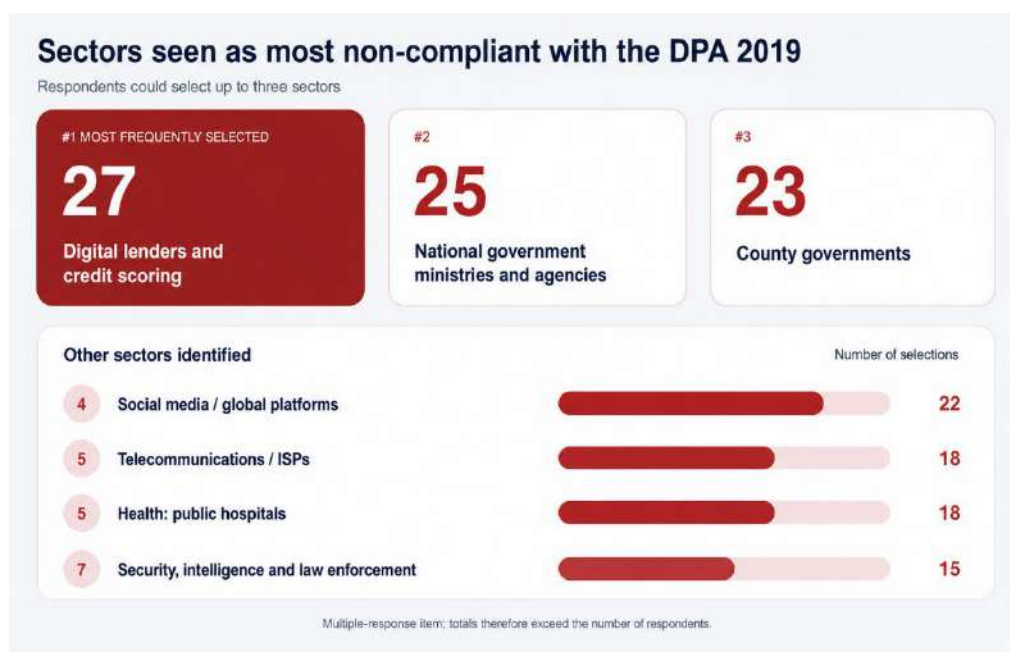


Figure 9. Sectors most frequently named as non-compliant with the DPA 2019.



Figure 10. Sectors most frequently named as compliant with the DPA 2019.

Why organisations fail to comply

The diagnosis is cultural and managerial before it is technical. Management indifference leads, followed by genuine ignorance of DPA obligations, a shortage of qualified DPOs in the market, the perceived cost of compliance relative to enforcement risk, and cultural resistance. This ordering matters for strategy: awareness-raising and executive engagement address the top two causes far more directly than another round of technical guidance would.



Figure 11. Primary reasons sectors fail to comply with the DPA 2019 (up to three).

Most-breached obligations and the private-sector verdict

The obligations most breached, in respondents' experience, are processing without a lawful basis under section 30 of the DPA, the failure to conduct a DPIA for high-risk processing, and the absence or inadequacy of privacy notices; the foundational duties of the Act.

On the overall state of private-sector compliance, the settled view is "moderate, improving but with significant structural gaps," with the remainder split between "good," "poor" and "very poor." Respondents singled out telecommunications companies, digital and mobile lenders, the hospitality and education sectors, SACCOs, and county and national government as warranting urgent ODPC attention.

08

SECTION 8

STATE SURVEILLANCE & THE POSITION OF TELCOS



Nowhere is professional opinion more emphatic than on state surveillance. Ninety-seven per cent of respondents are concerned about the use of personal data by Kenyan state agencies for surveillance, 42 of 62 “very concerned,” describing it as a serious and present threat to constitutional rights. This is not a fringe anxiety; it is the settled consensus of the profession.



Figure 12. Concern about state use of personal data for surveillance.

The activities that concern practitioners most

The specific practices of greatest concern are the interception of communications by intelligence and law-enforcement agencies under the NIS Act, digital tracking linked to mobile-money and payment ecosystems, CCTV and facial-recognition surveillance in public spaces without a governing legal framework, and IMEI/device and network-level monitoring by the Communications Authority and KRA. The centralisation of health data through SHA, biometric registration and digital-identity systems also feature prominently; a reminder that surveillance concern now attaches to civil registration and health infrastructure, not only to the security services.



Figure 13. State surveillance activities of greatest concern (up to three).

Is the DPA adequate against surveillance?

Practitioners do not think the current framework is equal to the problem. A majority say the DPA applies “in principle” but is defeated in practice by the national-security and law-enforcement exemptions; 17 more say state actors simply disregard the law, or that Kenya needs a dedicated surveillance or interception statute. Only 9 consider the DPA, read with Article 31 of the Constitution, adequate.

The professional view is that the exemptions in the DPA and the absence of a bespoke, oversight-anchored interception regime are the weak point.

The telcos

Telecommunications companies occupy an uncomfortable position in practitioners’ analysis.

A majority see them as at least partially complicit in unlawful state access to subscriber data: 17 “genuinely complicit,” 16 “partially complicit” for complying rather than challenging, and 10 “both” highly visible and insufficiently resistant. Only 8 attribute the blame primarily to their visibility. Free-text answers are pointed, referencing a court matter in which a telco acknowledged sharing data to help trace protesters, the government’s shareholding in the dominant operator, and a perceived unwillingness to risk licence revocation by resisting state demands.

What drives public suspicion, in respondents’ view, is the telcos’ position as the most visible intermediary between state and citizen, documented cases of subscriber data shared without court orders, and the absence of transparency reporting.



“Telcos are the first point of connection between illegal surveillance and state abuse of privacy. They are public-facing and routinely comply with illegal requests. There has never been a public announcement by a telco resisting such demands.”

Accordingly, 52 of 62 support a transparency-reporting obligation on telcos, 31 favouring a mandatory statutory duty to disclose the number of government data-access requests received, complied with and contested, and 20 preferring voluntary disclosure with regulatory guidance as a first step. Support for greater transparency is close to unanimous; only the mechanism is contested.

09

SECTION 9

ACTOR RESPONSIBILITY & RISK



Two complementary questions asked respondents to rank who is most responsible for data-governance failures, and to rate the risk each actor poses to individuals. Both point in the same direction: the state, and state-adjacent infrastructure, sit at the centre of Kenya's data-risk map.

Who poses the greatest risk to individuals

On a scale from 1 (low) to 5 (critical), respondents place four actors in high-to-critical territory: the National Police Service and DCI, the National Intelligence Service, the Kenya Revenue Authority and the telcos.

Data brokers and analytics firms and global digital platforms follow. That the KRA, a revenue authority, ranks alongside the security services reflects acute concern about the linkage of tax, financial and communications data. The lowest-rated actors, MSMEs and commercial banks/fintechs, still score above “significant,” underscoring that no actor is regarded as low-risk.



Figure 14. Mean data-governance risk posed to individuals, by actor (1 = Low, 5 = Critical; n = 51).

Who is most responsible

On the forced ranking of responsibility (1 = most responsible), state security agencies rank first (mean 2.06), ahead of the national government's legislating of broad security exemptions with weak oversight (2.26). Notably, the ODPC itself is ranked last on this measure (2.79): respondents locate primary responsibility with the actors doing the processing and the legislature enabling it, not with the regulator even as they call for that regulator to do more.



OSINT, data brokers, essential services and MSMEs

Beyond the headline actors, respondents flag a regulatory vacuum around new intermediaries. On OSINT actors, 39 of those who assessed the question see a significant or critical risk operating in a regulatory vacuum.

On data brokers, 44 say the framework is inadequate, either unenforced against brokers or effectively absent, with only 3 satisfied.

Essential-service providers (KPLC, water utilities, NTSA, county governments) are judged to govern their data “poorly” or “very poorly” by 31 respondents, with particular concern about NTSA data being shared beyond its stated purpose and bulk data-sharing between utilities and tax or security agencies.

The MSME sector is seen as a significant or extremely significant risk by 44 respondents, chiefly the indiscriminate collection of national-ID copies and photographs and the onward sharing of customer lists for marketing and debt collection.

The individual's own role

Practitioners do not absolve individuals: 50 of 62 believe Kenyans contribute to their own data exposure to a large or significant extent.

The behaviours of greatest concern are consenting to app permissions without understanding them, oversharing on social media, and casual sharing of national-ID copies with shops, hotels and other businesses. This supports a public-awareness dimension to DPGSK's mandate alongside its institutional advocacy though respondents are careful to frame individual behaviour as one factor alongside, not instead of, institutional failure.

10

SECTION 10

THE 2027 GENERAL ELECTION: DATA & AI RISKS



The survey's final substantive block turns to the 2027 General Election, and the results are among the starkest in the report. Practitioners regard the coming campaign as a moment of acute data-protection and information-integrity risk, and they want the law to move before, not after, the fact.

The scale of concern

Two-thirds are “extremely concerned” about personal-data misuse during the 2027 campaign, describing it as a critical and immediate threat to electoral integrity. On AI-generated content specifically deep-fake video, synthetic audio, fabricated news and AI-written propaganda, 39 respondents consider the threat “existential” and 17 “very significant,” so that 90% place it in the two most severe categories. Very few respondents took a sanguine view of either risk.

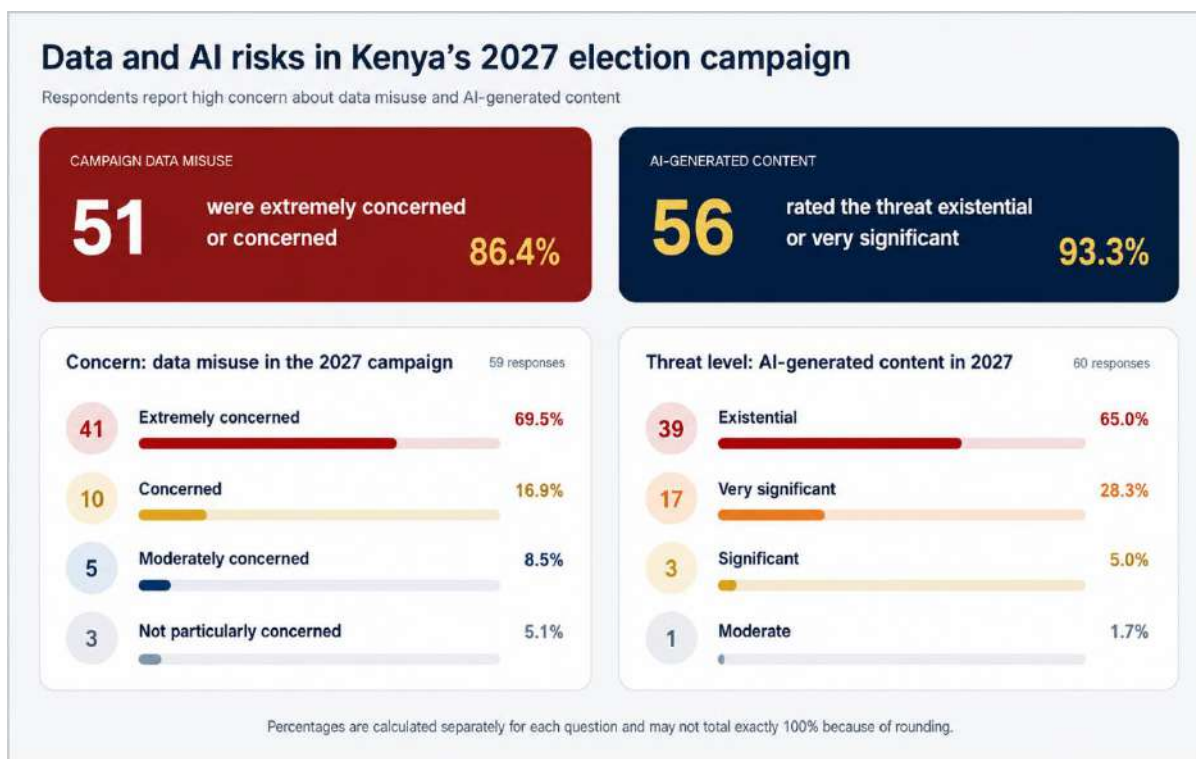


Figure 15. Concern about campaign data misuse (left) and the threat level of AI-generated content (right) in 2027.

Which risks rank highest

On the forced-ranking of electoral risks, the field is tightly bunched, every risk tested is taken seriously but security-agency data collection under the pretext of electoral security and state surveillance of opponents, civil society and journalists edge ahead of even AI deep-fakes and microtargeting.

The AI-specific risks that most concern respondents are deep-fake video fabricating candidate statements, manipulated audio clips, and AI-powered social-media bots engaged in coordinated inauthentic behaviour.

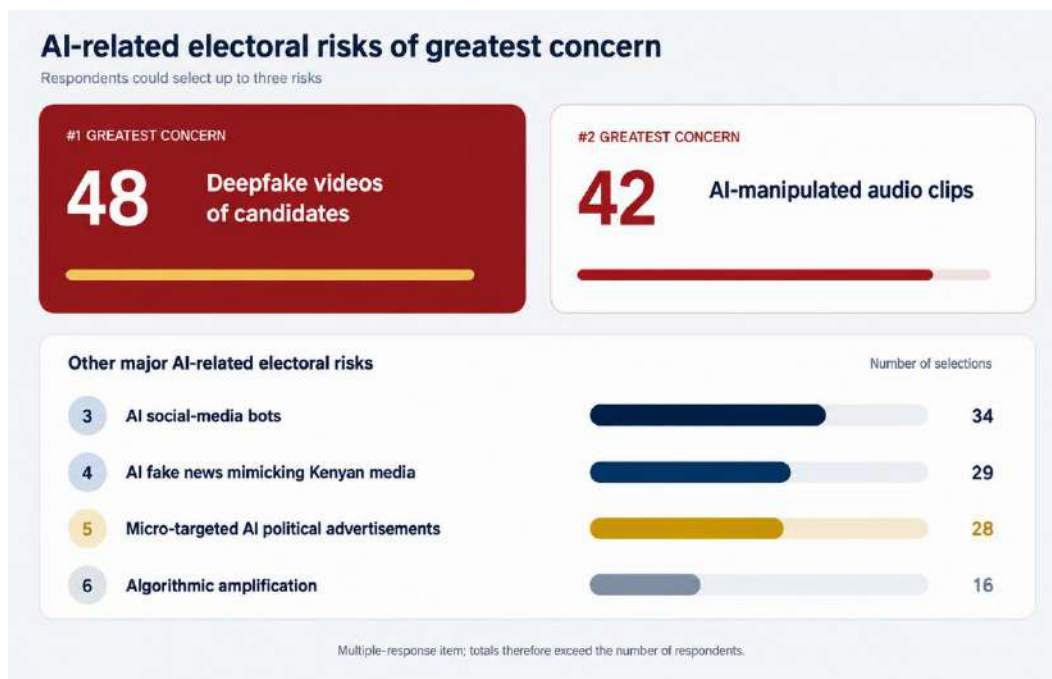


Figure 16. AI-related electoral risks of greatest concern (up to three).

What the profession wants done

The reform appetite is strong and specific. Only 8 of 62 think the current legal framework adequately protects voters' data; 52 see meaningful gaps or an urgent need for a dedicated electoral data-protection framework. Concrete majorities support:

- **Registering political actors as data controllers.** 55 of 62 support requiring political parties, candidates and campaign organisations to register with the ODPC before conducting digital campaign activities (46 favouring full registration).
- **AI-specific electoral legislation.** 53 of 62 want new law before 2027, 24 favour a standalone Electoral AI and Digital Integrity Act, 17 targeted amendments to the Elections Act and DPA, and 11 subsidiary regulations issued jointly by the IEBC, ODPC and Communications Authority.
- **Treating electoral data abuse as an electoral offence.** 55 of 62 agree that unlawful use of personal data in a campaign should carry electoral consequences, potentially candidate disqualification, annulment of a result, or deregistration of a party.

Asked to name the single most important reform the IEBC should undertake, respondents converged on a dedicated electoral data-protection framework, a mandatory DPIA of the voter register and electoral systems well ahead of polling, appointment of a DPO, independent auditing and secure storage of biometric data, and binding rules on microtargeting, cross-border transfers and data-sharing with parties and platforms.

11

SECTION 11

JURISPRUDENCE & ODPC DETERMINATIONS



A discipline matures when its practitioners follow, and are guided by, its case law. On this measure Kenya's data-protection community is well developed. Two-thirds of respondents follow ODPC determinations closely or very closely, and others rely on DPGSK summaries and peer discussion, a direct endorsement of the Society's knowledge-sharing role.

■ Determinations are changing practice

Respondents credit ODPC determinations with real influence: 28 consider them “very significant” in shaping compliance practice, and only a handful dismiss their impact.

More concretely, determinations have changed how practitioners advise and operate: 38 report altered consent-collection and management practices, 21 changed data-sharing or onward-transfer practices, 21 conducted a full compliance review, and 19 changed how they handle data-subject-rights requests. The regulator's adjudicative output, in other words, is doing tangible governance work even where formal penalties are rare.

■ The cases that shape practice

Court decisions are followed almost as closely as determinations, and the free-text answers name a coherent canon of influential Kenyan jurisprudence:

- ***Nubian Rights Forum v Attorney General*** (the Huduma Namba case), by far the most-cited, for establishing that biometric and digital-identity systems require a legal framework and safeguards before large-scale rollout.
- ***Katiba Institute v Communications Authority of Kenya***, cited on device-monitoring and the limits of state access to communications infrastructure.
- ***The LSK v Safaricom / DCI*** petition and related matters, cited repeatedly in connection with subscriber-data disclosure and the tracing of individuals.
- ***Republic v Tools for Humanity*** (the Worldcoin litigation), cited for setting standards on express, freely given consent and on cross-border transfers.
- ***Anampiu v Cleanshelf Supermarkets***, cited as a practical illustration of unlawful processing and CCTV/image misuse in a commercial setting, alongside ODPC compensation awards in the M-Pesa complaints.

The prominence of these matters confirms that litigation and determinations, not only statute now set the operational standard for Kenyan data-protection practice, and that practitioners actively track them.

12

SECTION 12

CONCLUSIONS & RECOMMENDATIONS



The 2026 survey portrays a profession that has found its voice. Practitioners are confident in the importance of their mandate, clear-eyed about where compliance is failing, and united in the conviction that the state is the principal source of data-governance risk in Kenya today. They are asking for three things above all: a firmer legislative footing for AI and surveillance, a more visible and audit-led regulator, and urgent, election-specific rules before 2027. The recommendations below are addressed to the institutions best placed to respond.

FOR THE OFFICE OF THE DATA PROTECTION COMMISSIONER

1. **Lead with audits and named enforcement notices.** Practitioners rank compliance audits and the public naming of data handlers above fines alone.
A visible, predictable audit programme with published outcomes would address the perception of inconsistency more effectively than sporadic penalties.
2. **Prioritise the public sector, health, digital lending and telcos.** These sectors score lowest on compliance and highest on risk and are where respondents most want enforcement focused in 2026–2027.
3. **Issue AI-specific and enforceable guidance.** Given that only a minority accept the DPA as sufficient for AI, the ODPC should issue practical guidance on automated decision-making, profiling and DPIAs for AI, coordinated with the emerging AI legislative framework.

FOR PARLIAMENT AND LAW REFORM

4. **Address the AI gap in the DPA.** Clarify how the Act applies to AI and automated decision-making whether through the AI Bill, 2026 or targeted DPA amendment rather than leaving practitioners to improvise.
5. **Enact an oversight-anchored surveillance/interception regime.** The near-universal concern about surveillance, and the view that the DPA's security exemptions defeat it in practice, point to the need for a bespoke interception statute with independent oversight and judicial authorisation.
6. **Mandate telco transparency reporting.** A statutory duty to publish government data-access requests received, complied with and contested commands broad support and would materially improve accountability at the state–citizen interface.

FOR THE IEBC AND THE 2027 ELECTION

7. **Adopt a dedicated electoral data-protection framework** covering the voter register, biometric data, microtargeting, cross-border transfers and data-sharing with parties and platforms.
8. **Conduct and publish a DPIA of the voter register and electoral systems, and appoint a DPO,** well ahead of polling, with independent auditing and secure storage of biometric data.
9. **Require political actors to register as data controllers** with the ODPC before conducting digital campaigns, and support treating unlawful electoral data use as an electoral offence.

FOR DPGSK AND THE PROFESSION

10. **Build the AI capacity practitioners are asking for.** Deliver practical AI DPIA templates, a structured course on AI ethics and risk, and a CPD session dedicated to the AI Regulation, the top three requested supports alongside a mentorship scheme and comparative-framework resources.



11. **Convene executive and board engagement.** Because management indifference is the leading cause of non-compliance, DPGSK-led CEO and board round tables would target the problem at its source, as respondents themselves proposed.
12. **Formalise and remunerate the expanded DPO role.** Advocate for the DPO title and mandate to be applied where the function is already performed informally, and for AI-governance responsibilities to be recognised in remuneration.
13. **Sustain the knowledge-sharing role.** Practitioners rely on DPGSK summaries of determinations and jurisprudence; expanding this service and public-awareness work on everyday data hygiene directly serves the community's needs.

“This report was prepared for the Data Privacy and Governance Society of Kenya from 62 professional responses collected between 5 June and 31 July 2026. Figures are drawn directly from the survey dataset; percentages are of those answering each question, and rating scale means exclude “not applicable” responses.”

🌐: www.dataprivacyke.africa

✉: info@dataprivacyke.africa

📷 Instagram: @DPGSK_Ke

✂: @DPGSK_Ke

🌐 LinkedIn: Data Governance Pros Kenya