DPGSK
Data Privacy and Governance Society of Kenya

Review of 2025 ODPC determinations

An analysis of determinations made by the Office of the Data Protection Commissioner (ODPC) in 2025

January 2026

In this report

Foreword

The 2025 determinations reflect a maturing data-protection enforcement environment in Kenya. While complaints continue to rise across sectors, the nature of the findings shows a shift by the Office of the Data Protection Commissioner (ODPC) from foundational compliance concerns toward structured remedies, monetary compensation, and, in some instances, referrals for prosecution.

Most complaints continue to arise from three recurring failures: the absence or poor recording of consent, inadequate information provided to data subjects at the point of collection, and the failure to honour erasure or objection requests. These issues cut across digital lending, education, telecommunications, marketing, retail, and digital media. The finance and digital-lending sector remain the highest-risk cluster, largely due to the widespread use of third-party agents and weak controls over downstream data use for marketing and debt-collection activities.

Viewed against enforcement trends from ODPC's inception in 2020 through to 2025, the trajectory is clear. Early enforcement focused on registration, privacy notices, and baseline compliance. By 2024 and into 2025, determinations increasingly emphasise accountability, enforcement notices, and compensation. This report captures those shifts and offers practical insights for organisations, practitioners, and policymakers seeking to strengthen compliance and data-governance practices.

Dr. Mugambi Laibuta, PhD, CIPM
Chairperson, DPGSK

Acknowledgement

The completion of this report was made possible through the time, commitment, and thoughtful contributions of volunteers drawn from the DPGSK community. Their collective effort, careful analysis, and willingness to engage deeply with the subject matter shaped the quality and depth of this work.

DPGSK extends its sincere appreciation to all who worked on this project. This report was compiled by Hawi Alot, Shanice Naisenya, and Maria Nambuya. It was edited by Grace Mutung'u. Data collection, coding and analysis was done by Esther Adwets, Abigail Sami W., Tess Wanjiku, Jully Kamollo, Harmony Wairimu Maina and Doris Matu.

DPGSK further appreciates the broader DPGSK membership for their ongoing engagement, dialogue, and shared commitment to advancing data protection awareness and culture in Kenya. Your support continues to strengthen and inform our collective work.

About DPGSK

The Data Privacy and Governance Society of Kenya (DPGSK) is a professional organisation dedicated to advancing awareness, compliance, and governance in data protection and privacy. Registered under the Societies Act, DPGSK champions the implementation and enforcement of the Data Protection Act, 2019 through research, capacity building, and stakeholder engagement.

Key contributions and activities include:

- **Advancing Professional Standards**: DPGSK builds networks of professionals, facilitates continuous development and certification, and sets ethical and professional benchmarks.

- **Fostering Collaboration**: The Society collaborates with regulators, public sector, private sector, plus regional and international societies to enhance knowledge sharing and improve compliance mechanisms.

- **Policy Advocacy**: DPGSK champions policy and legislative reforms, strategic litigation, and public awareness campaigns to shape a robust data protection ecosystem.

- **Mentorship and Outreach**: By providing guidance and mentorship to members, the society creates an engaging community that drives leadership in data governance issues.

- **Support for Enforcemen**t: DPGSK engages in promoting adherence to the Data Protection Act through capacity-building programs aimed at compliance.

The Society's membership includes members from public sector, private sector, civil society, academia, and university students. DPGSK offers membership categories tailored to meet individual and organizational needs. DPGSK's commitment to inclusivity and excellence drives its mission of shaping a responsible digital future for Kenya by addressing challenges in data protection and fostering accountability.

Executive Summary

This report presents an in-depth analysis of 96 complaints determined by ODPC of the Data Protection Commissioner (ODPC) in 2025. The figure represents almost double the number reviewed in 2024 (DPGSK Analysis of ODPC Cases, 2024).The increase reflects growing public awareness of data protection rights and a more assertive, visible ODPC exercising its mandate under the Data Protection Act, 2019 (DPA). The report examines enforcement trends, sectoral risks, and legal developments, and compares 2025 outcomes with determinations from previous years to assess the maturity of Kenya's data protection regime.

The report evaluates how data protection enforcement is evolving in Kenya and identifies systemic compliance gaps to inform policy, regulatory, and corporate decision-making. It uses qualitative legal analysis to identify recurring issues, enforcement approaches, remedies, and sectoral patterns. Comparative references to determinations from 2024 and earlier years provide context on enforcement trajectory and institutional development.

2025 marks a shift from foundational compliance to structured enforcement

Compared to previous years, 2025 marks a shift from foundational compliance to structured enforcement. While 2024 saw increased use of enforcement notices and early compensation awards, 2025 determinations demonstrate:

- A stricter and consistently applied standard for express consent, decisively rejecting implied or informal consent.
- More instances of enforcement of data subject rights, particularly regarding procedure, timelines, and obstruction.
- Escalation of consequences for non-cooperation, including explicit recommendations for prosecution of company directors.
- Cross-border regulatory cooperation, notably between Kenya's ODPC and Uganda's Personal Data Protection Office, establishing a practical model for handling multinational data breaches.

At the same time, the nature of complaints remains comparable to previous years, with recurring failures around consent, transparency, and rights requests continuing across sectors.

The 2025 determinations reflect a maturing enforcement environment characterised by:

- Stricter consent requirements, with the burden of proof resting entirely on data controllers and consent treated as dynamic rather than one-time.
- Stronger enforcement of data subject rights (DSRs), including the non-discretionary right to be informed and the absolute right to object to direct marketing.
- Expanded controller accountability, including liability for actions of agents and processors and application of a proportionality test when relying on legitimate interest.
- Clearer consequences for obstruction, with regulatory defiance treated as a serious offense rather than a procedural lapse.
- Clarification on remedies, confirming that compensation under the Data Protection Act addresses infringement of data protection rights and associated distress, not broader economic losses.

Complaints were most prevalent in the finance and digital lending sector, followed by telecoms, education, marketing, retail, and digital media. Persistent risks stem from poor consent management, inadequate transparency at data collection, and failure to honor erasure or objection requests.

The largest category of complaints in 2025 relates to digital lending and the broader financial technology sector, accounting for nearly a third of all cases.

The largest category of complaints in 2025 relates to digital lending and the broader financial technology sector, accounting for nearly a third of all cases. These frequently involve the repurposing of borrowers' data for unauthorized uses, often in the context of aggressive debt-recovery practices.

Notably, this increase has occurred despite the issuance of sector-specific guidance by ODPC, suggesting the need for further engagement between ODPC and the sector to ensure compliance.

The second major category concerns the unauthorized use of images for commercial or promotional activities, frequently tied to marketing, media, hospitality, and SME-driven businesses, where there tends to be unclear documentation of consent. Unsolicited marketing and spam cases, while smaller in number, continue to reflect a gap in understanding around consent, withdrawal mechanisms, and opt-out obligations, as well as proper implementation and governance.

Data Subject Request (DSR) failures form another significant cluster. The failures frequently resulted from excessive documentation, imposed procedural barriers, and failure to adhere to statutory timelines, signalling a recurring difficulty in operationalizing transparency, access, accuracy, and erasure obligations.

Finally, several complaints reflected unauthorized disclosures, including emails exposing sensitive information, improper sharing of customer details with third parties, and disclosures to employers or unrelated recipients. These cases demonstrate the need for organizations to strengthen internal governance frameworks, particularly those linked to the newly issued Data Sharing Code.

complaints reflected unauthorized disclosures, including emails exposing sensitive information, improper sharing of customer details with third parties, and disclosures to employers or unrelated recipients

Together, these categories reveal a maturing but uneven compliance environment. Awareness among data subjects continues to rise, and ODPC's 2025 guidance notes appear well-targeted to address the most prevalent issues, yet their impact will ultimately depend on the extent to which organizations embed these standards into operational practice.

Improving compliance in the most affected sectors requires sustained operational investment rather than regulatory awareness alone. This signifies the need for organizations to move beyond basic sensitization into data protection operationalization through data protection and governance frameworks.

The report recommends strengthening regulatory capacity, issuing sector-specific compliance guidance, formalizing regional cooperation mechanisms, improving oversight of agents and processors, and enhancing public and corporate awareness of data protection obligations.

Overall, 2025 represents a turning point in Kenya's data protection enforcement. ODPC has moved decisively from awareness-building to accountability, signaling that non-compliance now carries tangible legal, financial, and reputational consequences.

1.0 Introduction

The aim of this analysis is to trace how Kenya's data protection environment has evolved six years after the enactment of the Data Protection Act, 2019 and five years since the establishment of ODPC. We analyse the nature of complaints, enforcement outcomes, timelines, sectoral behaviour, and the interaction between data subjects, data controllers, and the regulator, and present a grounded view of Kenya's data protection ecosystem. The report serves as a tool for understanding how to manage data protection within Kenyan organisations. It is aimed at helping data protection professionals, compliance departments, as well as business entities to protect privacy and data rights in Kenya's ever evolving digital space.

The analysis serves several key objectives:

- To illustrate the practical application of the Data Protection Act of 2019. By a range of complaints and rulings, the analysis provides concrete examples of how DPA is interpreted and enforced.
- To highlight consistent patterns in rulings, particularly concerning unauthorized data use. The focus is on identifying trends in decisions related to issues like consent for commercial use of images and direct marketing.
- To identify inconsistencies or deviations from these patterns. The analysis seeks to explain why certain complaints might have different outcomes despite seemingly similar facts, shedding light on the nuances of applying data protection principles.
- To showcase ODPC's role in safeguarding data subject rights and promoting responsible data handling practices. The analysis aims to demonstrate the impact of ODPC's enforcement activities in upholding individual privacy.

A key focus of this report is the impact of ODPC's regulatory efforts, including the nine sector-specific guidelines issued in the past year these were:

1. Guidance Notes for Public Sector
2. Guidance Notes on Processing by MSMEs
3. Guidance Notes for Journalistic Purpose
4. Guidance Notes - Processing for Research Purpose
5. Guidance Notes for Processing on Publications of Recorded Media
6. Guidance Notes for Processing Children's Data
7. Guidance Notes on Biometric Data
8. Guidance Notes on Historical and Statistical Purposes
9. Data Sharing Code

The analysis evaluates whether these guidelines have influenced compliance behaviour, reduced sector-specific breaches, or clarified obligations for organizations operating in regulated industries. This comparison between the 2024 and 2025 datasets helps illustrate where improvements have taken hold, where gaps persist, and how awareness and enforcement have shifted across sectors.

Scope

This analysis encompasses 96 distinct complaints admitted by ODPC in 2025. Broadly, the complaints cut across both private and public sector actors including, telecommunications, insurance, education, healthcare, employment and recruitment, utilities, marketing and debt recovery services, as well as government and intergovernmental bodies, with the most recurrent sectors being financial services (including banks and digital lenders).

The complaints reveal a marked shift in the regulatory posture of ODPC in 2025, characterised by deeper scrutiny of systemic processing failures rather than isolated incidents, stricter evidentiary standards placed on data controllers, and a heightened emphasis on accountability across the entire data processing chain, including agents, affiliates, and cross-border partners. Notably, this approach extended beyond corporate entities, with at least one determination resulting in sanctions against a natural person, underscoring ODPC's willingness to impose personal accountability where individual conduct meets the threshold for enforcement. A significant number of complaints arose from routine operational activities such as customer onboarding, employee data transfers, billing notifications, marketing communications, and security surveillance demonstrating that compliance risks increasingly lie in everyday processes rather than exceptional events.

complaints reveal a marked shift in the regulatory posture of ODPC in 2025, characterised by deeper scrutiny of systemic processing failures rather than isolated incidents,

Several themes emerge as particularly striking in the 2025 determinations. These include the operationalisation of cross-border regulatory cooperation, especially within the East African region; the elevation of express consent as an ongoing legal standard; more assertive enforcement of data subject rights, particularly the rights to be informed, to object, and to rectification; and a clear intolerance for administrative obstruction or procedural delay by regulated entities.

Taken together, the 2025 complaints illustrate a maturing enforcement environment in which data protection compliance is treated as an organisational governance issue rather than a technical one time (check-box) obligation. The scope of this analysis therefore extends beyond individual outcomes to examine sector-wide patterns, regulatory expectations, and emerging risk areas that are likely to shape compliance obligations and enforcement trends in the years ahead.

2.0 Methodology

Scoping

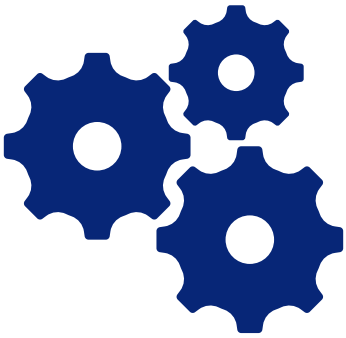
This report is based on an analysis of ninety-six (96) complaints formally determined by the Office of the Data Protection Commissioner (ODPC) during the 2025 calendar year. The analysis employed a qualitative review of each determination. Complaints were examined and categorized based on the date of the determination, the respondent's sector, the nature of the alleged data protection violation, the issues for determination and the remedies granted. A Comparative analysis was conducted to assess how enforcement practices, legal reasoning, and remedies in 2025 differ from those observed in earlier years, particularly 2024.

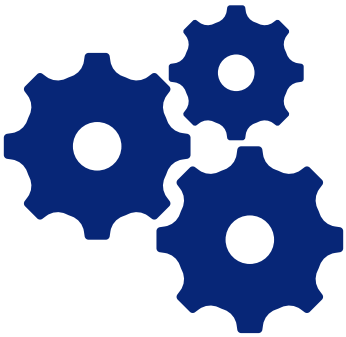
The report also involved an analysis of appellate proceedings arising from ODPC determinations. The report reviews fifteen (15) appeals and judicial review matters filed before the High Court during the 2025 reporting period, arising from ODPC determinations issued in both 2024 and 2025. This appellate review was undertaken to assess the sustainability of ODPC decisions on appeal, judicial treatment of ODPC's mandate and enforcement powers, and emerging jurisprudence on procedural fairness, proportionality, and administrative action under the Data

Data Collection

This report analyzed all determinations from the year 2025. Researchers collated the complaints from ODPC website and cross-referenced published determinations with supplementary public reports or legal updates from ODPC. They then coded the data and categorised by sector, type of complaint, and outcome. They also linked complaints to regulatory developments such as sector- guidance notes issued by ODPC as well as laws and actions from other regulators such as the Central Bank of Kenya. Only complaints that had been fully determined and documented on the website of ODPC were analysed.

Appellate decisions were sourced separately from the Kenya Law website. Appeals and judicial review matters were identified through reported decisions referencing ODPC determinations. These appellate materials were reviewed to extract information on the identity of appellants, grounds of challenge, procedural posture, and the outcome of each matter.





Analysis

The report incorporates quantitative, qualitative and comparative analysis. Qualitative analysis involved reviewing the determinations published on ODPC's website to identify recurring data protection issues, legal principles applied and trends in complaints. Quantitative analysis provides a statistical examination of the determinations by sector, recurring data protection concerns, and outcomes of complaints.

A comparative analysis of decisions involving the public sector and private sector was conducted to examine the level of scrutiny compared to the private sector. The analysis also incorporates a review of sector-specific regulatory guidance issued by ODPC during the year. In particular, the report examines the impact of the sector-specific guidelines released in the past year and evaluates the extent to which ODPC's regulatory guidance has informed compliance standards, influenced enforcement decisions, and contributed to greater clarity and consistency in the application of the Data Protection Act, 2019 across different sectors.

Limitations

The report is subject to the limitations that should be considered when interpreting its findings:

- The analysis was conducted through a human-led review process and is therefore inherently susceptible to human error, including possible inaccuracies in classification, interpretation, or data extraction from the source material.
- The report is limited to matters formally determined and published on ODPC portal. Complaints resolved through Alternative Dispute Resolution (ADR) or other informal mechanisms are not publicly disclosed and are therefore excluded from this analysis. As a result, the findings may not fully reflect the total volume or full range of data protection disputes handled by ODPC during the period under review.
- Matters that were withdrawn, discontinued, or otherwise not concluded through formal determination are also excluded, as such outcomes are similarly not shared on ODPC platform. Consequently, the trends and patterns identified in this report represent only a subset of all complaints received and handled by ODPC in 2025.
- The appellate analysis is limited to decisions reported on the Kenya Law website. Appeals that were filed but not yet determined or not publicly reported are not captured. As a result, the trends and patterns identified in this report represent only a subset of all complaints and appeals arising during the 2025 reporting period.

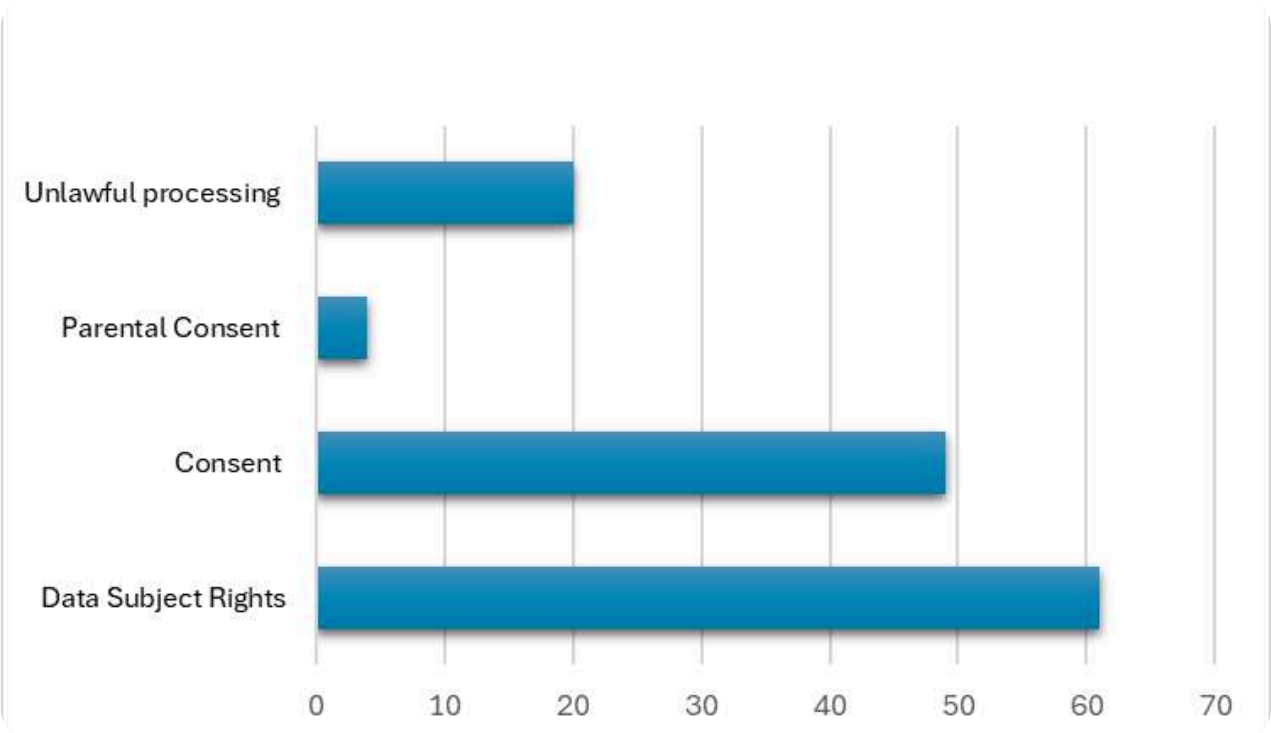
3.0 Findings

The main areas of non-compliance that led to the majority of complaints and enforcement action include the widespread use of implied or verbal consent, which falls short of the legal requirement for express, informed, and specific consent under DPA. Many entities engaged in unsolicited direct marketing through persistent promotional SMS and calls, often ignoring opt-out requests.

A significant number of breaches arose from the unregulated use of third-party agents, including sales representatives, debt collectrs, and call-centre partners, who processed or disclosed personal data without proper oversight or a lawful basis. High-volume or automated communication systems requently resulted in continued messaging despite objections, failures to act on erasure requests, or the contacting of individuals who were not customers.

Several entities also engaged in excessive or unnecessary data collection, such as demanding MPESA statements unrelated to the stated purpose, contravening the principle of data minimization. Unlawful disclosures of personal or financial information to employers, relatives, guarantors, or agents were also prevalent. Finally, many entities also failed to respect the right to object to processing, particularly in the context of direct marketing, despite this right being absolute under DPA.

3.1 Types of complaints



3.1.1 Unlawful Processing

There were 21 complaints involving unlawful processing, which referred to situations where the data controller had no authority at all to collect or process the personal data not even under a misconstrued basis.

In ***Mwikali Nzyoka v Kenya Women Microfinance Bank, Family Bank & Co-operative Bank***, one institution admitted to obtaining the complainant's personal data through "market intelligence" for a loan-takeover promotion. ODPC found that this amounted to unauthorized data collection and processing, as no lawful basis or consent existed.

> ...admission that they acquired the Complainant's data through "market intelligence".....without the Complainant's consent constitutes strong evidence of unautorised data processing

Another illustration is E***ric Munene Njuguna v Chapeo Capital Limited (ZK Pesa) & Ericson Lubale Okota***. The complainant discovered he had been listed as a loan guarantor without his knowledge. The second respondent had disclosed his personal data to the lender without verifying its accuracy or obtaining consent. ODPC found that this disclosure constituted an offence under section 72 of DPA and recommended prosecution of the second respondent.

3.1.2 Consent

There were 53 complaints where the primary issue was failure to obtain explicit consent before processing personal data.

The most significant case was ***Chizzy Taabu Orwa, Shelmith Nyawira Gitonga & Stanley Kinyua Wachira v Mast Jägermeister SE,*** which resulted in the highest fine of the year (KES 1,500,000). The organisation argued that it displayed large disclaimer notices at events in both English and Swahili informing attendees that photographs could be taken. They further argued that by entering the event and posing for photos, participants gave implied consent. ODPC rejected this position. It held that disclaimer notices, no matter how prominently displayed, do not amount to express consent for processing personal data for commercial purposes. ODPC clarified that such notices serve only as general information and cannot replace the clear, affirmative action required by DPA.

3.1.3 Parental Consent

Out of the 53 consent cases, 4 involved minors and were treated as a distinct category due to the heightened protections afforded to children.

A key determination was in ***Hilda Musimbi Anyama (on behalf of Minor L.K.) v Friends School Keveye Girls High School***. The Deputy Principal recorded the minor performing a punishment and later posted the video on social media, where it went viral. The complainant acknowledged the punishment itself was not in dispute but argued that the school had no authority to record and publish the minor's image.

ODPC found violations of the transparency principle, as the minor was not informed that the video would be taken or shared. It also held that the necessity principle was breached because the data collected was neither limited nor proportionate to the intended purpose. Under section 33, which protects the rights of children, ODPC noted that the school could have addressed the matter without revealing the student's identity. In this case, even consent would not have cured the violation.

Other complaints in this category involved unauthorized use of minors' images for commercial purposes, raising broader questions about who should receive compensation from the parent or the minor, especially where the parent is the one lodging the complaint.

3.1.4 Data subject rights

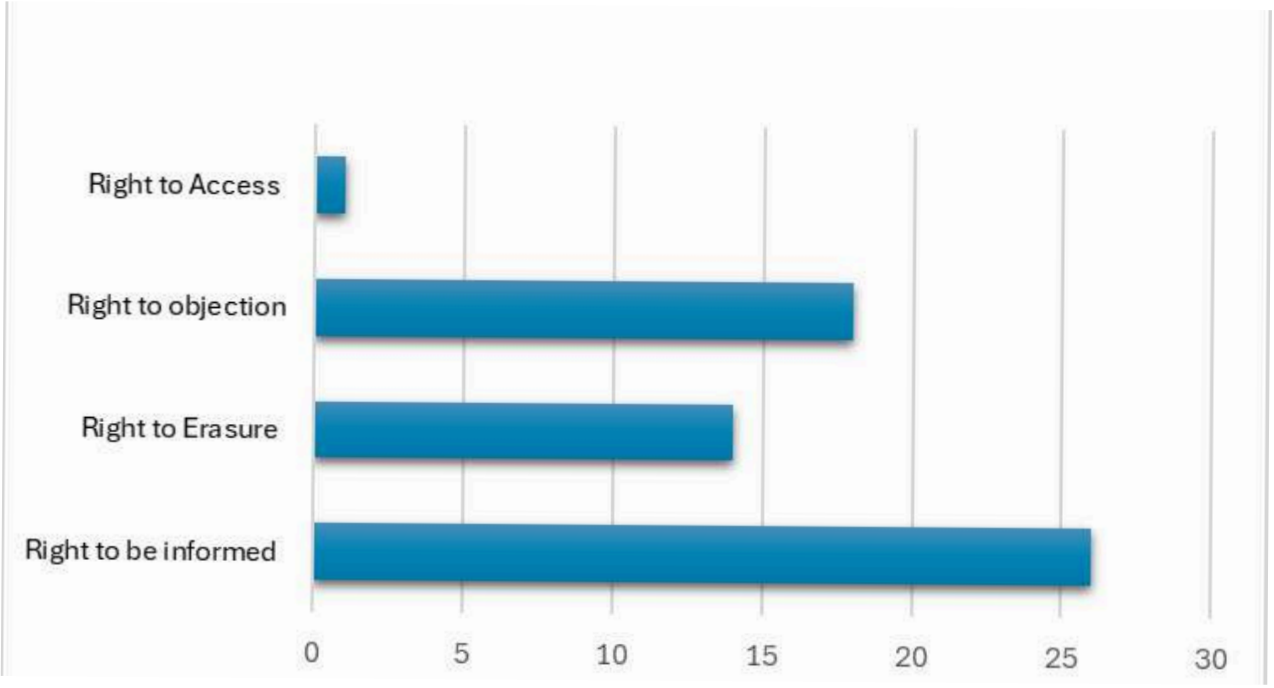
Complaints relating to the exercise of data subject rights formed the largest category, with 61 cases recorded. The most common issue was failure by data controllers to meet their obligations under DPA, especially where individuals attempted to enforce their rights but organizations either ignored the requests or handled them poorly.

For example in ***Yasin Abukar v Wananchi Group (Kenya) Limited T/A Zuku Fibre Kenya*** the complainant, a former customer of the respondent, alleged that the respondent continued to process and retain his personal data long after he had terminated their services. The complainant attempted to exercise his rights under the Data Protection Act, 2019, using the channels provided by the respondent, including the designated email address. However, these channels were defective, preventing him from effectively submitting his requests. Despite multiple follow-ups via telephone and other communications, the respondent failed to comply and continued sending promotional messages. Consequently, ODPC imposed a compensation order of KSh 500,000 payable to the complainant and directed the respondent to immediately delete his personal data, with proof of compliance to be submitted within seven days.

complaints relating to the exercise of data subject rights formed the largest category, with 61 cases recorded.

Similarly in ***Philip Bolo v Platinum Credit Limited,*** the complainant received unsolicited promotional calls and messages despite explicitly requesting their cessation via email and telephone. ODPC found that the communications were linked to the respondent, rejecting claims of third-party impersonation, and emphasized that under Section 36 of the DPA, the right to object to processing for direct marketing purposes is absolute. The respondent was therefore ordered to pay KSh 900,000 in compensation.

This pattern of non-compliance was also evident in ***Abraham Owen Guumba Otieno vs. 360 Degrees Court Apartment Resident Association*** where the complainant repeatedly requested, through text and phone calls, that unsolicited emails be stopped and that his data be removed from the mailing list. ODPC found that the respondent failed to update its records following a change of ownership, thereby continuing to process inaccurate personal data.



Right to be informed (27 complaints)

These complaints arose where data controllers collected personal data in unclear or ambiguous ways. In several cases, organizations collected data for one stated purpose, but later repurposed it or disclosed it to third parties without informing the data subjects. This included instances where organizations appeared to shift their intended purposes mid-way, treating the collected data as available for broader use without obtaining fresh consent or meeting lawful basis requirements.

Right to erasure (14 complaints)

These cases often involved continued communication despite opt-out requests. A common pattern was where customers on mailing or SMS marketing lists asked to stop receiving promotional messages, but the organization continued to send them. This frequently pointed to weak governance structures, inadequate internal workflows for handling data subject requests, or outdated systems.

A significant portion of these complaints came from the digital lending sector, where individuals were listed as guarantors for loans without their knowledge. Once the borrower defaulted, the individuals were aggressively contacted and, when they requested that the harassment stop, the callers became even more hostile. These cases highlighted both unlawful processing and failure to honour deletion and objection rights.

Right to object (19 complaints)

Most complaints involved persistent direct marketing even after the individual had sent a "STOP" message or otherwise objected. ODPC has repeatedly stressed that the right to object to processing for direct marketing is absolute. This position was reinforced in ***Cherry Fiona Mwendwa v Acceler Global Logistics,*** where ODPC emphasized that once an objection is raised, the controller must cease processing immediately.

Right of access (1 complaint)

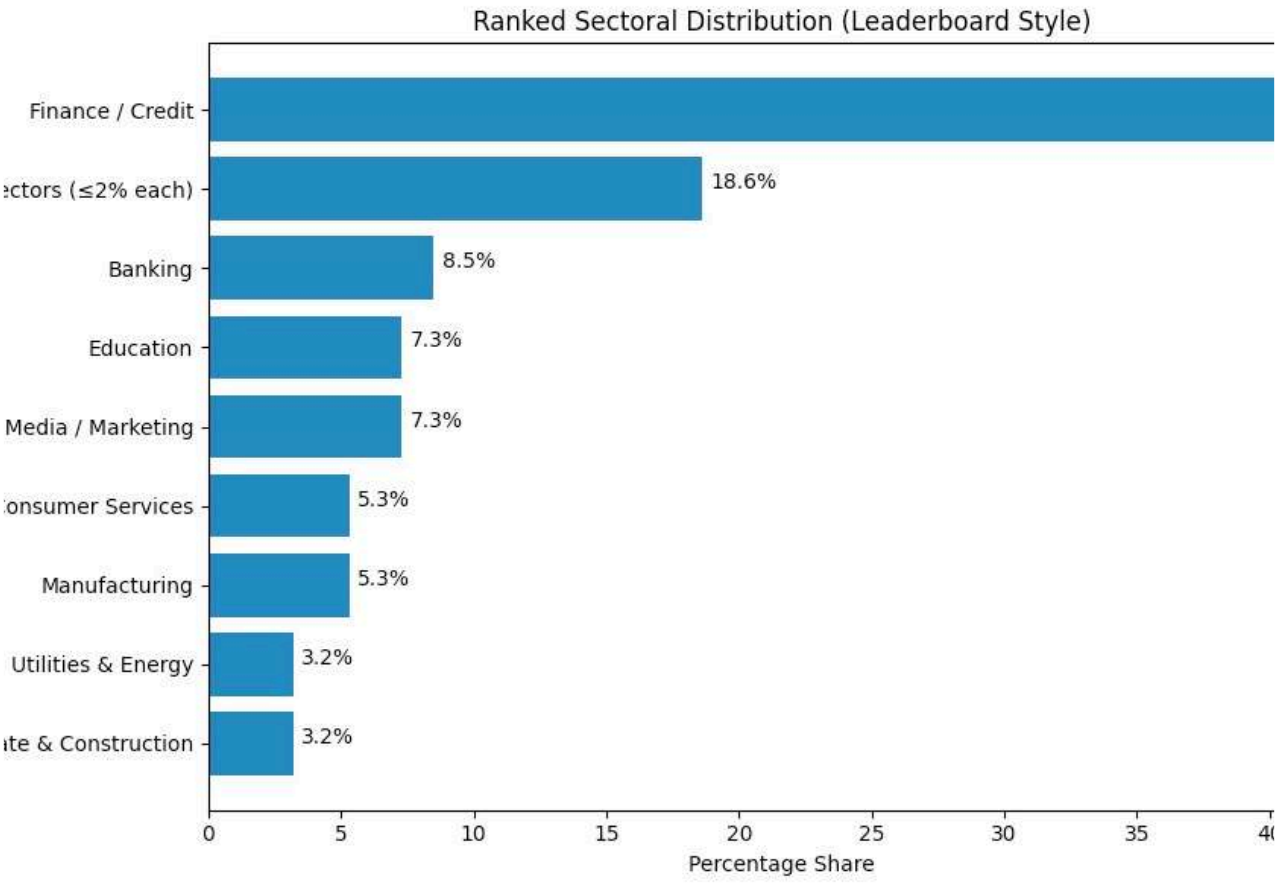
A single complaint related to failure to grant access to personal data, mirroring the first ODPC case of this kind several years ago. In ***Margaret Nzula v United Winners DT SACCO & Shirika DT SACCO***, the complainant applied for a job, was shortlisted, then rejected after her previous employer issued an adverse report about her. When she requested access to the report, the employer refused to provide it, leading to a clear violation of her right to access.

Right to correction/rectification (2 complaints)

One case that stood out involved a public entity: ***Elias Cheruiyot Korir v Thika Water and Sewerage Company.*** The complainant kept receiving billing messages meant for a deceased third party, whose phone number had been reassigned to him. Despite multiple requests, the company failed to update its records, resulting in recurring messages that could have been resolved through simple correction of inaccurate data.

3.2 Complaints by sector

Finance and credit institutions, including microfinance entities, digital lenders, and SACCOs accounted for the largest share of ODPC penalties. They were followed closely by entities in the digital media and marketing sectors, particularly those engaged in advertising, promotions, and public relations, which also attracted significant fines. The finance and credit sector remains the most data-intensive, as these institutions handle large volumes of sensitive personal information in the course of offering and managing financial services. This deep reliance on personal data creates numerous points of vulnerability and increases the likelihood of breaches when safeguards, consent mechanisms, or oversight processes are inadequate.



Other sectors recorded fewer complaints largely because their data processing activities are narrower and less sensitive, though breaches still occurred in predictable patterns. Retail and hospitality entities were mainly cited for using customer images without consent and sending marketing messages without providing an opt-out.

In the education sector, most complaints involved the misuse of minors' images, failures to obtain parental consent, and broader transparency lapses. Digital media and photography organizations were frequently implicated for the commercial use of images without clear, recorded consent. Utilities and real estate players attracted complaints for CCTV over-reach, unlawful disclosure of tenant data, and weak internal access controls, while non-profit and ICT entities struggled with governance gaps, accidental disclosures, and inadequate security safeguards. These variations reflect cross-sector themes: persistent reliance on implied rather than express consent, insufficient privacy notices, unlawful direct marketing, frequent disclosures to inappropriate third parties, excessive data collection, and poor oversight of agents and processors. Strengthening compliance, therefore, requires sector-specific measures, including proper consent documentation, visible privacy notices, lawful CCTV deployment, de-identification of minors, clear contractual terms for image use, automated opt-out mechanisms, regular audits, and tighter supervision of third-party actors.

Digital media and photography organizations were frequently implicated for the commercial use of images without clear, recorded consent

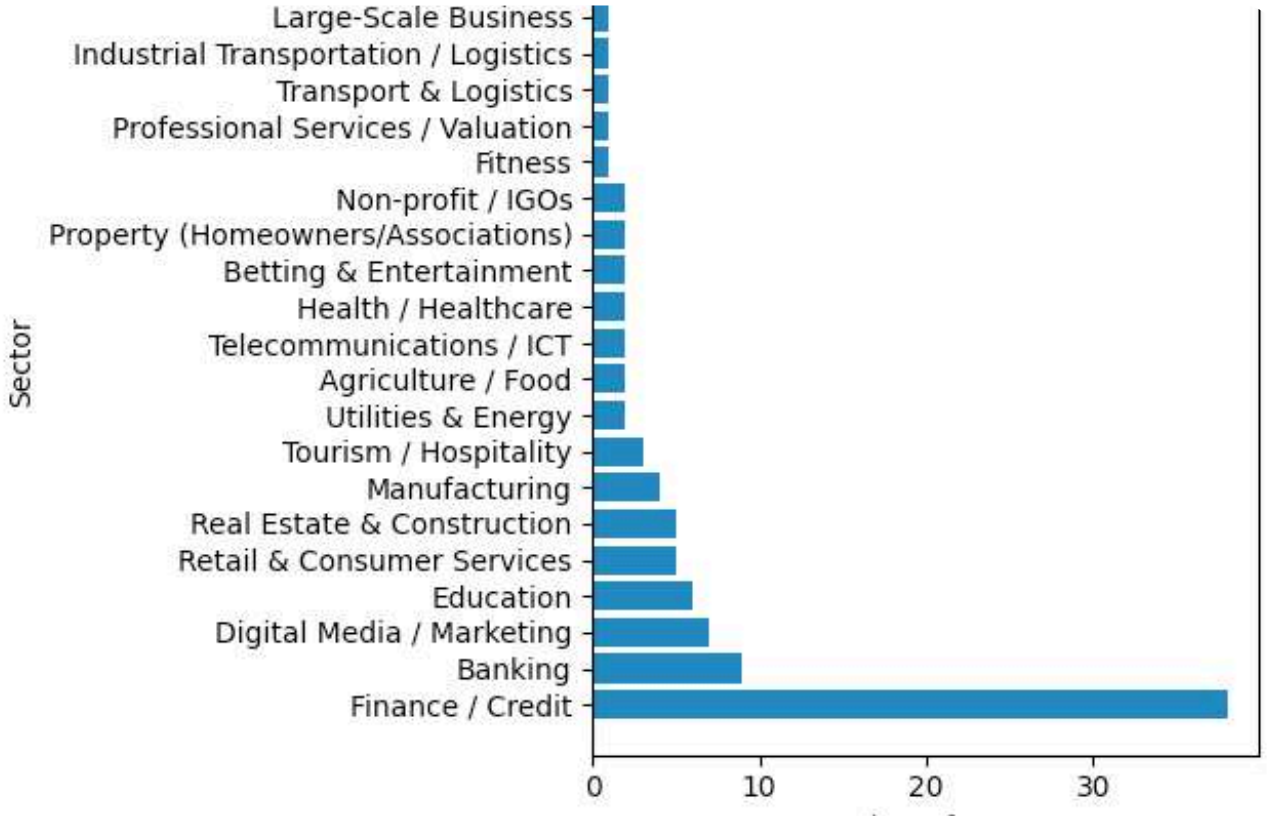
Overall, the pattern of complaints demonstrates that while all sectors face data protection risks, the severity and frequency of breaches correlate directly with the volume, sensitivity, and complexity of the personal data they handle. Finance and credit institutions remain the most exposed, but the issues seen across retail, education, digital media, utilities, real estate, and non-profit entities reflect common shortcomings in consent practices, transparency, and accountability. Strengthening compliance will therefore require a deliberate shift toward clearer consent mechanisms, better communication with data subjects, improved internal controls, and tighter oversight of third-party processors. As ODPC's decisions become more defined and consistent, entities that handle personal data responsibly and transparently will face fewer regulatory issues and are more likely to retain the trust of the people they serve.

3.3 Penalty types

Out of the 96 cases, 82 resulted in fines and compensation awards, 35 of the cases resulted in enforcement notices, and 8 were dismissed for lack of evidence. There were no cases resolved by alternative dispute resolution.

3.3.1 Fines

Of the 96 complaints, 76 were fined, representing about 83% of cases penalised. The Finance/Credit sector was most fined, making up about 40% of cases (38/96). Banking, Digital Media, and Education are the next most frequent sectors.



The average fine is approximately Ksh. 324,000, reflecting a balance between punitive and corrective intent.The lowest fines were around Ksh. 20,000–50,000, mostly in minor Finance/Credit or Banking sector cases, which may suggest leniency for lower-risk or first-time infractions.The highest fines were Ksh. 1,500,000, applied in cases with multiple complainants or high-impact violations, signaling ODPC's willingness to impose strong deterrents for serious or systemic breaches.

The penalty approach is tiered and proportional, favoring moderate fines for routine breaches but escalating sharply for serious, repeated, or high-impact violations, balancing deterrence with fairness.

Compensation award (Ksh)	Sector
1,500,000	Digital Media / Marketing (Alcoholic Beverages) & Betting/Entertainment
900,000	Finance/Credit (Platinum Credit)
750,000	Tourism/Hospitality (Hotel Tobriana)
700,000	Education (DMI Education Services Manufacturing (Hair Manufacturing)
700,000	Telecommunications (Liquid Telecom Education (St. Joseph International Science School)

3.3.2 Compensation awards

Compensation awards varied widely, with common awards ranging from KES 200,00–1,500,000, with multiple higher awards where commercial misuse of images or persistent non-compliance occurred. ODPC increasingly uses compensation (not just administrative penalties) to remedy privacy harms especially where the breach is commercial or persistent.

The largest total monetary award in 2025 was KES 1,500,000, issued in cases involving the unlawful use of images for commercial promotions. These matters ***Chizzy Taabu Orwa & Others v Mast Jägermeister SE*** *and* ***Patrick Matasi, Kenneth Muguna & Austine Odhiambo v Betnare*** involved multiple complainants whose images were used in marketing without their express consent. In both cases, ODPC found that the respondents relied on misplaced assumptions about implied consent. The use of publicly accessible or event-related images did not remove the need for express consent for commercial exploitation. Each complainant was awarded KES 500,000, leading to the higher overall figure because of the number of individuals affected.

Where only a single complainant was involved, the highest award in 2025 was Ksh. **900,000** in ***Philip Bolo v Platinum Credit Limited***. The case involved persistent unsolicited marketing calls and messages sent through an agent whose actions the respondent could not sufficiently account for. ODPC held the company responsible for failing to demonstrate proper oversight, a valid data processing arrangement, or a lawful basis for direct marketing. The award reflects two aggravating factors: ongoing intrusion and the violation of the absolute right to object to direct marketing.

The lowest fine was Ksh. 20,000 in ***Eric Mutune Mwamwee v Rosky Credit Limited.*** Although ODPC confirmed that the respondent breached the duty to inform at the point of collection, the penalty was reduced significantly due to several mitigating factors: the processing occurred once, was not recurrent, did not involve profiling or commercial exploitation, and caused no tangible harm. These circumstances explain why ODPC issued a lower penalty even though the complainant had sought KES 400,000 in compensation.

Top sectors that from where compensation was awarded were as follows:

Sector	Number of compensation awards
Finance/Credit	34
Banking	9
digital media/marketing	6
education	6

3.3.3 Enforcement Notices

Enforcement notices are orders from the Data Commissioner to a non-compliant data controller/processor, directing for specific actions to fix a data breach or non-compliance within a given timeframe. There were 13 such orders in 2025. The sectors that received enforcement notices include:

sector	entities
Finance/Credit	Quest Holding, Betika, Chapeo Capital, Incredo Finance
Utilities & Energy	Thika Water and Sewerage
Health	AGC Tenwek Hospital
Telecommunications	Liquid Telecom
Banking	Diamond Trust Bank

In most cases, ODPC issued an enforcement notice to compel deletion, proof of erasure, cessation of communications and remedial steps. This was mostly seen where the data controller failed to respond to a data subject request, especially a request to cease and desist.

3.3.4 Cases dismissed

7 out of the 96 cases were dismissed for lack of evidence/merit. These include: Martin Gikonyo vs. Kingdom Bank Limited; Rebecca Atieno Odock & Brenda Achieng vs. Jackline Wanjiru; Ruth Murugu Nyaga v Megatank Solat Energy Ltd & Xinda Accounting Firm; Joseph Kimani Githinji v Platimun Credit Ltd; faith Wanjiku Waruru v Farmers Choice Kenya Ltd; and Anonymous vs Regional Center for Mapping of Resources for Development/

3.3.5 Other Remedies

In a few matters, ODPC went beyond corrective orders and issued recommendations for prosecution, particularly where the conduct was severe, deliberate, or obstructive. These referrals typically arise in situations involving false information, unauthorized disclosure, or unlawful processing.

A notable example is ***Eric Munene Njuguna v Chapeo Capital Limited (ZK Pesa***), where ODPC found that the 2nd Respondent had effectively assumed the role of a second data controller by disclosing the complainant's personal data without consent. His conduct fell squarely within Section 72 of the Data Protection Act, which criminalizes the disclosure of personal data without lawful excuse and in a manner incompatible with the original purpose of collection.

Given the seriousness of the breach and its alignment with the statutory offence, ODPC directed that the matter be referred for prosecution in accordance with DPA and its Regulations.

Of note is that this year (2025) the determinations of ODPC resulted in compensation that is required to be paid to the Complainant directly as opposed to issuing of penalty notices as well as administrative fines that were issued last year (2024).

3.4 Post-determination

Once a determination has been issued by ODPC, several paths can be taken:

- parties can follow ODPC's orders in the determination and conclude the matter;
- a party against whom an order has been made can fail to obey the order, forcing the other party to initiate enforcement proceedings at the High Court
- parties who are dissatisfied with the determination can appeal to the High Court

3.4.1 Enforcement of awards

A persistent challenge is the absence of an explicit enforcement mechanism for compensation awards under the Data Protection Act. While DPA allows ODPC to issue orders, including monetary awards, it does not set out how those awards should be executed.

In practice, an ODPC compensation award cannot be enforced on its own. A complainant who wishes to execute the award must approach the High Court, as many practitioners take the position that the determination must first be adopted as a court order. This requires the complainant to file an application asking the High Court to recognize and issue ODPC's award as an order of the court, after which normal execution procedures can follow.

3.4.2 Appeals

The DPA provides that a person who is dissatisfied with the determination of ODPC can appeal to the High Court. 15 determinations were appealed in 2015. The appeals arose from 2024 and 2025 determinations. Notably, all but three of the appeals were instituted by respondents who were dissatisfied with the findings and enforcement notices issued by ODPC.

In two cases, the Appellants were complainants who were aggrieved by ODPC's decision to either dismiss their complaint or issue a determination that they did not find favourable. In one case, both complainant and respondent had been dissatisfied with ODPC's determination and lodged an appeal and cross-appeal

Appeal decisions demonstrate continued judicial support for ODPC's mandate, while simultaneously reinforcing the need for procedural fairness, adherence to due process, and proportionality in the imposition of administrative penalties.The appellate trends observed in 2025 reflect a maturing data protection enforcement landscape in Kenya.

1 was **partially allowed,** resulting in a reduction of the administrative penalty imposed by ODPC.*(Regus Kenya Limited v Data Protection Commissioner & another)*
1 was **dismissed for want of prosecution** after the Appellant failed to pursue the matter. (*Okaja Ltd t/a Casa Vera Lounge*)
1 is **pending substantive determination**, with the High Court having granted a stay of execution of ODPC decision and enforcement measures. (*Kenya Breweries Ltd v Muriithi)*
1 was allowed on **procedural grounds,** and the matter **remitted back to ODPC for reconsideration** in line with the principles of fair administrative action and the right to a fair hearing. (*Metropolis Star Lab Kenya Ltd v Kioko & another*)
1 found that ODPC's actions were entirely **ultra vires** for failing to adhere to the principles of fair hearing and administrative action, and the Court quashed the enforcement notice and determination by ODPC, setting aside the award to the Complainant. *(Premier Credit Ltd. v Kimaru)*
The remaining appeals either upheld ODPC's findings in full, dismissed improper judicial review applications for failure to exhaust statutory appeal mechanisms, or affirmed the legality of enforcement and penalty notices, save for limited judicial moderation of penalties in appropriate cases. (*Okaja Limited t/a Casa Vera Lounge*, *Talanta Institute v Office of the Data Protection Commissioner*; *Mulla Pride Limited v Office of the Data Protection Commissioner; Aventus Technology Limited v Ndambuki*; *Swara Acacia Lodge v Office of the Data Protection Commissioner & another*; *Regus Kenya Limited v Data Protection Commissioner & another*; *Moja Expressway Company v Cyrus Mwaniki Ndungu; Ndururi v Office of the Data Protection Commissioner & 2 others;Shah v Prime Bank Limited*; *Muthoni v Solpia Kenya Limited t/a Sista Kenya*; *Republic v Data Protection Commissioner; Hotel Waterbuck Limited*

4.0 What we learn from 2025 determinations findings

This analysis examines determinations issued by the Office of the Data Protection Commissioner (ODPC) in 2025 to identify key enforcement trends, recurring compliance failures, and the evolving interpretation of data subject rights under the Data Protection Act, 2019. Drawing from complaints across multiple sectors, the analysis highlights a marked concentration of violations around the handling of data subject requests, failures in transparency, consent, and timely responses.

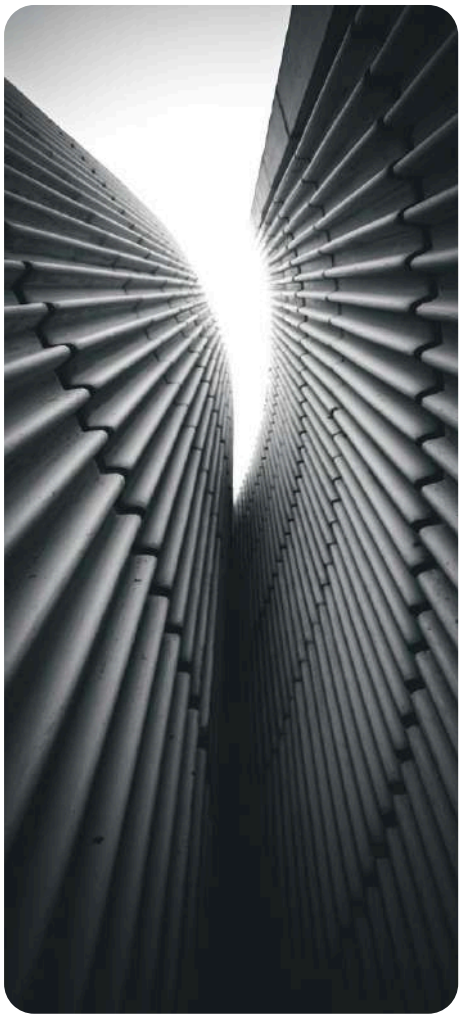
the findings illustrate a regulatory shift from formal compliance toward practical enforcement, revealing both systemic weaknesses in organisational data governance and the emerging direction of data protection regulation in Kenya.

The analysis further shows that ODPC applied stricter procedural and evidentiary standards in 2025, strengthened accountability for data controllers, and adopted a more consistent, proportionate approach to penalties and compensation. Collectively, the findings illustrate a regulatory shift from formal compliance toward practical enforcement, revealing both systemic weaknesses in organisational data governance and the emerging direction of data protection regulation in Kenya.

Key shifts observed in 2025 determinations include some regulatory shifts in how ODPC handled complaints, as well as sectoral issues. Examples of regulatory shifts include international cooperation, and stricter enforcement of data subject rights. Sectors discussed are public agencies as well as the digital lenders.

4.1 Regulatory shifts in ODPC determinations in 2025

Key shifts observed in 2025 determinations include some regulatory shifts in how ODPC handled complaints, as well as sectoral issues. Examples of regulatory shifts include international cooperation, and stricter enforcement of data subject rights. Sectors discussed are public agencies as well as the digital lenders.



4.1.1 International collaboration

The case of ***Aaditi Rajput vs. Diamond Trust Bank Kenya Limited & Diamond Trust Bank Uganda Limited*** involved a complaint, alleging improper disclosure of a third party's sensitive financial data (monthly bank statements) to her email address since November 2022. The complainant claimed she had no connection to Diamond Trust Bank Uganda (DTB Uganda, or the third party, yet received the third party's statements from DTB Uganda's email system. As a result of DTB Kenya's attempts to resolve the issue (e.g., adding her email to a "Do Not Contact" list in May 2025), she lost access to her own DTB Kenya statements and transaction notifications, leading to financial difficulties, distress, anxiety, loss of trust in banking systems, and potential risks like identity theft or data misuse.

Since DTB Uganda is incorporated in Uganda and falls under Ugandan jurisdiction, ODPC sought assistance from Uganda's Personal Data Protection Office (PDPO) to initiate investigations.This compelled DTB Uganda to respond, which they did via a letter submitted through the PDPO and incorporated into ODPC's investigation.

> sending third-party financial statements to an unintended recipient constitutes a breach of confidentiality and indicates insufficient technical and organizational measures. Although statements are password protected, the disclosure of sensitive banking information including the identity of a customer and partial transaction information amounted to unauthorized disclosure and inadequate security safeguards.

This cross-border cooperation ensured ODPC could access responses and evidence from an entity outside its direct jurisdiction, highlighting a practical mechanism for handling multinational data breaches.This case exemplifies effective regional collaboration in data protection enforcement, addressing the challenges of cross-border data processing in East Africa. As data flows increasingly transcend national boundaries, we hope to see more such collaborative efforts between ODPC, PDPO Uganda, and other regional bodies in future cases to strengthen privacy rights and deter systemic breaches

4.1.2 Stricter standards for consent

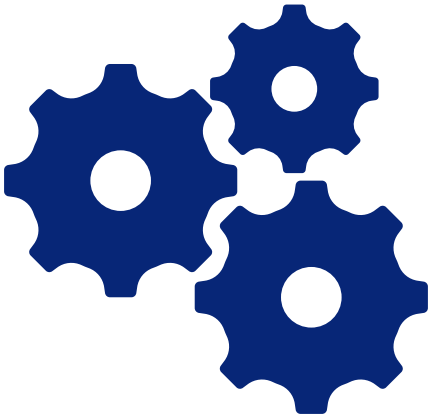
The standard for consent moved definitively away from reliance on implied or indirect consent to demanding strict express consent. 2025 determinations show that:

- **Proof of Consent:** The burden of proving valid consent rests entirely on the data controller. To meet this high standard, ODPC clarified in 2025 that oral consent must be reduced into writing or recorded electronically for it to be provable by the respondent. *(Samuel Kamau Waweru v Platimum Credit Ltd; Comfort Muthoni Gachiri vs. The Storage Trading Company Limited)*
- **Inadequacy of general notices**: General measures, such as disclaimer notices displayed on large-sized notice boards in events, are legally insufficient and do not constitute express consent for processing personal data for commercial purposes. *(Chizzy Taabu Orwa, Shelmith Nyawira Gitonga & Stanley Kinyua Wachira vs Mast Jagermeister Se)*
- **Consent is dynamic**: Consent is not a static, one-time event. ODPC ruled that any material change in the processing operation, such as transferring employee and next-of-kin data from one insurance provider to another, necessitates obtaining new consent from the data subjects. *(Erick Kabuyefu Zakayo & 12 Others vs Bohemian Flowers Ltd.)*

4.1.3 Stronger enforcement of data subject rights (DSRs)

Enforcement has been significantly strengthened regarding DSR adherence, particularly concerning procedure and timelines. Notably:

- **The Right to be informed**: ODPC ruled that the obligation to inform the data subject (Section 26(a)) is mandatory and non-discretionary, regardless of the scope or frequency of processing. A generic privacy notice issued after the fact cannot satisfy the requirement for specific and unequivocal notice prior to or at the point of data collection. *(Lynda Namusonge Maturu vs. Kenya Bankers SACCO)*
- **Prohibition of DSR obstruction**: A key shift in 2025 involves strictly penalising controllers who create unnecessary hurdles to restrict a data subject's rights. For instance, conditioning account erasure on the production of excessive or irrelevant documents (such as three months' M-Pesa statements) was deemed an unlawful restriction and a violation of the data minimization principle. *(Bosco Otieno v Betika Kenya:)*
- **Absolute right to object**: The right of a data subject to object to processing for direct marketing purposes is treated as an absolute right in cases of direct marketing. *(Philip Bolo v Platimum Credit Ltd; Cherry Fiona Mwendwa vs. Acceler Global Logistics Ltd; Timothy Murithi Kaung'u vs. Mycredit Limited; Richard Malelu vs. Fairdeal Furniture Limited)*



4.1.4 Clarity on remedies

ODPC clarified the statutory limits of its powers regarding compensation:

- **Economic Loss Excluded:** Compensation awarded under the DPA is primarily limited to violations of data protection rights and does not expressly provide for compensation for economic losses (such as lost job opportunities), which typically fall under employment law. *(Margaret Nzula vs. United Winners DT SACCO, & Shirika DT SACCO)*

4.1.5 Increased controller accountability and proportionality

The determinations set clearer, system-level expectations for data controllers across all sectors:

- **Liability for Agents**: Data controllers remain obligated to ensure lawful processing even if the violation originated from an independent sales agent (data processor) used for marketing purposes. *(Samuel Kamau Waweru v Platimum Credit Ltd; Philip Bolo v Platimum Credit Ltd)*
- **Proportionality Test**: Even when invoking a lawful basis like "legitimate interest" (e.g., for security or debt recovery), the processing must satisfy a proportionality test. If a security measure, like a CCTV camera, unlawfully captures a neighboring private residence, it violates the principles of privacy, lawfulness, fairness, and data minimization. Similarly, transmitting financial obligations to an employer without consent fails the proportionality test. *(Lilian Nyawira Nderitu & John Gitahi Mureithi v Josephat Karungo & Freshia Mugo Waweru)*

4.1.6 Severe consequences for obstruction

Compared to 2024, the consequences for obstructing regulatory processes have escalated significantly in 2025 determinations:

- **Prosecution Recommendations**: ODPC explicitly issued recommendations for prosecution against the directors of companies found to have obstructed the Data Commissioner in the exercise of their powers or given false/misleading information. (*Yasin Abukar vs Wananchi Group (Kenya) Limited T/A Zuku Fibre Kenya; Ayub Odanya Naburi v Geosky Service Ltd; Antony Mwenda v Ceres Tech Ltd T/A Rocketpesa; Lee Mutunga v Milestone Games Ltd T/A Sportspesa; Eric Munene Njuguna vs. Chapeo Capital Limited (ZK Pesa), & Ericson Lubale Okota; Jimmy Owiti vs. Natal Tech Limited)*

4.1.7 Criteria for determinations and outcomes

The analysis show a notable consistency in how ODPC penalises similar types of offences.

- Cases involving unauthorised disclosure, unlawful processing, or misuse of contact information—especially by Finance/Credit providers, digital lenders, and marketing/promotions entities—tend to attract similar fine ranges, usually Ksh. 50,000–500,000. Repeat patterns appear across sectors:
- Finance/Credit and Banking offences generally attracted fines of Ksh. 50,000–250,000 fines.
- Marketing/Promotions and high-reach digital firms consistently receive higher fines, often KES 400,000–1,500,000, reflecting the broader impact of their breaches.
- Minor or technical breaches resulted in no fines or small penalties.

Overall, in 2025, ODPC applied penalties in a predictable, proportional manner, where similar violations lead to similar fine bands, showing a deliberate effort to maintain fairness and consistency across determinations.

From the foregpoing, some of the criteria observed from ODPC's determinations in 2025 include proportionality, harm, accountability, and sector-specific risk. Breaches involving clear unlawful processing, unauthorised disclosure, or misuse of personal data attracted penalties, while cases with insufficient evidence, minimal harm, or procedural defects tend to be dismissed. The analysis concluded that some of the factors assed by ODPC include:

- **Severity of harm to the data subject** (distress, reputational damage, intrusion).
- **Nature of the data involved** (sensitive vs. ordinary personal data).
- **Scale and reach of the violation** (one person vs. mass marketing or automated outreach).
- **Conduct of the respondent,** including cooperation, intent, and recurrence.
- **Sectoral risk,** with higher expectations placed on regulated sectors like Finance, Banking, Health, and Telecommunications.
- **Corrective behaviour,** where issuance of enforcement notices was preferred when compliance gaps could be remedied.

4.2 Sectoral patterns and systemic compliance challenges

The analysis noted several patterns across sectors, such as recurring compliance weaknesses in high-risk industries such as finance, credit, and digital lending, as well as emerging issues in public sector and cross-border data processing.

4.2.1 Government and Public Sector Bodies

In 2025, ODPC of the Data Protection Commissioner (ODPC) issued two (2) determinations against government and public sector bodies. The first,, involved an anonymous complainant against the ***Regional Centre for Mapping of Resources for Developmen***t, an intergovernmental non-profit organization focused on resource mapping for public development initiatives. The complainant alleged unlawful processing of sensitive personal data without consent or knowledge. ODPC dismissed the complaint, ruling that the processing was lawful and necessary under Section 25 of the Data Protection Act, 2019, as it served overriding public interest in resource allocation and development planning, with no breach of data minimization or purpose limitation principles identified.

ODPC dismissed the complaint, ruling that the processing was lawful and necessary under Section 25 of the Data Protection Act, 2019, as it served overriding public interest in resource allocation and development planning,

The second case, ***Elias Cheruiyot Korir vs Thika Water and Sewerage Company***, involving a county-government-operated public utility providing water and sewerage services. The complainant claimed persistent erroneous billing notifications via SMS despite his explicit objection on 26 March 2025, alleging violations of his data subject rights. ODPC upheld the complaint on grounds that:

- the respondent breached the complainant's right to object to processing under Section 26(c) by continuing the disputed messages until 24 June 2025;
- it also failed to uphold data protection principles of accuracy and rectification under Section 25, as the billing errors stemmed from unverified and outdated records.

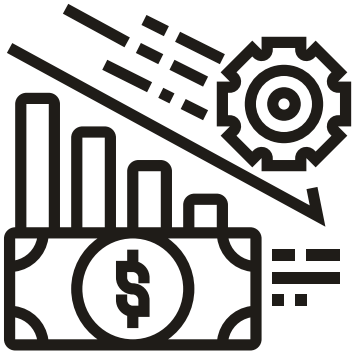
Consequently, ODPC imposed a penalty of KShs 250,000 on Thika Water, ordered immediate cessation of the processing, deletion of the disputed data, and compensation to the complainant for resulting distress, emphasizing the utility's duty to integrate objection mechanisms into operational systems.

4.2.2 The finance sector

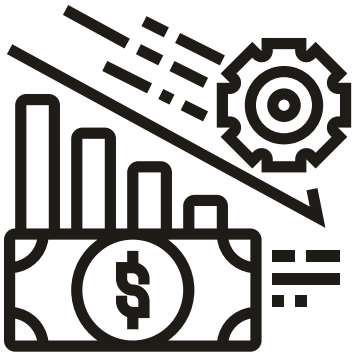
The compliance challenges in this sector center around systemic failures in transparency, consent, and respecting the privacy of data subjects and third parties:

- **Lack of Proper Consent Management:** Respondents frequently failed to obtain or demonstrate express consent for processing personal data for commercial purposes, especially direct marketing. The reliance on implied consent or general terms is consistently rejected by ODPC.
- **Unauthorized Disclosure (Third-Party Contacts):** A common violation, especially among digital lenders, is the unauthorized disclosure of data for debt recovery purposes. This includes the unlawful processing of personal data for unauthorized purposes, such as listing a complainant as a guarantor without their prior knowledge or consent.
- **Violations of Data Subject Rights (DSRs): F**inance institutions frequently infringe on core DSRs:
- **Right to Object:** Companies, including SACCOs and digital lenders, were found liable for violating this right, particularly by ignoring objection requests and continuing to send unsolicited messages. The right to object to processing for direct marketing purposes is treated as an absolute right.
- **Right to be Informed:** These violations are widespread, where controllers failed to notify the data subject of the use their data would be put to.
- **Right to Erasure/Obstruction:** Some respondents were found liable for denying a complainant the opportunity to exercise their right to erasure by requesting un necessary personal data not relevant to the account closure.
- **Obstruction of Investigations:** Obstruction of the Data Commissioner during investigations is a recurring and severe factor, often leading to heavy penalties and official recommendations for prosecution against the Directors of the respondent company. For instance, Ceres Tech Limited T/A Rocketpesa faced a recommendation for prosecution due to obstruction and providing false or misleading information to ODPC.

The recurring nature of these specific violations in the financial sector suggests systemic compliance challenges, primarily rooted in the high-speed, automated nature of digital credit operations:



- **Systemic automation without proper governance:** Digital lenders rely on automated collection processes and aggressive recovery strategies that often override legal requirements for express consent and notification, leading to breaches like the unauthorized contact of third parties or continued harassment via unsolicited messages.
- **Weak accountability for agents:** Determinations confirm that the Data Controller is held liable for unlawful processing performed by its independent sales agents, even if the agent is no longer employed. This suggests a failure in implementing proper Data Processing Agreements and oversight.
- **Lack of proportionality:** ODPC is increasingly applying a proportionality test. Practices such as transmitting a borrower's financial obligations to their employer without consent, or imposing unlawful restrictions (like demanding three months of M-Pesa statements for account closure), violate the principle of data minimization and purpose limitation. This suggests the sector struggles to balance its legitimate interests with fundamental data rights
- **Security lapses:** Cases involving unauthorized disclosure, even sensitive data like health information, point toward lapses in technical and organizational measures.



Data-sharing also emerged as a cross-sectoral concern. Several cases demonstrated unlawful sharing of personal data with third-party agents, while evidence indicated a persistent misunderstanding of purpose limitation. Outside the digital lending ecosystem, numerous organisations relied on historical or vague consent to justify new processing activities, underscoring the need for robust and demonstrable consent management practices.

Collectively, these trends suggest that the next phase of Kenya's data protection evolution must focus on moving beyond policy declarations toward technical, procedural, and governance maturity. Strengthening internal accountability frameworks, implementing systematic record-keeping, embedding data protection by design, and ensuring enforceable consent management will be critical for organisations across all sectors to meet statutory obligations and build customer trust.

5.0 Recommendations

The majority of complaints filed to ODPC in 2025 originated from high-risk sectors such as finance, digital credit, and marketing, which collectively accounted for approximately 40% of the cases. These sectors exhibited significant compliance challenges, particularly due to the prevalent reliance on implied consent and unauthorized disclosure of personal data, hence the need for enhanced regulatory oversight. With this noted, policy makers and data handlers should:

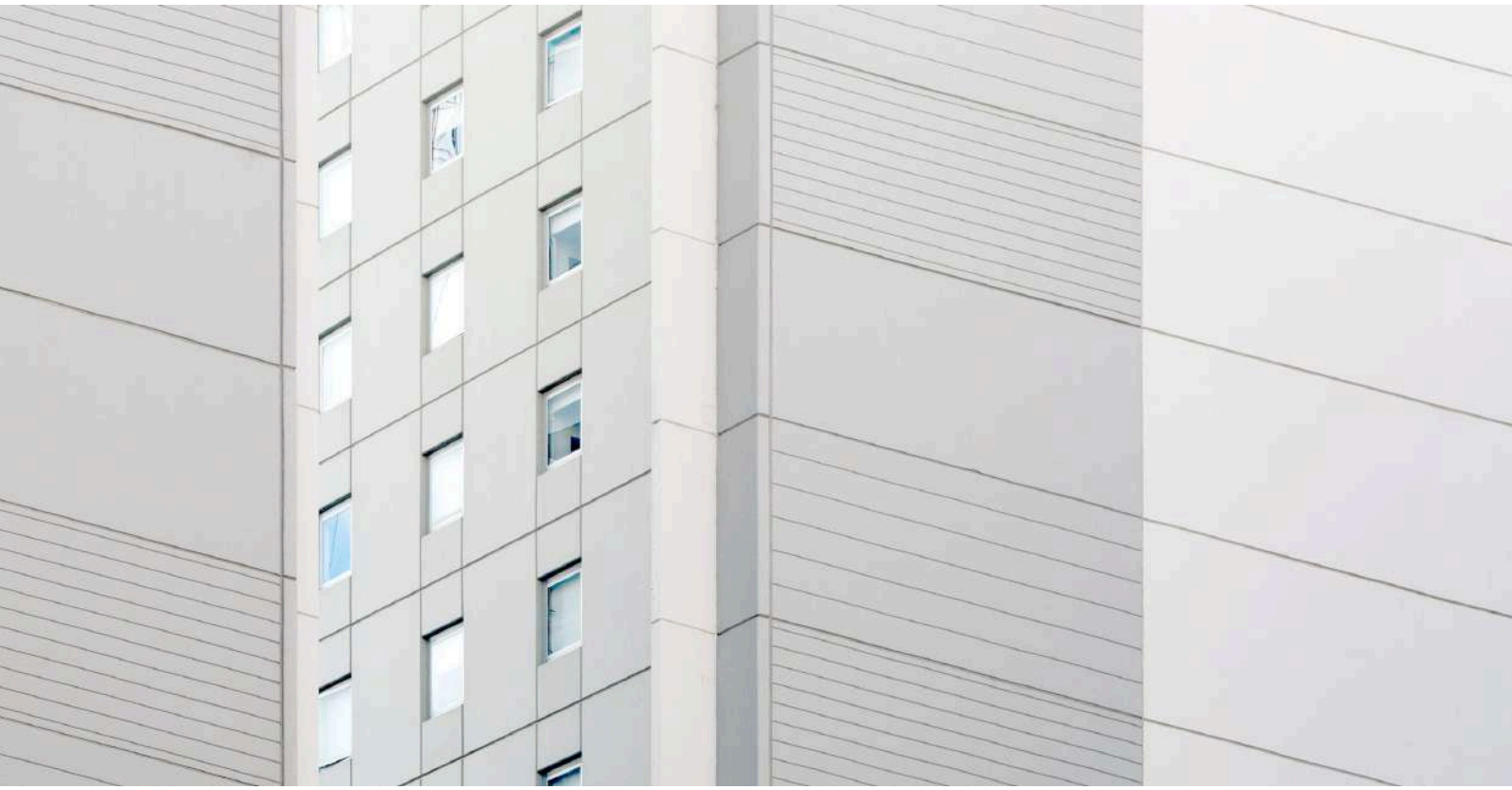
Strengthen agent oversight: By requiring clear data processing agreements and regular audits for third-party agents involved in digital lending. Since controllers are ultimately responsible for any breaches, they should also add criminal penalties for those who obstruct investigations, as seen in the recent prosecution case of Platinum Credit.

Improve data subject rights (DSR) processes: By making it mandatory for organizations to provide automated opt-out options and respond to rights requests within 30 days. This addresses over 60 complaints where people faced unnecessary hurdles like demands for excessive documentation.

Enforce sector-specific guidelines and support: To build on ODPC's nine guidelines planned to link compliance to license renewals in sectors like finance, education, and telecoms. This approach will help reduce ongoing problems such as unwanted marketing messages despite previous warnings.

Simplify judicial procedures: By amending the Data Protection Act to grant ODPC decisions the force of court orders, executable directly via garnishee or asset attachment, without separate judicial confirmation. As Mugambi Laibuta notes in his thesis on data protection adequacy, courts uphold ODPC's authority yet Section 64 appeals cause delays, therefore reforms here would ensure timely remedies for data subjects

DPGSK
Data Privacy
and Governance
Society of Kenya



info@dataprivacyke.africa

dataprivacyke.africa