



***DATA PRIVACY & GOVERNANCE SOCIETY***

# **ODPC DETERMINATIONS IN 2024 ANALYSIS REPORT**

---

# Contents

About DPGSK

01

Acknowledgements

02

Executive Summary

03

Analytical Framework

05

Key Findings

06

Common Types of Complains

07

Key Sectoral Determinations

08

Penalty Types

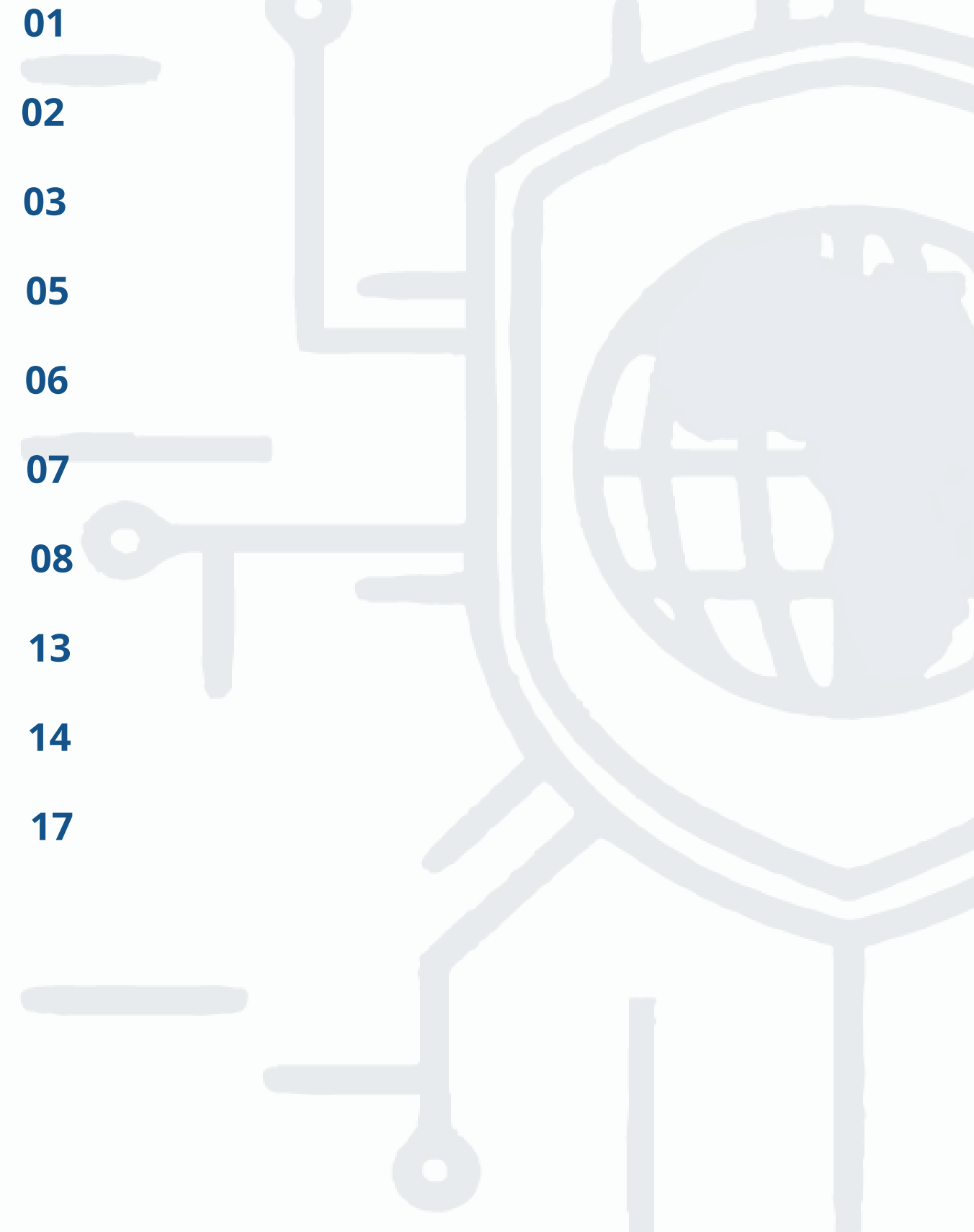
13

Dismissed Complaints

14

Alternative Dispute Resolution Mechanisms

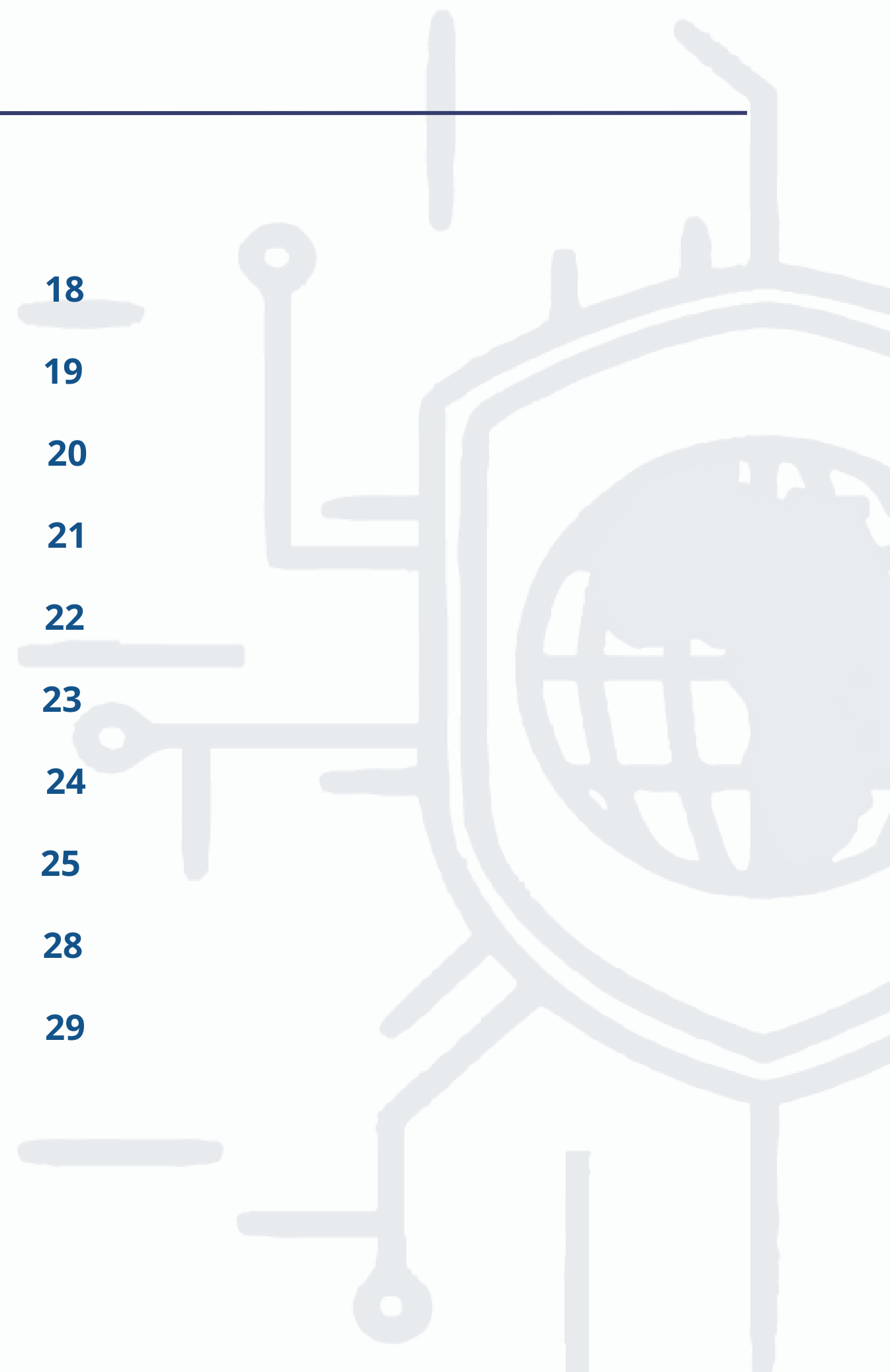
17



---

# Contents

Statutory Non-Compliance	18
Major Legal or Systemic changes	19
Government and Public Sector Bodies	20
Decisions against Digital Lenders	21
Digital Lending Sector Challenges	22
Consistency in Outcomes	23
Cross- Sectoral Insights	24
Trends and Implications	25
Recommendation For Policy Makers	28
What Next?	29





# 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 Enforcement:** 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.

---

# Acknowledgement

The completion of this report was made possible through the dedication, expertise, and collective effort of volunteers from DPGSK.

DPSGK appreciates Naisenya Shanice, who served as the team leader, for her leadership, strategic guidance, and commitment throughout the research and analysis process.

DPGSK expresses gratitude to the dedicated team members whose contributions in research, and data analysis were invaluable. Special thanks to Dr Mugambi Laibuta, Grace Mutung'u, Hawi Alot, Mitchell Musyoka, Georgina Giathi, Franc Monyango, and Mercy Wafula.

DPGSK recognizes and appreciates the support of the DPGSK community, whose continuous engagement, discussions, and insights contribute significantly to the advancement of data protection awareness and compliance in Kenya.



## EXECUTIVE SUMMARY

This Office of the Data Protection Commissioner (**ODPC**) Determinations Analysis Report provides insights into Kenya's data protection enforcement environment; analysis included reviewing the **51 determinations** made by ODPC in 2024.

Complaints made to the ODPC in 2024 spanned sectors such as financial, health, education, and digital lending. Key challenges identified in this Analysis Report include improper consent management, unsolicited communication, data breaches, and third-party harassment. The financial and digital lending sectors account for a significant proportion of determinations made by the ODPC. The ODPC issued substantial fines, averaging **Ksh. 522,308**. ODPC also issued enforcement notices to address violations.

Major systemic changes emphasize express consent, strict enforcement of data subject rights, and penalties for obstructing investigations. Recommendations include strengthening sector-specific compliance frameworks, enhancing ODPC resources, promoting public awareness, and adopting privacy-enhancing technologies.

By fostering cross-sector collaboration and addressing compliance gaps, Kenya can build a robust data protection ecosystem that safeguards individual privacy, strengthens accountability, and supports sustainable economic growth.

# 2024 ODPC Determinations: Analysis Report

## Background

The Data Privacy and Governance Society of Kenya (DPGSK) recognizes the critical role of data privacy and governance in ensuring compliance with data protection regulations across diverse economic sectors.

As data continues to shape every aspect of modern life, it is essential to understand the nature of complaints and analyze them carefully, deriving insights that shape the development of regulations.

## Scope

The analysis based on the 51 determinations made by the Office of the Data Protection Commissioner (ODPC) in 2024; exploring trends and compliance challenges under the Data Protection Act, 2019.

This Report examines issues such as unauthorized data use, transparency, and sector-specific compliance. .

# ANALYTICAL FRAMEWORK

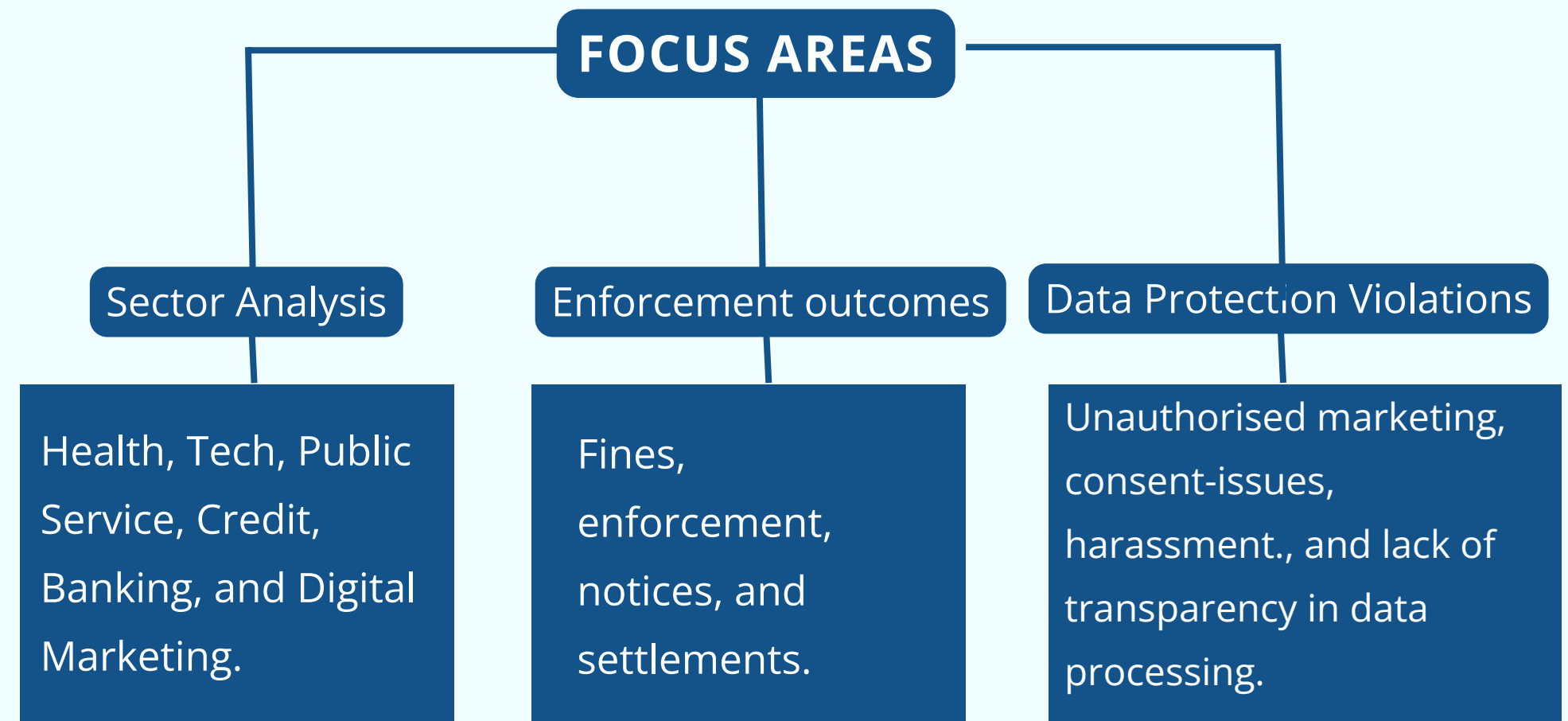
This Report for the 2024 ODPC Determinations Analysis combines qualitative, quantitative, and comparative methods.

Determinations were categorized by **sector**, **type**, and **outcome**, focusing on recurring data protection issues.

Qualitative analysis reviewed legal principles, such as consent and data subject rights, while quantitative analysis identified trends like sector representation and penalties issued.

Comparative analysis evaluated public versus private sector determinations, revealing inconsistencies in enforcement.

The analytical approach provides insights into systemic gaps, sector-specific challenges, and the effectiveness of Kenya's Data Protection Act enforcement.



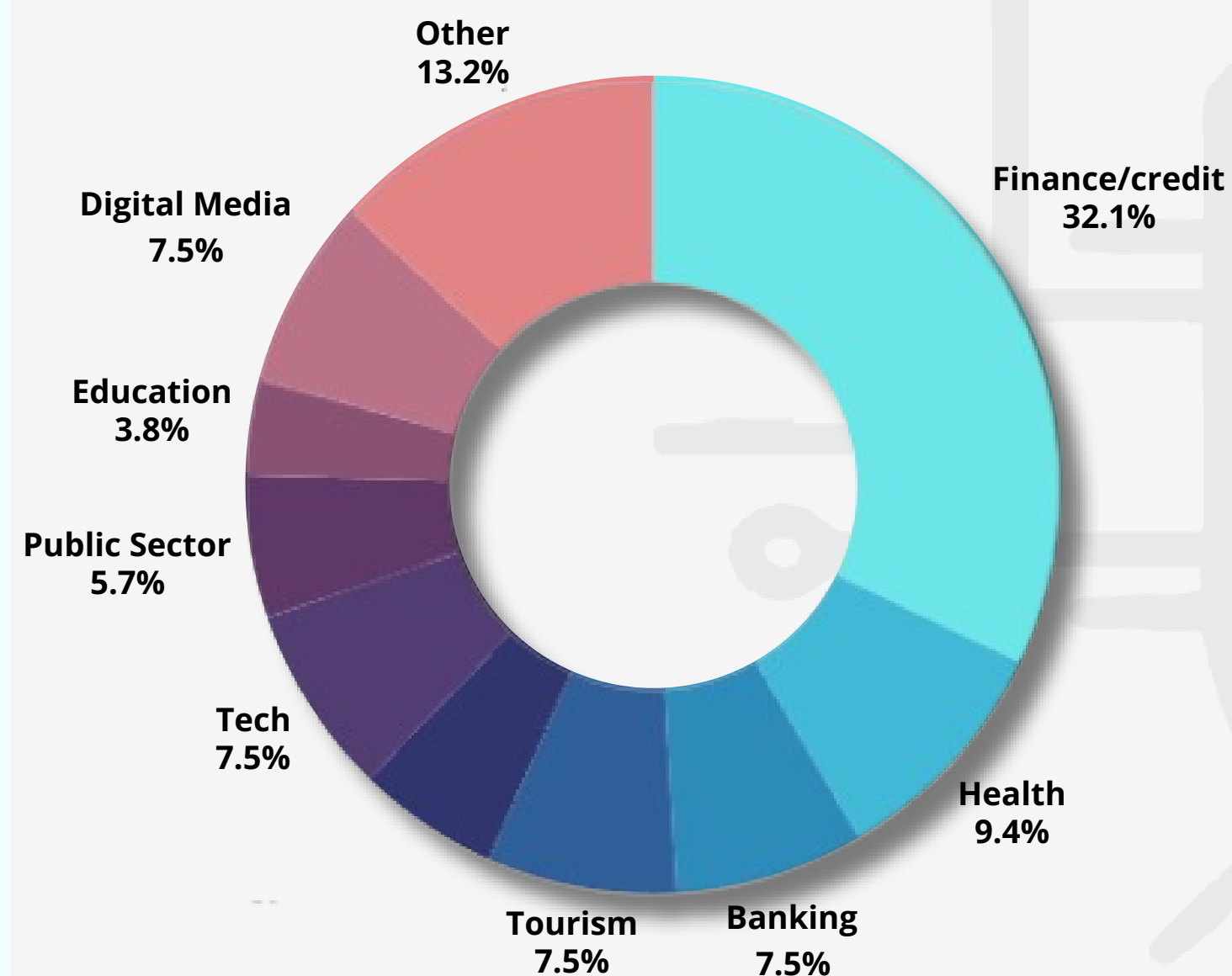


## KEY FINDINGS

The **financial services, fintech, and microfinance sectors** led with **17 determinations**, highlighting data protection challenges in digitization. **Health (5), banking (4), education (4), and digital media (4)** sectors faced issues with sensitive personal data processing. Sectors such as **travel, agriculture, and tech** had fewer determinations but still revealed data protection compliance concerns.

The spread of determination within the various sectors indicates the need for more robust and sector specific data protection compliance programmes and improved data subjects' awareness.

Cited sectors ought to continually make reference to Guidance Notes issued by the Office of the Data Protection Commissioner for a nuanced approach towards compliance.





## COMMON TYPES OF DETERMINATIONS

Common determinations related to **unauthorized use of personal images**, **unsolicited marketing messages**, and **improper consent management**. There were many complaints of harassment by digital lending entities who have aggressive debt collection strategies. Unauthorized disclosure of sensitive personal data and lack of transparency in processing were also critical concerns for this sector.

Violation of minors' privacy rights in education and advertising also emerged as critical issues. The recurrence of determinations on the cited issues underscores significant compliance gaps across multiple sectors.

The **financial** and **digital lending** sectors ought to implement comprehensive consent management frameworks, data subject rights management protocols, and ethical debt collection practices as steps towards compliance with the Data Protection Act. Digital lending entities should also cooperate with investigators as required by law. Healthcare and education institutions ought to enhance safeguards for sensitive personal data and minors' personal data, ensuring strict adherence to confidentiality and parental consent requirements.

The **advertising** and **marketing sectors** should prioritize consumer privacy by obtaining **explicit consent** before processing personal data and acting on data subject requests and complaints within timelines set out under the Data Protection (General) Regulations.

---

# KEY SECTORAL DETERMINATIONS

## HEALTH

In *N\*\*\*\*o\*\*\* v Malibu Pharmacy* the Pharmacy was found in violation of the complainant's privacy rights as envisioned under section 25(a) and (d) of DPA by exposing the complainant's medical diagnosis details to a third party while delivering a medical package. The complainant was awarded damages amounting to Ksh 700,000/= for the violation.

This determination points to the fact that sectors handling sensitive personal data may face stricter penalties for breaches, given the critical nature of the data.

## BANKING

In *Kevin Kiprotich Rono v. SBM Bank Kenya*, the Bank was found liable for unlawfully processing Rono's personal data even after Rono had asked the bank to cease the processing.

The determination is a reminder to entities that market to customers to periodically review their databases to ensure that they are not unlawfully sending marketing emails to former clients.

Organizations also need to update their employee offboarding protocols particularly for employees who handled data subject requests to ensure that requests are not left unattended during transition.

---

## TOURISM

### ***Victor Kibet Siel v Hotel Waterbuck Ltd.***

In this case, Siel who worked as a receptionist at the hotel contested use of his image in marketing the Hotel. ODPC determined that the Hotel did not seek express consent from the Complainant when taking his photo as required by the Data Protection Act, 2019. Siel was awarded Ksh. 500,000.

This determination is a caution to entities that use images on websites and other marketing platforms to obtain express consent from the data subjects to avoid claims based on unauthorized data processing.

Entities should also handle requests to take down images within timelines set out under the Data Protection (General) Regulations so as not to violate data subject rights.

## EDUCATION

In ***Fatuma Hadi Ali suing on behalf of J.A.A(minor) v Nova Pioneer Kenya LTD*** a parent complained that their child's image had been used for commercial advertising purposes without the parent's consent or knowledge. The parent was awarded Ksh. 950,000.

This determination highlights the need for consent management for entities that deal with children. Where a child's image or other personal data is to be used, it is vital that consent is expressly obtained from a parent or guardian of the child.

Entities must also have protocols for taking down children's image or other data where the child's parent or guardian requests.

---

# DIGITAL MEDIA

## ***Caroline Wanjiru Kang'ethe-vs- Circus 254 % Sarakasi Trust***

In this determination, Kang'ethe attended an event hosted by Sarakasi. She later saw her photo posted on Sarakasi's social media platforms (Facebook & Instagram) for promotional purposes without her consent. Sarakasi pleaded that they had posted 'photo zone' notices to warn revellers of areas where they could be photographed. ODPC however found that such notices did not constitute consent and awarded Kang'ethe Compensation of Kshs 500,000.

This determination serves as a warning to event organisers on the importance of obtaining express consent for photos of data subjects before posting them on their social media spaces.

In addition to obtaining consent, media companies should have protocols for responding to data subject requests to take down their images.

# PUBLIC SECTOR

***Allan Chacha v County Assembly of Migori*** Chacha complained that his CV was published on the county assembly's website. Chacha had submitted his CV as part of his application to become county assembly speaker but had not consented to publication of the same. ODPC found that the county assembly did not have a lawful basis for publishing the cv. ODPC awarded Chacha Ksh.950,000.

The determination underscores the principle that the misuse of personal and sensitive personal data, especially when published without lawful basis, attracts significant penalties.

Public agencies should carry out Data Protection Impact Assessments to establish the legitimate basis for any personal information they have published.

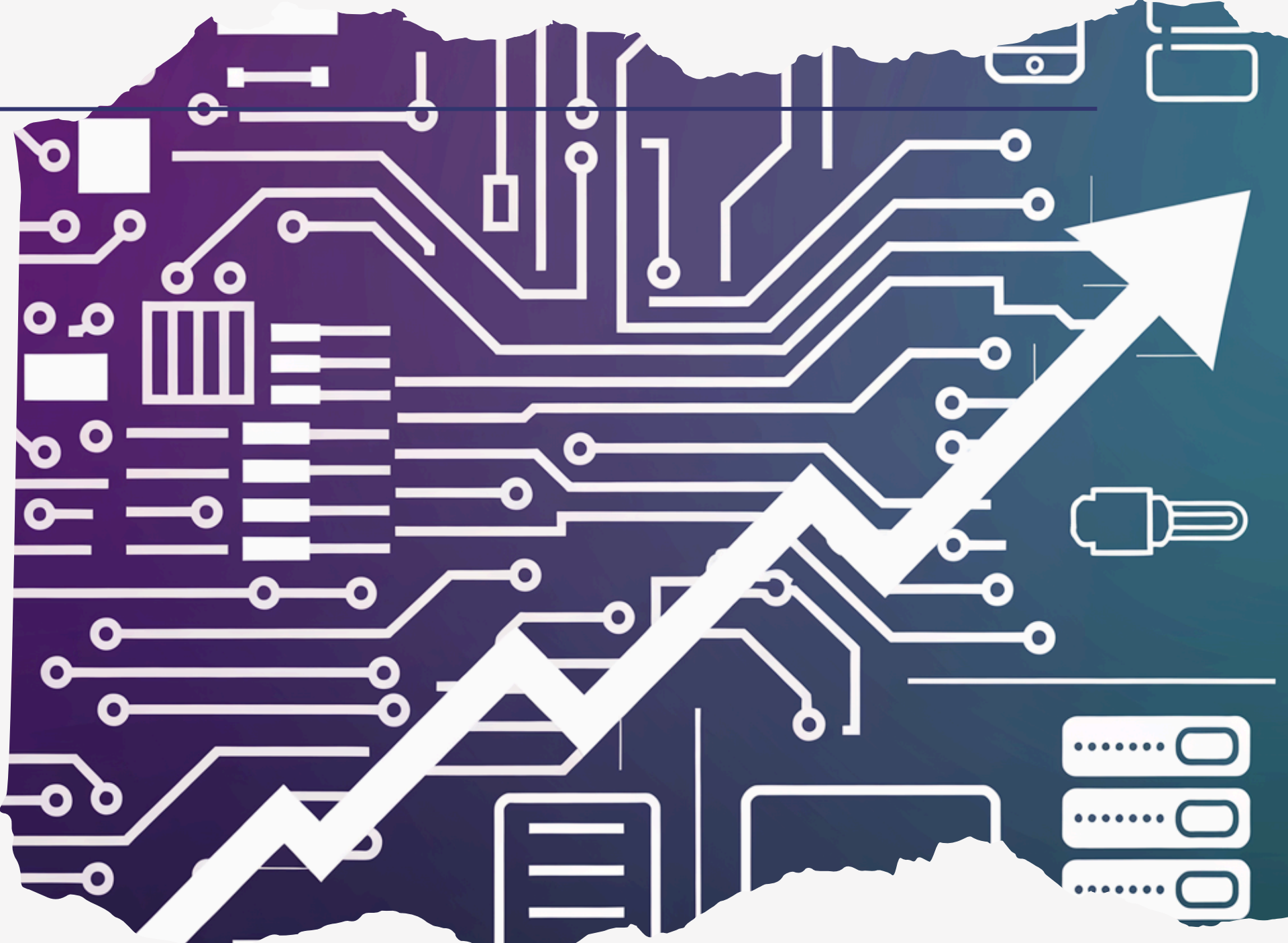
Further, public agencies should establish protocols for responding to data subject requests.

# TECH

## *Kennedy Wainaina Mbugua v. Bolt Operations OU and Bolt Support*

Kenya Limited Mbugua complained that Bolt unlawfully accessed and processed his personal information, resulting in the unlawful disclosure of his personal data to third parties who used his ride-hailing driver account information for fraudulent purposes. ODPC found that Bolt failed to uphold Mbugua's request to access data that Bolt held about him. **He was awarded Ksh.500,000.**

Entities whose business models are significantly based on data processing have to maintain high standards of data protection. They ought to set up technical and organisational measures to protect customer data from breach. These include verifying identity and communication channels to protect data subjects



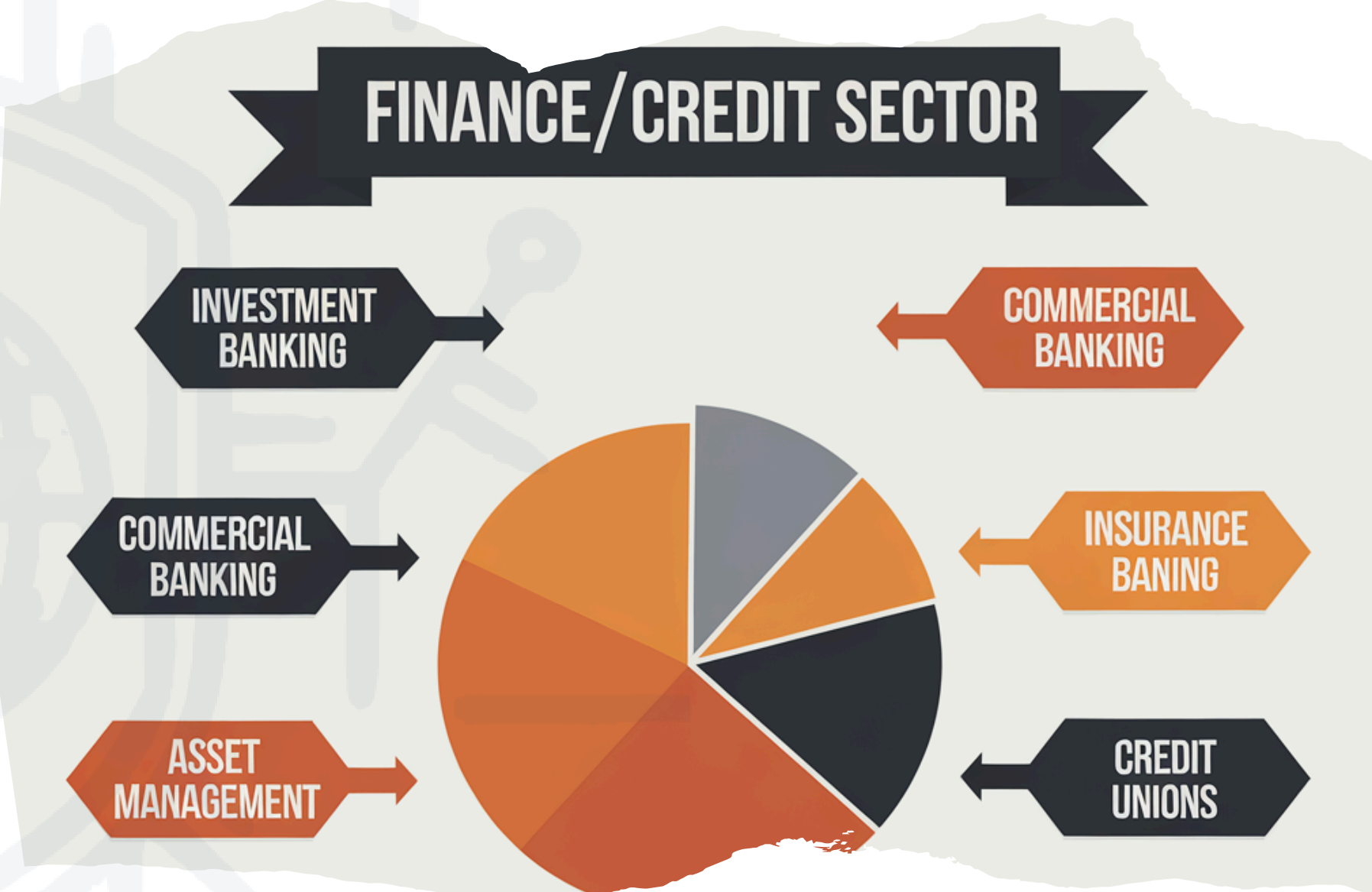
Data handlers need to carry out proactive compliance by undertaking DPIAs and monitoring their systems to prevent unauthorized access. They should also have protocols for reporting any breaches.

# FINANCE/ CREDIT

## *Victory Owino v Mhasibu Housing Company LTD, Mhasibu NWDT Sacco Society LTD*

In this determination, Owino complained that after completing a conveyancing transaction, he was bombarded with marketing emails, calls and texts. Although ODPC could not find that the Housing Company had shared Owino’s data, ODPC found that there was a violation of Owino’s rights and ordered the SACCO to compensate Owino to the tune of Ksh.650,000.

This determination demonstrates the need for training and raising awareness on privacy and data protection. Employees in entities that process sensitive personal data should be made aware of the standard operating procedures required to comply with the Data Protection Act 2019



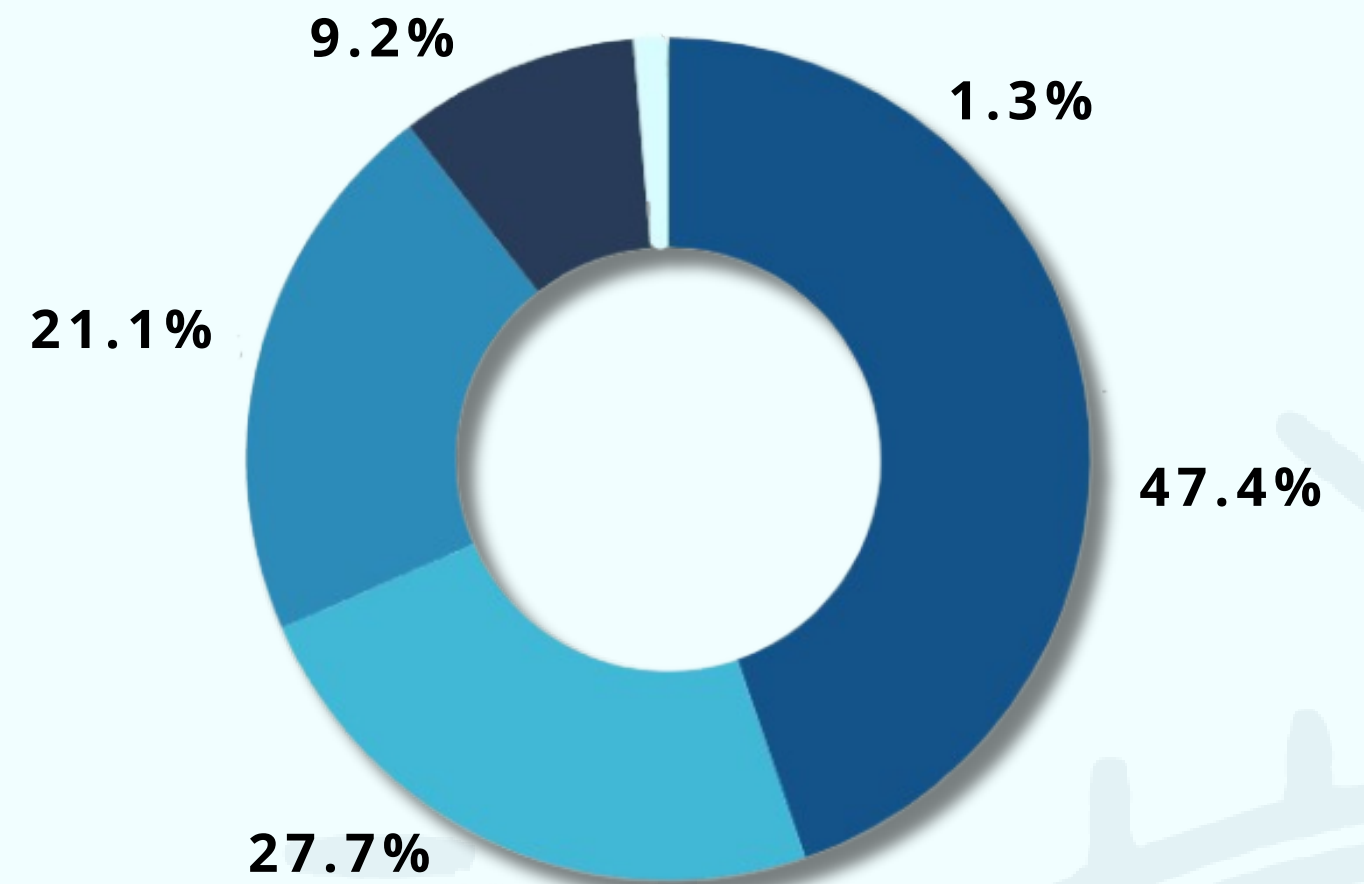
## PENALTY TYPES

Out of **51 determinations**, **34** resulted in awards for damages to the complainants. The awarded damages ranged from **Ksh. 25,000** to **Ksh. 1,200,000**; averaging **Ksh. 522,308**.

Higher penalties and award for damages in favour of the complainants targeted repeat offenders, willful non-compliance, and data processing for commercial gain.

18 complaints resulted in enforcement notices. 16 cases resulted in both awards for damages and enforcement notice. Some complaints were resolved amicably or dismissed.

The fines and enforcement notices highlight growing regulatory scrutiny.




### KEY

- Awards for Damages to Complainants
- Enforcement Notices
- Both Fines and Enforcement notices
- Amicable Settlements
- Dismissals.




---

## DISMISSED COMPLAINTS

 *In Denis Mwangi Alias Dennis Mint v Mulla Pride Limited*, Dennis Mint complained that Mulla Pride's agents were sending him messages that he was an emergency contact to a person he was not familiar with. He further complained that the agents further used various phone numbers to abuse and shame him. This complaint was dismissed because the **ODPC could not establish that the numbers used to contact Denis indeed belonged to Mulla Pride.**

This case **shows the burden placed on complainants to prove** that respondents violated their privacy. Complainants need to provide evidence implicating the data handler of privacy violations.

Since acquiring information regarding data handlers may be a challenge, complainants could **consider naming both the agents and the company as respondents.**

 *Eric Kariuki Vs Ceres Tech Limited T/A Lemoncash.* In this determination, Eric Kariuki alleged that on 21st November 2023, he received **over 200 calls in less than half an hour** from the Lemoncash, demanding payment of a loan he was not party to. Eric was forced to switch off his phone and unable to work, as his work relies on phone calls. Similar to the case of Denis Mwangi Alias Dennis Mint v Mulla Pride Limited, **the complaint was dismissed** because the complainant did not establish that the phone calls in question were actually from Lemoncash.

This is a curious determination because the **ODPC notes that the Respondent did not cooperate with investigators, denied them access** to the backend of their database to verify whether the Complainant was in the database, and whether the said mobile numbers belonged to the Respondent. **The Respondent therefore obstructed investigations** contrary to the Data Protection Act, but despite their obstruction, the complaint was dismissed.

---

## DISMISSED COMPLAINTS



In *Derrick Kiamba v. Ceres Tech Limited T/A RocketPesa*, Derrick complained about unsolicited marketing calls from RocketPesa agents. Despite informing them that he was not interested in their products, the agents continued calling him in attempts to get him to take a loan from the company.

The complaint was dismissed as the Office of the Data Commissioner was unable to establish that the mobile phone numbers that contacted the Complainant belonged to the Respondent.

Another curious determination that appears to place the burden of proving that phone numbers belong to the respondent, **even where the respondent is uncooperative with OPDC investigators.**



*Dennis Gitonga Ndururi Vs Twiga Foods Limited:* Dennis complained that his image was used without consent for commercial purposes without his consent or compensation to him. This non-consensual use of his image however happened in 2018, before commencement of the Data Protection Act. This complaint was dismissed for two reasons: Dennis could not show that he contacted Twiga Foods to assert his rights, and since the DPA was enacted in 2019, it could not apply retrospectively.

A complainant wishing to complain about a privacy violation that occurred prior to Nov 2019 should consider **other avenues such as a civil suit** since the OPDC may not entertain complaints about events that occurred **prior to enactment of the Data Protection Act, 2019.**

## DISMISSED COMPLAINTS



***Hilda Mwangi suing as legal guardian of MNN versus Edgar Obare:*** Hilda Mwangi complained that Edgar Obare who runs celebrity gossip sites, had unlawfully used her minor's image without her consent. Hilda had posted the child's photo on social media and Edgar had subsequently posted it on his Telegram channel. The complaint was dismissed as ODPC reasoning that the photo was lawfully processed as it was retrieved from publicly posted social media post.

This determination restated the position that the burden of proof lies with the complainant. A complainant who alleges that a respondent has made commercial gain from personal information should provide proof of the commercial gain.



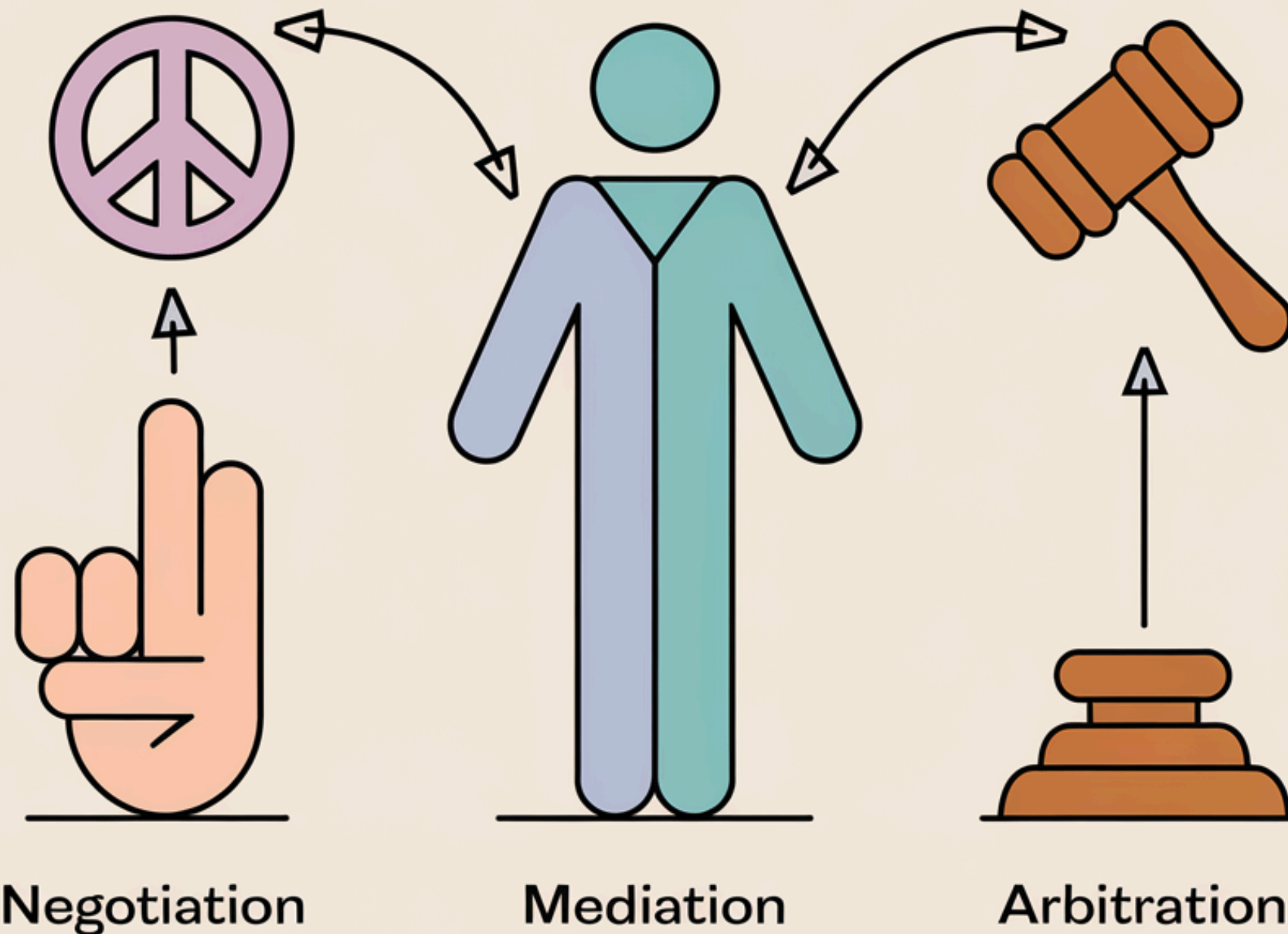
***Inga Kimaru v Amref Pension Trustees:*** A pensioner complained that she had discovered that the pension trustees had **disclosed her personal information to third parties without her consent.** The complaint was dismissed because the **complainant failed to serve the cease and desist letter** on the Respondent in order to exercise her right to objection.

This determination demonstrates that **complaints can be dismissed for lack of merit.** Complainants should review their claims and where necessary, attempt other procedures such as asserting their data subject rights by writing to data handlers. Correspondence between a Complainant and a data handler can serve as evidence when lodging a complaint to ODPC

# ALTERNATIVE DISPUTE RESOLUTION MECHANISMS

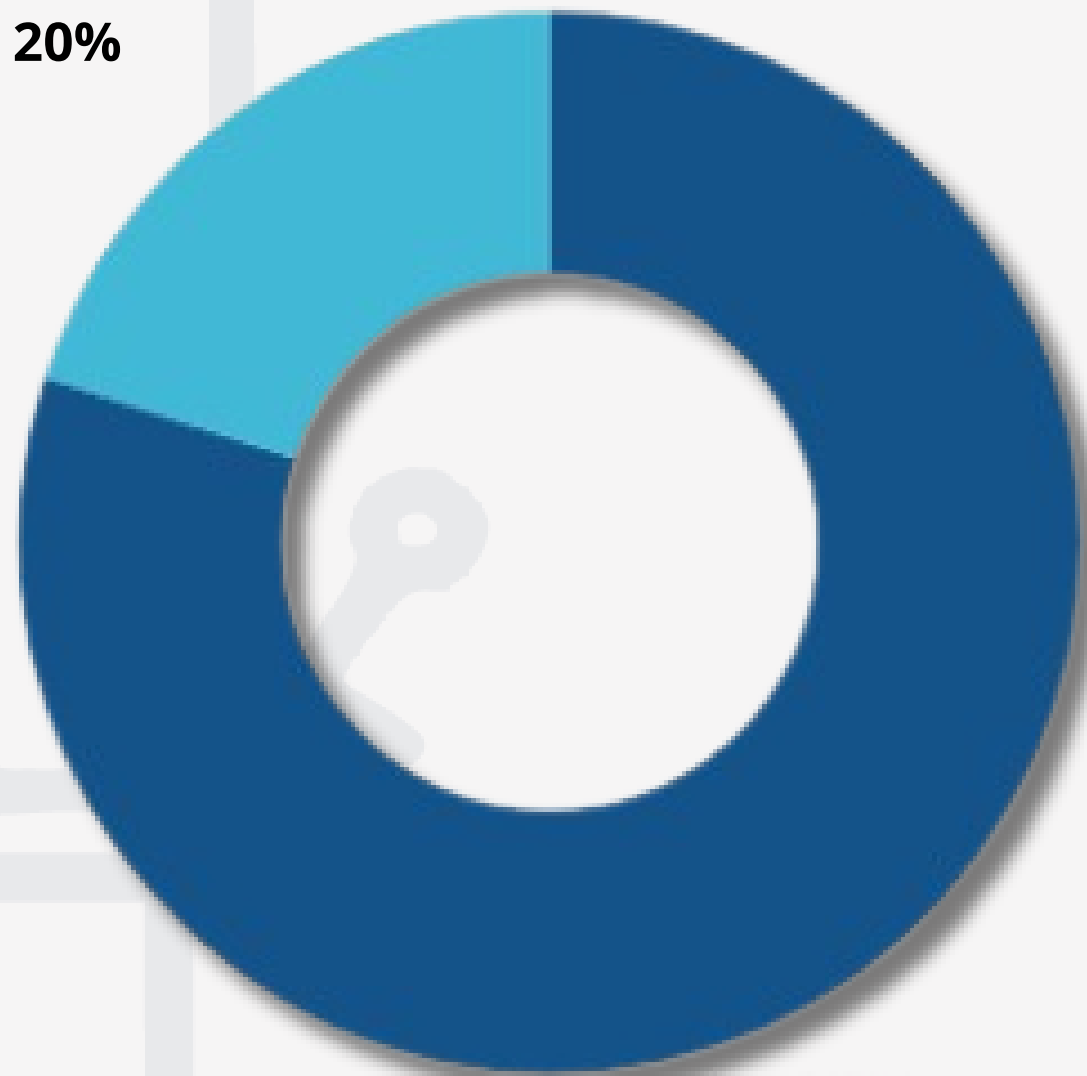
Alternative Dispute Resolution mechanisms are emerging as a significant avenue for resolving data privacy disputes, offering a potentially effective and more amicable alternative to formal legal proceedings.

*Anne Ndun'gu v. Zamaradi Capital & Credit Group LTD* demonstrates that some digital credit providers are embracing ADR, with **7.1% of complaints** against digital credit providers being resolved through this method to the complainants' satisfaction. This suggests a growing recognition of the value of ADR in the data protection landscape. The Data Commissioner has the power to facilitate conciliation, mediation, and negotiation on disputes arising from the Data Protection Act. The Commissioner has put in place an ADR Framework/Guideline for this purpose. ADR mechanisms may be the better alternative to resolving data protection relation disputes. They can be **less adversarial** and **more focused on finding mutually acceptable solutions**. They offer a **more efficient** and **cost-effective** way to settle disagreements, tailoring solutions to your specific needs and circumstances.



# STATUTORY NON-COMPLIANCE

Compliant  
20%



Statutory non-compliant  
80%

An analysis reveals an **80% rate of non-compliance** with data protection regulations, highlighting gaps in how data handlers deal with data subject rights, particularly the right to erasure. To illustrate, in the determination of **Maina Jackson Irungu v Family Bank Ltd**, the bank was fined **Ksh. 250,000** for delays in processing data erasure requests.

The high non-compliance rate points to underlying challenges, including a lack of awareness about legal obligations, technical challenges in managing data, and procedural inefficiencies. With respect to data subject rights management, data handlers ought to:

- Establish a structured protocol for receiving, verifying, and responding to data subject requests.
- Ensure clear communication channels with data subjects.
- Implement identity verification steps to prevent unauthorised access to personal data.
- Maintain compliance timelines set out under the Data Protection (General) Regulations.
- Automate request processing for efficiency where possible.
- Keep records of data subject requests for audit and compliance purposes.

Data handlers should have comprehensive data subject request procedures, train staff on handling requests, leverage on technology, and regularly assess or audit their data protection compliance operations.

# MAJOR LEGAL OR SYSTEMIC CHANGES

On the issue of consent which has featured in a large percentage of the ODPC determinations, data handlers ought to have a robust consent management framework that includes:

- **Clear and Transparent Consent** – Data subjects should understand what they are consenting to in relation to their personal data.
- **Granular Consent** – Separate consent for different personal data processing activities.
- **Revocable Consent** – Data subjects should be able to withdraw consent easily at any time.
- **Documented Consent** – Data handlers should keep records of when, how, and what was consented to.
- **No Pre-Ticked Boxes for Consent** – Active data subject action is required



Clear Consent



Granular Consent



Revocable Consent



Documented Consent



No Pre-Ticked Boxes



## GOVERNMENT AND PUBLIC SECTOR BODIES

**Only two determinations** by the ODPC related to public sector data handlers. The determinations were not as harsh as those that related to private sector data handlers.

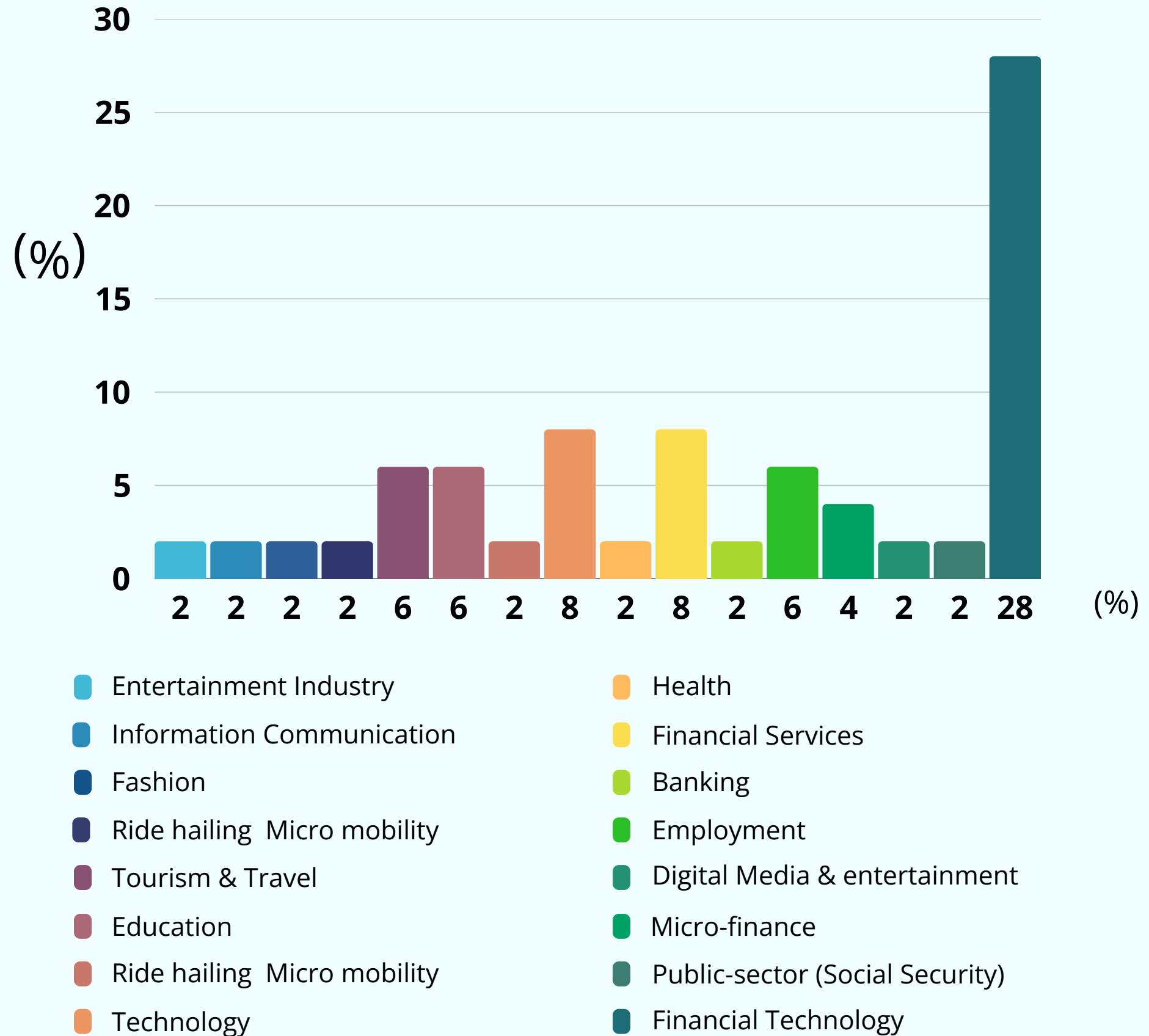
Is it that public sector data handlers are more compliant? or are data subjects not taking action against such handlers?

With public sector data handlers being instrumental to promotion and protection to the right to privacy, ODPC needs to ensure transparency and scrutiny of data protection compliance in the public sector.

# DECISIONS AGAINST DIGITAL LENDERS

Digital lenders accounted for **28% of ODPC determinations** in 2024; with frequent violations including improper consent management, unsolicited communication, harassment of third parties, and aggressive debt collection practices.

Many obstruct ODPC investigations or provide false information. While some complaints are dismissed due to lack of evidence, **alternative dispute resolution** has resolved **7.1%** of the complaints.





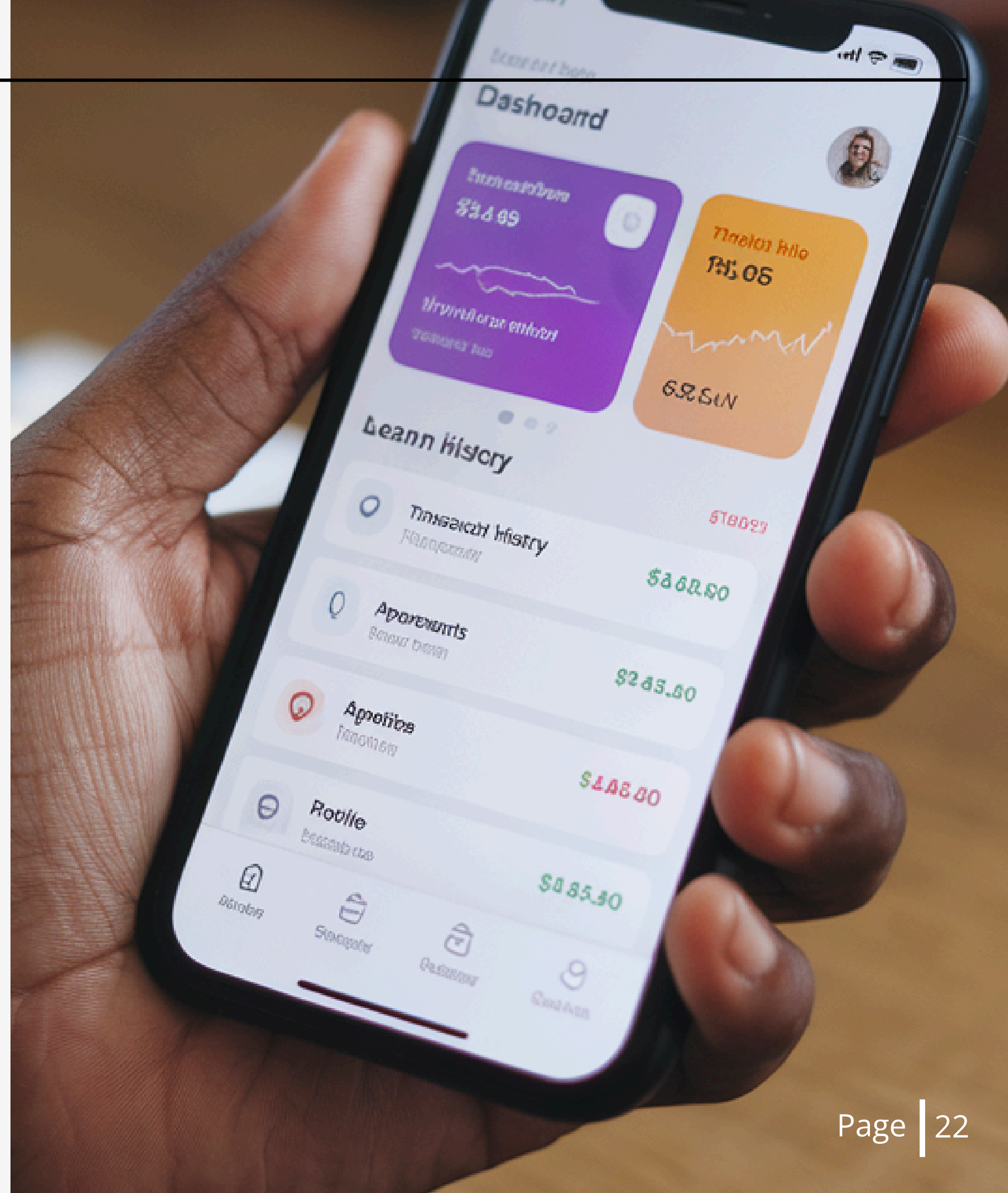
## DIGITAL LENDING SECTOR CHALLENGES

The digital lending sector revealed challenges such as the failure to secure proper consent for data collection, an over-reliance on implied consent, and the use of aggressive unsolicited marketing strategies.

Harassment of third parties, particularly those connected to loan defaulters, is still widespread, compounded by actions that obstruct investigations by ODPC through denying access to data and furnishing misleading information.

A significant number of determinations relating to digital lenders stem from the mishandling of personal data. However, some complaints were dismissed due to insufficient evidence.

To address privacy concerns, digital lenders should implement clear consent mechanisms, adopt ethical marketing practices, cooperate fully with investigations, and strengthen internal data handling processes to improve compliance and reduce the risk of non-compliance.



## CONSISTENCY IN OUTCOMES

This analysis reveals consistency in how ODPC awards damages and issues penalties. However, it is instructive that ODPC publishes the formula used to arrive at awards for damages and penalty notices. Nonetheless, from an analysis of the determinations, key factors such as the **severity of the violation**, the **intent behind it**, and the **data handler's prior compliance record** played significant roles in penalty assessment, with repeat offenders encountering steeper fines.

The determinations indicate a clear prioritization of the **vulnerability of data subjects**, especially when it comes to **minors**, with significant penalties levied for breaches involving minors' data. Commercial benefits derived from unauthorized data usage also result in increased fines.

The ODPC emphasizes **transparency, accountability**, and **cooperation** from data handlers as non-cooperation leads to severe punitive measures.





# CROSS-SECTORAL INSIGHTS

The analysis reveals compliance challenges as prevalent across sectors, with common issues such as **unclear consent**, **inadequate privacy notices**, and **failure to meet statutory timelines**.

Financial services, fintech, and banking face heightened scrutiny due to delays in responding to data subject requests and repeated violations, leading to stricter enforcement.

The health sector struggles with distinguishing express from implied consent, while employment-related privacy concerns revolve around balancing individual rights with national interest.

Digital media, entertainment, and fintech should refine consent management and data processing transparency, while public administration, e-commerce, and the fashion industry should adapt to evolving compliance requirements, particularly regarding data handling and consent records.

# TRENDS AND IMPLICATIONS

In order to enhance data subject trust and institutional transparency, a balance between procedural diligence and responsiveness must be struck.

This is achieved by emphasizing; verification, timeline management, and formal response preparation.

By integrating proactive issue identification, policy assessments, and structured team coordination, the process mitigates risks while reinforcing regulatory adherence.

## Data Protection Complaint Handling Process



## Data Protection Incident Response

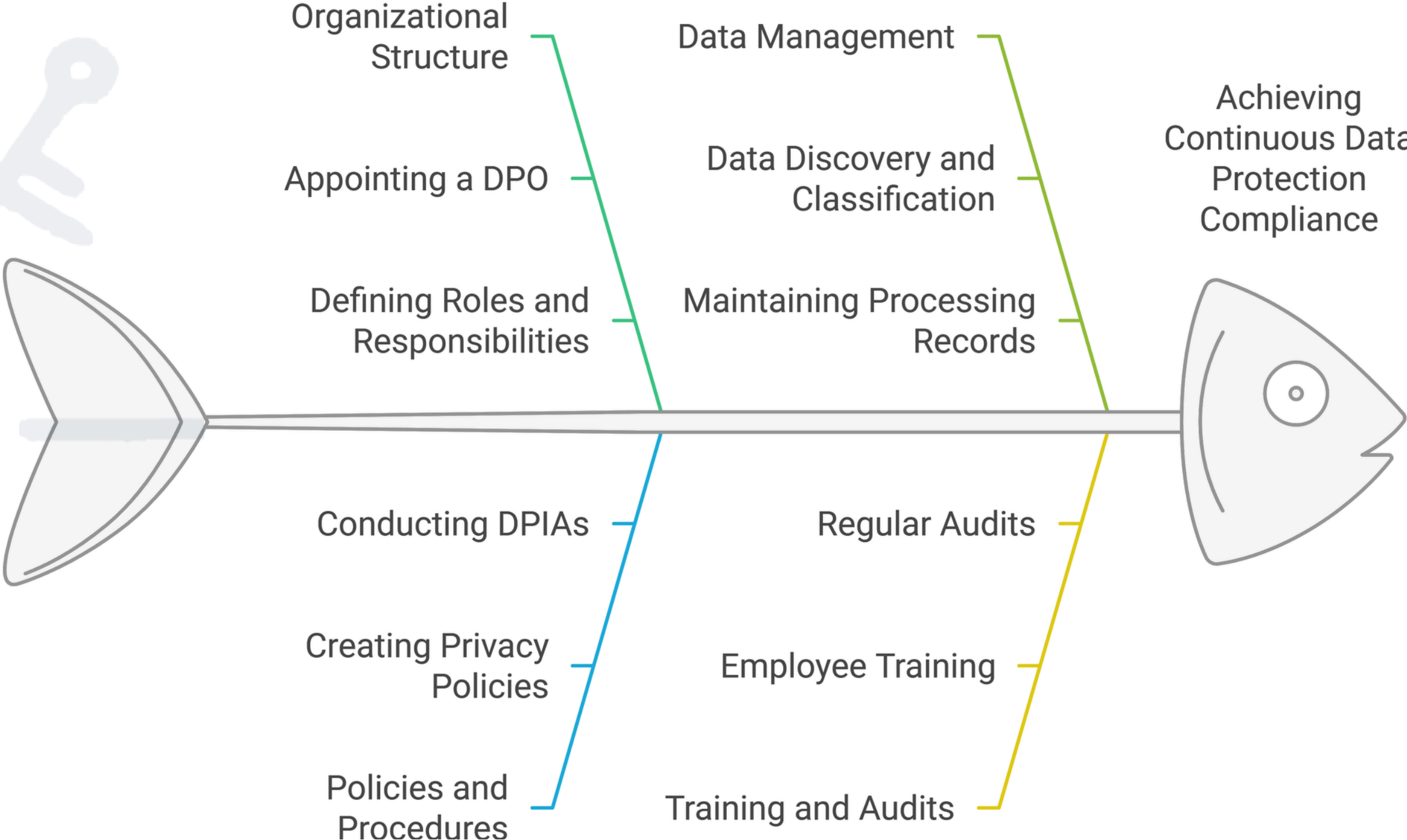


A proactive, multi-layered approach to mitigating breaches and maintaining compliance is integral to incident response.

By integrating continuous monitoring, internal audits, and structured remediation, the process not only ensures regulatory readiness but also reinforces institutional resilience and accountability in handling data security incidents.

# TRENDS AND IMPLICATIONS

Ensuring Data Protection Compliance





# RECOMMENDATIONS FOR POLICYMAKERS

This Report calls for strengthening sector-specific compliance frameworks, particularly for high-risk industries like financial services, health, and education, to address their unique data protection challenges. Sector regulators should explore co-regulation with ODPC to achieve the objectives of the Data Protection Act.

Enhancing regulatory oversight by equipping the ODPC with more resources and ensuring data protection laws keep pace with technological advancements is critical. Public awareness and education are key, with proposed campaigns to inform citizens of their rights and mandatory training for organizations to improve compliance.

Strengthening data subject rights through clearer complaint mechanisms and ensuring timely responses to requests is another priority. Cross-sector collaboration is encouraged to bridge systemic gaps, while leveraging technology is recommended to enhance enforcement and mitigate data breaches.

Additionally, policymakers should monitor informal sectors to identify compliance gaps and implement interventions without stifling innovation. These measures aim to create a strong, adaptable data protection framework that balances individual privacy with economic development.

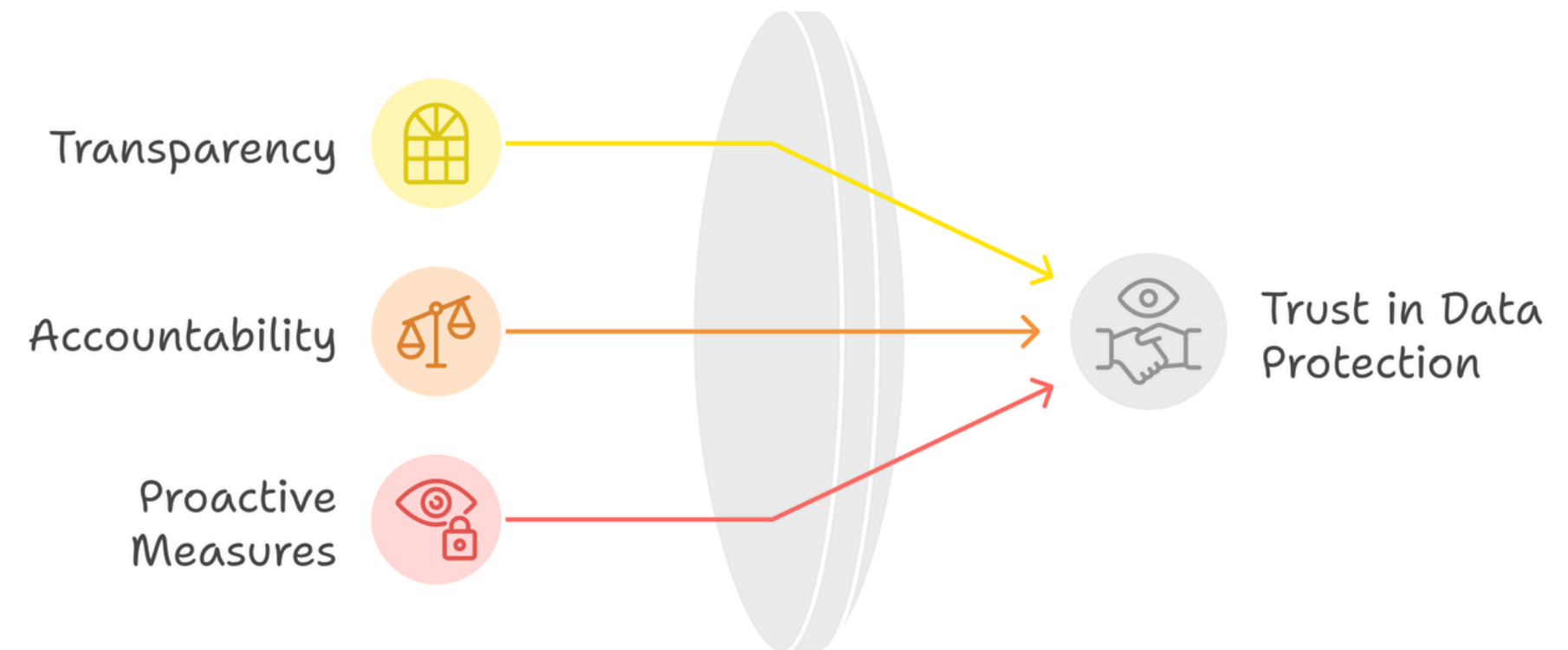
# WHAT NEXT?

The 2024 ODPC determinations highlight Kenya's commitment to data protection enforcement, impacting various sectors.

To promote accountability and trust, data handlers need to **enhance data governance, adopt clear privacy policies, respond promptly** to data requests, and secure personal data. Collaboration across sectors, ongoing training, and investment in compliance are vital for meeting regulatory standards.

As Kenya's data protection environment evolves, shifting from reactive to proactive governance is essential. The ODPC's actions signal a need for a privacy-focused culture that protects rights and supports innovation. Now is the time to implement best practices, making data privacy a competitive advantage.

## Building Trust Through Compliance





To learn more about Data Governance Pros Kenya and how to get involved, please contact us at [info@dataprivacyke.africa](mailto:info@dataprivacyke.africa). You can also connect with us on LinkedIn at Data Governance Pros Kenya and follow us on Twitter at

@DataGovProsKe  
[www.dataprivacyke.africa](http://www.dataprivacyke.africa)

Edited By

Naisenya Katampoi  
Member DPGSK

Grace Mutung'u  
Secretary DPGSK

**DATA PRIVACY & GOVERNANCE SOCIETY**