KENYA PRIVACY LAW REVIEW

VOLUME I,

Consent, Data Protection & Digital Rights:

Forty Case Digests from the Courts and Tribunals of Kenya

40 CASES • 100 PAGES OF CASE DIGEST ANALYSIS

FEATURING TOP CASES

KPLR001

Grain Industries Limited v E.M. & Office of the Data Protection Commissioner

Consent to the commercial use of personal data must be attributable to the data subject herself.

Page 1

KPLR030

Nubian Rights Forum & 2 Others v Attorney General & 6 Others

Biometric data collection by the State must be necessary, proportionate and backed by an adequate legal framework.

Page 73

KPLR032

Republic v Tools for Humanity Corporation (US) & 9 Others

Collection of biometric data (Worldcoin project) without a lawful basis violates the right to privacy under Article 31.

Page 78

LANDMARK DECISIONS

Key judgments shaping data protection jurisprudence in Kenya.

PRACTICAL INSIGHTS

Clear summaries, issues, holdings and ratios for quick reference.

STRATEGIC GUIDANCE

Understand your rights, obligations and risks in a digital world.

ESSENTIAL RESOURCE

For lawyers, DPOs, compliance officers, academics & policy makers.

Muchangi Patrick

Advocate of the High Court of Kenya

Specializing in:

Privacy & Data Protection Law | Data & AI Governance | Technology Law

+254 722 878 607 | +254 736 358 938 | patrick@dataprivacyadvocates.co.ke | www.dataprivacyadvocates.co.ke

KENYA PRIVACY LAW REVIEW

❖

CASE DIGEST SERIES

By *Patrick Muchangi*

VOLUME I

Consent, Data Protection & Digital Rights: Forty Case Digests from the Courts and Tribunals of Kenya

40 CASES · 100 PAGES OF CASE DIGEST ANALYSIS

❖

OMPILED AND EDITED BY

Muchangi Patrick

Advocate of the High Court of Kenya

specializing in:

Privacy & Data Protection Law | Data & AI Governance |Technology Law

+254 722 878 607 • +254 736 358 938 • patrick@dataprivacyadvocates.co.ke • dataprivacyadvocates.co.ke

TABLE OF CASES

Forty case digests, grouped by subject and paginated for reference

PART I — CONSENT, LIKENESS & PURPOSE LIMITATION

PART II — DISCOVERY, ACCESS & THIRD-PARTY DISCLOSURE

PART III — CONFIDENTIALITY, PUBLICATION & STATUTORY MANDATE

PART IV — LAWFUL BASIS, STATUTORY MANDATE & LAW-ENFORCEMENT PROCESS

PART V — DIGITAL IDENTITY, BIOMETRICS & PUBLIC-INTEREST LITIGATION

PART VI — TRIBUNAL DECISIONS ON AUTOMATED DECISION-MAKING & DATA ACCURACY

GLOSSARY OF TERMS

Key terms used throughout this volume, cross-referenced to a leading authority

Article 31

The provision of the Constitution of Kenya, 2010 guaranteeing every person the right to privacy, including protection from unnecessary information about family or private affairs, and from unlawful use or disclosure of information.

See KPLR030, p.73

Complainant / Petitioner / Claimant

The party who initiates a grievance — before the Data Commissioner (complainant), by constitutional petition (petitioner), or by ordinary civil suit (claimant). This Review anonymises this party where they are a private individual.

See Editorial Note, below

Consent

A freely given, specific, informed, and unambiguous indication of a data subject's agreement to the processing of their personal data. An incentive or a pre-existing relationship does not, by itself, establish that consent was voluntary.

See KPLR001, p.1; KPLR032, p.78

Data Commissioner / ODPC

The Office of the Data Protection Commissioner, Kenya's statutory regulator for data protection, established under the Data Protection Act, 2019, with powers to investigate, determine, and enforce compliance.

See KPLR026, p.61

Data Controller

A natural or legal person, public authority, agency, or other body which, alone or jointly, determines the purpose and means of processing personal data.

See KPLR001, p.1

Data Protection Impact Assessment (DPIA)

A documented assessment, required under section 31 of the Data Protection Act where processing is likely to result in high risk, evaluating the origin, nature, and particularity of that risk before processing begins.

See KPLR026, p.61; KPLR032, p.78

Data Subject

An identified or identifiable natural person whose personal data is processed.

See KPLR030, p.73

Enforcement Notice

A notice issued by the Data Commissioner directing a controller or processor to take, or refrain from taking, specified steps to remedy a contravention of the Data Protection Act.

See KPLR004, p.9

Exhaustion (of Remedies)

The principle that a party should generally pursue an available statutory complaint mechanism — such as a complaint to the ODPC — before resorting to constitutional litigation, subject to recognised exceptions.

See KPLR002, p.4; KPLR020, p.43

Personal Data

Any information relating to an identified or identifiable natural person, including a name, identification number, location data, or an online identifier.

See KPLR029, p.70

Processing

Any operation performed on personal data, including collection, recording, storage, alteration, retrieval, disclosure, or destruction.

See KPLR001, p.1

Purpose Limitation

The principle that personal data collected for a specified purpose may not, without independent lawful basis, be processed for a materially different, incompatible purpose.

See KPLR004, p.9; KPLR007, p.17

Ratio Decidendi

The point in a case that determines the outcome — the binding legal principle for which a decision stands as authority, as distinct from obiter dicta or background observation.

See Editorial Note, below

Right to Erasure

A data subject's right to request deletion of their personal data in specified circumstances, including where it is no longer necessary for the purpose for which it was collected.

See KPLR001, p.1

Right to be Informed

A data subject's right to know that their personal data is being collected and the purpose of that collection, ordinarily exercised at or before the point of collection.

See KPLR001, p.1

Sensitive Personal Data

Personal data revealing matters such as race, health, genetic or biometric data, or data concerning a person's sex life, family details, or property, attracting heightened statutory protection.

See KPLR032, p.78; KPLR034, p.83

Stay of Execution

An order suspending enforcement of a determination or decree pending the outcome of an appeal, granted where the applicant shows no unreasonable delay, that substantial loss would otherwise result, and that adequate security is offered.

See KPLR021, p.46

Verification Hold

This Review's own editorial marking for an entry where the primary judgment could not be independently retrieved or fully confirmed at the time of compilation; such entries are not cited for detailed ratio pending verification.

See KPLR007, p.17; KPLR008, p.20

EDITORIAL NOTE

Consistent with this Review's editorial policy, the natural person who brought or was the data subject of each complaint, petition, or claim is identified by initials or procedural role rather than by full name; companies, government offices, and tribunal panel members are named in full. Entries marked Verification Hold could not be fully confirmed against the primary judgment at the time of compilation and should not be cited for detailed ratio without further verification.

KENYA PRIVACY LAW REVIEW

❖

CASE DIGEST SERIES

By *Patrick Muchangi*

VOLUME I · DIGEST NO. 001 · PART I: CONSENT, LIKENESS & PURPOSE LIMITATION

Grain Industries Limited *v* E.M. & Office of the Data Protection Commissioner

[2024] KEHC 14003 (KLR) · Civil Appeal E186 of 2024

High Court of Kenya at Mombasa · Hon. J. K. Ng'arng'ar J. · 12 November 2024

On appeal from ODPC Complaint No. 387 of 2024

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Mombasa (Civil Appeal)
OUTCOME	*Appeal dismissed; Commissioner's determination upheld in full*
COMPENSATION	**KES 1,000,000 (upheld)**
CORE QUESTION	***Whether an intermediary's consent may substitute for the data subject's own consent to processing personal data?***

PRINCIPAL DOCTRINE

> *Consent to the commercial use of personal data must be attributable to the data subject herself; a controller may not rely on consent obtained from another person in relation to her image.*

BRIEF FACTS

Grain Industries Limited used E.M.'s photograph, without her consent, on billboards along the Mombasa–Malindi Highway and in YouTube and social-media advertising captioned "Tunashukuru mama wa Ajabu." She came upon the billboard herself on or about 30 August 2023; the image had reached the company indirectly, through a marketing arrangement made separately by her adult daughter.

On her complaint of 6 March 2024, the Data Commissioner's officers inspected the sites, confirmed the billboards had since been removed, and found the use unlawful for want of the Respondent's own consent — together with violations of her rights to be informed and to erasure. She was awarded KES 1,000,000 in compensation, and an enforcement notice was issued.

Grain Industries appealed on procedural grounds and on the finding that her adult daughter should be treated as a data controller in her own right.

ISSUES

1. Whether the Commissioner violated Grain Industries' procedural and fair-hearing rights.
2. Whether the Commissioner's determination was issued within the statutory period.
3. Whether Grain Industries unlawfully processed the Respondent's personal data.
4. Whether Grain Industries had complied with its obligations under the Data Protection Act.
5. Whether the compensation awarded was justified.

HOLDING

Appeal dismissed. The High Court upheld the Commissioner's determination in full — findings on the rights to be informed and to erasure, and on unauthorised commercial use — together with the KES 1,000,000 award. Neither the procedural nor the limitation-period objection warranted disturbing it; consent, the Court held, must be connected to the actual data subject.

COURT'S REASONING

Commercial use of the Respondent's image was processing of her personal data, requiring a lawful basis tied to her as the data subject. That the photograph reached the company through her daughter did not, without more, establish her own authorisation.

A family, agency, or intermediary relationship does not by itself establish the data subject's consent: authorisation must be traceable to her, and to the specific processing undertaken.

RATIO DECIDENDI

> *A controller using an individual's image commercially must establish a lawful basis attributable to that individual. An intermediary's consent, absent proof of authority to bind the data subject, is no substitute.*

SIGNIFICANCE

Binding on advertisers and marketers using personal likenesses: consent is personal to the data subject, and lawful possession of an image confers no automatic authority to repurpose it commercially.

> **KEY TAKEAWAY**
> *Possession of an image, or an intermediary's consent, is not consent from the person depicted. Demonstrate your own lawful basis for the specific commercial use.*

Source: Kenya Law · [2024] KEHC 14003 (KLR)

❖

CASE DIGEST · KPLR 002

VOLUME I · DIGEST NO. 002 · PART I: CONSENT, LIKENESS & PURPOSE LIMITATION

M. *v* Julie Njuhi Muiruri (T/A Human Hair Center)

[2024] KEHC 6970 (KLR) · Petition E032 of 2023
High Court of Kenya at Nairobi · Hon. L. N. Mugambi J. · 13 June 2024

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Constitutional Petition
OUTCOME	Petition succeeds; Respondent liable for unauthorised commercial use of the Petitioner's image
COMPENSATION	KES 240,000 (privacy & dignity) plus costs
CORE QUESTION	Whether a licence to one business extends to an unrelated third party's commercial use

PRINCIPAL DOCTRINE

> *Where commercial exploitation of a person's image implicates dignity and privacy beyond ordinary data processing, the High Court's constitutional jurisdiction is not ousted by the Data Protection Act's exhaustion requirement.*

BRIEF FACTS

The Petitioner contracted with New Level Collection Limited on 19 January 2022 to provide modelling services for one year — an arrangement that, during its term, barred her from entering any other modelling agreement. Around 2022, she discovered her photographs advertising hair products on the Instagram page of the Respondent, a business with no agreement with her, or, on her case, with New Level Collection for that purpose.

On her complaint, New Level Collection had the photographs removed. The Respondent nonetheless maintained the claim was unfounded, relying on the relationship between the Petitioner and the modelling agency through which the images had been obtained, and raised a preliminary objection that the dispute should first have gone to the Data Commissioner.

The central factual question was whether the Petitioner's contractual relationship with New Level Collection authorised an unrelated third party, the Respondent, to use her image for its own commercial advertising. She sued, denying consent and framing the claim as implicating her constitutional rights to dignity, privacy, and property.

ISSUES

1. Whether the preliminary objection on exhaustion was merited.
2. Whether the Respondent violated the Petitioner's rights to dignity, privacy, and property under Articles 28, 31, and 40.
3. Whether the Petitioner was entitled to the reliefs sought.

HOLDING

Petition allowed. The Court rejected the exhaustion objection — the claim's constitutional dimensions took it beyond the Data Protection Act's ordinary complaint mechanism — and found the Respondent's commercial exploitation of the Petitioner's image, without her consent, violated her rights to dignity and privacy. It awarded KES 240,000 in compensation, with costs.

COURT'S REASONING

Although section 8(1)(f) of the Data Protection Act empowers the Commissioner to investigate processing complaints, the petition invoked dignity, privacy, and property under Articles 28, 31, and 40 — claims the statutory mechanism did not confine, leaving the High Court's Article 165(3)(b) jurisdiction intact.

On the merits, the Petitioner's agreement was with New Level Collection alone; the Respondent, a stranger to that contract, could not treat it as authority to exploit her image for its own advertising. A licence to one entity is not a licence to another.

RATIO DECIDENDI

> *A contractual licence to use a person's image, granted to one entity, does not extend to an unrelated third party absent an independent legal basis; and where commercial exploitation of an image implicates dignity and privacy, the claim may proceed constitutionally without first exhausting the Data Protection Act's complaint mechanism.*

SIGNIFICANCE

Clarifies that image and personality-rights claims bound up with dignity and privacy need not first exhaust ODPC complaint procedures, and confirms that a business cannot rely on a rival's licensing arrangement to justify its own commercial use of someone's likeness.

> **KEY TAKEAWAY**
>
> *A licence you were never given is not yours to rely on. Verify your own lawful basis before commercially using an image obtained through someone else's arrangement.*

Source: Kenya Law · [2024] KEHC 6970 (KLR)

❖

CASE DIGEST · KPLR 003

VOLUME I · DIGEST NO. 003 · PART I: CONSENT, LIKENESS & PURPOSE LIMITATION

MIND QUEST LIMITED *v* M. & 2 OTHERS

[2025] KEHC 3891 (KLR) · Civil Appeal E674 of 2024

High Court of Kenya at Nairobi · Hon. S. N. Mutuku J. · 5 March 2025

On appeal from ODPC Complaint No. 151 of 2024, decided 22 April 2024

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Civil Appeal
OUTCOME	Appeal allowed; Commissioner's determination and compensation set aside
COMPENSATION	KES 1,500,000 award set aside; each party to bear own costs
CORE QUESTION	Whether an unproven model-release agreement could establish a time-limited consent

PRINCIPAL DOCTRINE

> *A complainant alleging that consent was contractually confined to a fixed period must prove the existence and terms of that limitation; the Data Protection Act's burden on controllers to show consent does not excuse a complainant from proving the contractual restriction relied upon.*

BRIEF FACTS

MIND QUEST LIMITED used photographs of the Respondents taken at a commercial photoshoot for its "Accessorize with Style" brand, engaged through Couture Magazine and evidenced by an invoice dated 17 May 2017; the Respondents had each already been paid KES 5,000 for their images.

The Respondents alleged Mind Quest continued using the photographs beyond the period to which they said they had agreed, and claimed KES 700,000 per year of unauthorised use — KES 6.3 million in total — together with cessation and removal of the images.

On complaint, the Data Commissioner found Mind Quest liable for commercial use without express consent and awarded KES 1.5 million. Mind Quest appealed, disputing the finding of no consent and arguing the Commissioner had wrongly relied on an unexecuted draft contract to infer a three-year limit on the permitted use.

ISSUES

1. Whether a valid contract existed between Mind Quest and the Respondents.
2. Whether the evidence established the scope and duration of consent.
3. Whether the Commissioner properly weighed the documents presented.
4. Whether the continued commercial use of the images was unlawful.
5. Whether the compensation award could stand.

HOLDING

Appeal allowed. The High Court set aside both the Commissioner's determination and the KES 1,500,000 award; each party was ordered to bear its own costs.

COURT'S REASONING

The Respondents relied on a model-release agreement but produced no signed copy — the record held only a blank template. The Court could not determine whether a binding contract existed, its terms, or whether it truly limited image use to three years.

Section 32(1) of the Data Protection Act places the burden of proving consent on the controller, but that burden does not relieve a complainant of proving the factual foundation of a contractual restriction they themselves allege.

RATIO DECIDENDI

> *A complainant alleging that consent was contractually confined to a fixed period must prove the existence and terms of that limitation; the controller's statutory burden to demonstrate consent does not substitute for that proof.*

SIGNIFICANCE

Clarifies that the Data Protection Act's burden-shifting on consent operates alongside, not instead of, ordinary evidentiary rules: a complainant who alleges a specific contractual limit must still prove it.

> **KEY TAKEAWAY**
>
> *An unsigned template proves nothing. If you rely on a model-release period to challenge continued use, produce the signed agreement — not a blank draft.*

Source: Kenya Law · [2025] KEHC 3891 (KLR)

❖

CASE DIGEST · KPLR 004

VOLUME I · DIGEST NO. 004 · PART I: CONSENT, LIKENESS & PURPOSE LIMITATION

AVENTUS TECHNOLOGY LIMITED *v* D.N.

[2025] KEHC 9218 (KLR) · Civil Appeal 447 of 2024
High Court of Kenya at Nairobi · Hon. A. N. Ongeri J. · 27 June 2025
On appeal from ODPC Complaint No. 2506 of 2023

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Civil Appeal
OUTCOME	Appeal dismissed; determination and compensation upheld; compliance directed within 30 days
COMPENSATION	KES 250,000 (upheld)
CORE QUESTION	Whether data given to identify an emergency contact could be repurposed for debt-collection calls

PRINCIPAL DOCTRINE

> *Personal data supplied to identify an emergency contact cannot automatically be repurposed for debt collection; purpose limitation confines processing to the function for which the data was given.*

BRIEF FACTS

AVENTUS TECHNOLOGY LIMITED, through agents collecting on a Lendplus loan, repeatedly called the Respondent from various numbers, subjecting him to verbal abuse over a debt he said was not his own. He had never borrowed from Lendplus; on his account, another person had listed him as an emergency contact, without his details being repurposed for debt recovery in mind.

Aventus maintained that the actual borrower had supplied the Respondent's number as a contact person to be reached when the borrower was unavailable, and denied that it had itself improperly controlled the data.

On complaint, the Data Commissioner found the Respondent's rights violated, awarded him KES 250,000 in compensation, and issued an enforcement notice. Aventus appealed, denying that the processing was properly attributed to it and disputing the evidentiary basis for the compensation awarded.

ISSUES

1. Whether Aventus lawfully processed the Respondent's personal data.
2. Whether information supplied to identify an emergency contact could be repurposed for debt recovery.
3. Whether the Commissioner properly attributed the processing to Aventus.
4. Whether the compensation award was justified.

HOLDING

Appeal dismissed. The High Court upheld the Commissioner's determination and the KES 250,000 compensation, and directed compliance with the enforcement notice within 30 days.

COURT'S REASONING

Lawful collection of personal data for one purpose creates no general licence for a different, incompatible purpose; an emergency-contact number is supplied for that limited function alone.

It cannot be converted into a debt-collection communication channel without its own lawful basis — the borrower's disclosure of the Respondent's number did not supply one.

RATIO DECIDENDI

The lawful collection of personal data for one purpose does not create a licence for subsequent incompatible processing; an emergency-contact number cannot be repurposed as a debt-collection channel absent an independent lawful basis.

SIGNIFICANCE

Directly relevant to digital lenders and collection agents: data supplied by a third party for a limited reference function may not be redirected to debt-recovery communications without separately justifying that new purpose.

KEY TAKEAWAY

An emergency contact is not a debt-collection target. Verify the lawful basis for each new purpose before repurposing data a third party supplied for something else.

Source: Kenya Law · [2025] KEHC 9218 (KLR)

❖

CASE DIGEST · KPLR 005

VOLUME I · DIGEST NO. 005 · PART I: CONSENT, LIKENESS & PURPOSE LIMITATION

METROPOLIS STAR LAB KENYA LTD *v* J.K. & ANOTHER

[2025] KEHC 8211 (KLR) · Civil Appeal E1140 of 2024

High Court of Kenya at Nairobi · Hon. A. C. Mrima J. · 12 June 2025

On appeal from consolidated ODPC Complaints Nos. 0784 and 0916 of 2024

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Civil Appeal
OUTCOME	Appeal allowed; determination quashed for procedural unfairness and remitted
COMPENSATION	None — determination quashed; each party to bear own costs
CORE QUESTION	Whether the ODPC's own complaints process complied with Articles 47 and 50(1)

PRINCIPAL DOCTRINE

> *A statutory regulator's own status does not exempt its complaints process from the constitutional and statutory guarantees of procedural fairness owed to the party under investigation.*

BRIEF FACTS

METROPOLIS STAR LAB KENYA LTD was the subject of consolidated ODPC complaints — Nos. 0784 and 0916 of 2024 — brought by the Respondents, who alleged their telephone numbers were used for marketing despite repeated opt-out requests. The Commissioner investigated and determined against the company.

Metropolis appealed, contending it had not been afforded a fair and procedurally lawful opportunity to respond to aspects of the investigation and determination, invoking Article 47, Article 50(1), the Fair Administrative Action Act, and the Data Protection (Complaints Handling Procedure and Enforcement) Regulations.

The Respondents maintained that the underlying processing of their numbers for marketing was itself unlawful, and that their rights had been violated notwithstanding their attempts to opt out.

ISSUES

1. Whether the Commissioner followed a lawful and procedurally fair complaints process.
2. Whether the Appellant received the procedural protections required by Article 47.
3. Whether the Article 50(1) fair-hearing requirements applied and were met.
4. Whether the Data Protection Act complaints regulations had been followed.
5. Whether the determination could stand despite the procedural defects.

HOLDING

Appeal allowed. The High Court declared the Commissioner's determination non-compliant with Article 47, Article 50(1), the Fair Administrative Action Act, and the Complaints Handling Procedure and Enforcement Regulations, quashed it, and remitted the matter for fresh determination according to law, with each party to bear its own costs.

COURT'S REASONING

The Commissioner is a statutory regulator, but that status does not exempt its own complaints process from the constitutional and statutory guarantees of procedural fairness owed to the party under investigation.

Regulation 3 commits the complaints process to fairness, impartiality, and due expedition, and Regulation 13(3) requires the Commissioner, when investigating, to be guided by the Fair Administrative Action Act — obligations the Court found had not been met.

RATIO DECIDENDI

A regulator's own procedural fairness obligations under Articles 47 and 50(1), and under its governing complaints regulations, apply with full force to its own investigative and determinative process; non-compliance renders the determination liable to be quashed regardless of the substantive merits.

SIGNIFICANCE

A caution to the ODPC as much as to controllers: an otherwise sound substantive finding cannot rescue a determination reached through an unfair process. Controllers under investigation should test the process itself, not only the outcome.

KEY TAKEAWAY

A regulator must follow its own rules. If you are investigated without fair notice or a genuine chance to respond, the determination — however substantively justified — is vulnerable on procedure alone.

Source: Kenya Law · [2025] KEHC 8211 (KLR)

❖

CASE DIGEST · KPLR 006

VOLUME I · DIGEST NO. 006 · PART I: CONSENT, LIKENESS & PURPOSE LIMITATION

K. *v* Chuka University

[2026] KEHC 3493 (KLR) · Constitutional Petition E001 of 2023
High Court of Kenya at Chuka · Hon. R. L. Korir J. · 17 March 2026

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Chuka — Constitutional Petition
OUTCOME	Petition dismissed on the merits; jurisdiction upheld but infringement not proved
COMPENSATION	None — petition dismissed; each party to bear own costs
CORE QUESTION	Whether the Petitioner proved he was identifiable in the photograph and that the University was responsible

PRINCIPAL DOCTRINE

> *Establishing jurisdiction over a privacy claim does not establish liability; a claimant alleging unauthorised use of an image must still prove identification, provenance, and use by the respondent.*

BRIEF FACTS

The Petitioner alleged that Chuka University had used his image, as part of a group photograph, for financial or commercial purposes without his consent. An earlier preliminary objection challenging the High Court's jurisdiction over the claim had already been dismissed.

The proceedings that followed therefore turned on a distinct question: not whether the Court had jurisdiction — that was settled — but whether the Petitioner could actually prove the infringement he alleged, including that he was identifiable in the photograph and that the University was responsible for its use.

ISSUES

1. Whether the Court retained jurisdiction despite the ODPC's statutory mechanism.
2. Whether the earlier jurisdictional ruling precluded re-litigation of the same objection.
3. Whether the Petitioner established that he was identifiable in the photograph.
4. Whether he proved the University was responsible for the image.
5. Whether the alleged use violated Articles 28, 31, and 40.

HOLDING

Petition dismissed. The Court confirmed its jurisdiction but found the Petitioner had not established, on the balance of probabilities, that he was among the persons depicted or that the photograph originated from the University. Each party was ordered to bear its own costs.

COURT'S REASONING

Clearing a jurisdictional or exhaustion objection settles only the Court's power to hear the claim; it does not establish substantive liability. A claimant alleging unauthorised use of an image must still prove the essential factual elements — identification, provenance, and use by the respondent.

On the evidence, the Petitioner could not establish either that he appeared in the photograph or that it came from the University, and the petition failed on that footing alone.

RATIO DECIDENDI

Surviving a jurisdictional or exhaustion challenge does not establish substantive liability; a claimant alleging unauthorised use of an image must still prove identification, provenance, and use by the respondent on the ordinary civil standard.

SIGNIFICANCE

A cautionary case for claimants: a privacy or image-rights claim cannot rest on an assertion that a photograph may contain the claimant. It also confirms that jurisdictional victories are procedural only, not a shortcut to the merits.

KEY TAKEAWAY

Winning the jurisdiction argument is not winning the case. If you allege your image was used without consent, be ready to prove it is actually you, and where the image came from.

Source: Kenya Law · [2026] KEHC 3493 (KLR)

❖

CASE DIGEST · KPLR 007

VOLUME I · DIGEST NO. 007 · PART I: CONSENT, LIKENESS & PURPOSE LIMITATION

JAGGYS (KIENYEJI CHICKEN) *v* G.

[2026] KEHC 6856 (KLR) · Civil Appeal E657 of 2024

High Court of Kenya · Coram and exact date not confirmed in the available record

THE CASE AT A GLANCE	
FORUM	High Court of Kenya — Civil Appeal
OUTCOME	Appeal partly succeeds; unlawful processing affirmed, compensation varied down
COMPENSATION	KES 50,000 (varied down from the ODPC's original KES 250,000)
CORE QUESTION	Whether a phone number obtained for an M-Pesa transaction could be repurposed for direct marketing

PRINCIPAL DOCTRINE

> *Transactional acquisition of a customer's telephone number does not itself constitute consent to use that number for direct marketing; purpose limitation follows the data even where it was lawfully obtained in the first place.*

BRIEF FACTS

JAGGYS, TRADING AS KIENYEJI CHICKEN, obtained the Respondent's mobile number in connection with an M-Pesa transaction and later used it to send promotional direct-marketing messages, without his express consent to that different purpose.

The Respondent purchased chicken from the Appellant, ***Jaggys (Kienyeji Chicken)***, and paid for the transaction through **M-Pesa**. In the course of that transaction, the Appellant obtained the Respondent's mobile phone number.

The Appellant subsequently used the Respondent's phone number to send **promotional/marketing messages** to him. The Respondent had **not consented to the use of his phone number for direct marketing**.

The Respondent complained to the **Office of the Data Protection Commissioner (ODPC)**. The ODPC found that the Appellant had unlawfully processed the Respondent's personal data and awarded **KShs. 250,000 compensations**.

The Appellant appealed to the High Court, challenging the ODPC's determination and the compensation awarded. The High Court upheld the finding of unlawful processing but **reduced the compensation to KShs. 50,000**, considering the limited nature of the infringement and the absence of financial loss or disclosure to third parties.

ISSUES

1. Whether the phone number obtained during the payment transaction could lawfully be used for marketing.
2. Whether the original transactional purpose authorised subsequent direct marketing.
3. Whether consent was required for the new purpose.
4. Whether the compensation awarded by the Commissioner was proportionate.

HOLDING

Appeal allowed in part. The High Court affirmed that transactional acquisition of a customer's telephone number does not itself constitute consent to use that number for direct marketing, but varied the compensation award down from KES 250,000 to KES 50,000.

COURT'S REASONING

Purpose limitation operates at the level of the specific purpose for which data was obtained; collecting a telephone number to process an M-Pesa transaction does not automatically authorise its later use for promotional communications.

Liability and quantum are separate questions: that processing was unlawful does not mean every infringement attracts the same level of compensation.

RATIO DECIDENDI

> *Purpose limitation follows the data even where it was lawfully obtained: a telephone number collected for a transactional purpose may not automatically be used for direct marketing, and compensation for such an infringement is assessed on its own facts rather than by a fixed quantum.*

SIGNIFICANCE

Relevant to any business collecting phone numbers through M-Pesa, card payments, till systems, bookings, or account-opening: transactional data cannot be folded into a marketing programme without its own lawful basis.

> **KEY TAKEAWAY**
> *A number collected to complete a payment is not a marketing list entry. Keep transactional and marketing purposes separate, and document the lawful basis for each.*

Source: Kenya Law · [2026] KEHC 6856 (KLR) — primary judgment not independently retrieved; corroborated by secondary commentary only.

❖

CASE DIGEST · KPLR 008

VOLUME I · DIGEST NO. 008 · PART I: CONSENT, LIKENESS & PURPOSE LIMITATION

St Joseph Health Care *v* M.

Citation, coram, and full case number not confirmed in the available record
High Court of Kenya — Civil Appeal (nature confirmed; further particulars not confirmed)

THE CASE AT A GLANCE	
FORUM	High Court of Kenya — Civil Appeal
OUTCOME	Appeal allowed; underlying ODPC determination set aside
COMPENSATION	Original ODPC award set aside on appeal; figure not confirmed in the available record
CORE QUESTION	Whether a former employee's image was used in institutional publications without consent
VERIFICATION	***Full judgment not retrieved; only the principal doctrine, a skeletal fact pattern, and the bare disposition are available — do not cite for detailed ratio***

PRINCIPAL DOCTRINE

> *The Data Protection Act does not authorise continued use of a former data subject's image in institutional publications once the relationship underlying the original consent has ended, without a fresh lawful basis for the continued use.*

BRIEF FACTS

The Respondent was formerly associated with St Joseph Health Care and alleged that his image continued to appear in the institution's publications after that association had ended, without a fresh lawful basis for that continued use.

The Data Commissioner determined the continued use unlawful and made an award in the Respondent's favour; St Joseph Health Care appealed.

ISSUES

1. Whether continued use of the Respondent's image after the relationship ended required a fresh lawful basis.
2. Whether the Commissioner's determination was properly reasoned.
3. Whether the appeal disclosed grounds to set the determination aside.
4. Whether the original compensation award could stand.

HOLDING

Appeal allowed; the ODPC determination was set aside. The corpus available for this digest preserves only that the appeal succeeded and the determination was set aside — the High Court's detailed reasoning is not presently available for citation.

COURT'S REASONING

Not available in the material accessible for this digest. Consistent with this project's verification standard, no reasoning is reconstructed by inference; this entry will be completed once the primary judgment is retrieved and checked.

RATIO DECIDENDI

Not established in the material presently available. Do not cite this entry for a specific ratio pending verification against the original judgment.

SIGNIFICANCE

Provisionally allocated to consent and purpose-limitation for continued use of a person's image following the end of the relationship that originally justified it — to be confirmed once the primary judgment is verified.

KEY TAKEAWAY

Consent tied to a relationship does not survive indefinitely. Revisit the lawful basis for using a person's image once the relationship that justified the original use has ended.

Source: Kenya Law — full judgment not independently retrieved for this digest; verification required before further reliance.

❖

CASE DIGEST · KPLR 012

VOLUME I · DIGEST NO. 012 · PART II: DISCOVERY, ACCESS & THIRD-PARTY DISCLOSURE

G.M. & ANOTHER *v* MICROSOFT EAST AFRICA LIMITED

[2021] KEELRC 526 (KLR) · Petition No. 223 of 2019 (consolidated with Petition No. 6 of 2020)
Employment and Labour Relations Court at Nairobi · Hon. J. Rika J. · 9 November 2021

THE CASE AT A GLANCE	
FORUM	Employment and Labour Relations Court at Nairobi — Consolidated Petitions
OUTCOME	Application to compel production of non-party employee records declined
COMPENSATION	Not applicable — interlocutory discovery ruling; no order as to costs
CORE QUESTION	Whether comparator evidence for a discrimination claim justifies disclosing non-party employees' private payslips

PRINCIPAL DOCTRINE

> *Third-party employees' records cannot ordinarily be compelled merely because they may assist a discrimination claim; privacy and data-protection obligations continue to protect non-party employees even where their information could serve as comparator evidence.*

BRIEF FACTS

THE PETITIONERS, former employees of Microsoft East Africa Limited, alleged they had been denied performance bonuses on account of race and sought declarations of discrimination, payment of the withheld bonuses, and damages. By an application dated 2 November 2020, they sought an order compelling Microsoft's Human Resource Manager to produce three named comparator employees' certified payslips for the bonus period, together with each comparator's performance results from Microsoft's internal MINT system.

Their stated purpose was to compare performance, work done, and bonuses paid across the group, and they proposed that the comparator records be certified confidential and sealed, available only to the Court and the parties.

Microsoft opposed the application as a fishing expedition into the private, confidential records of employees who were not parties to the suit, and warned that production could itself expose it to liability under the Data Protection Act.

Patrick Muchangi

ISSUES

1. Whether the Court should compel production of the non-party employees' payslips and performance information.
2. Whether the Petitioners could establish their discrimination claim without compelling those records.
3. Whether the proposed confidentiality and sealing safeguards adequately addressed the comparators' privacy interests.

HOLDING

Application declined, with no order as to costs. The Court found the Petitioners could prosecute their discrimination claim without infringing their former colleagues' privacy and confidentiality, and declined to strike out Microsoft's response for non-production.

COURT'S REASONING

Each employee's remuneration was individually agreed and contractual; the Court treated the payslips as private and confidential records regardless of their possible evidential value.

Placing the documents before the Court would not remove their private character — once part of the court record, they would become subject to public scrutiny and contestation, so the Court weighed not merely initial disclosure but its downstream consequences.

RATIO DECIDENDI

> *A party alleging discrimination must establish the evidential basis of the claim; a court will not necessarily facilitate a fishing expedition into the confidential employment records of non-party employees merely because that information could serve as comparator evidence.*

SIGNIFICANCE

An early post-DPA authority confirming that litigation need, however genuine, does not itself extinguish a non-party's privacy interest in their employment records; relevance is not synonymous with automatic discoverability.

> **KEY TAKEAWAY**
> *Needing comparator evidence is not enough. Identify precisely what you need and why it's necessary — courts will protect a non-party colleague's payslip even from a genuine discrimination claim.*

Source: Kenya Law · [2021] KEELRC 526 (KLR)

❖

CASE DIGEST · KPLR 013

VOLUME I · DIGEST NO. 013 · PART II: DISCOVERY, ACCESS & THIRD-PARTY DISCLOSURE

N.K. *v* Credit Bank PLC

[2024] KEELRC 2142 (KLR) · Cause E555 of 2023
Employment and Labour Relations Court at Nairobi · Hon. L. Ndolo J. · 31 July 2024

THE CASE AT A GLANCE	
FORUM	Employment and Labour Relations Court at Nairobi — Employment Cause
OUTCOME	Discovery application disallowed, with costs in the cause
COMPENSATION	Not applicable — interlocutory discovery ruling
CORE QUESTION	Whether a request for entire email accounts, rather than identified documents, meets the threshold for discovery

PRINCIPAL DOCTRINE

> *A discovery application seeking access to an entire institutional email account is impermissible where the applicant fails to identify specific documents that are relevant and necessary to the proceedings.*

BRIEF FACTS

The Claimant, formerly employed by Credit Bank PLC, lost access to her official email accounts when her employment ended. By a Notice of Motion dated 29 January 2024, she sought access to her employment contracts and to all correspondence between 1 February 2019 and 8 March 2023 from her individual account and from a shared Westlands branch account, for use as evidence in her employment case.

Credit Bank opposed the application, explaining that the Westlands account was a group account used by multiple staff and containing customer as well as employee communications, and that the Claimant already held the documents necessary to prosecute her case.

The Bank argued the request was vague, amounted to a fishing expedition, and that unrestricted access to a shared account risked violating Article 31 and the Data Protection Act by exposing third parties' communications.

ISSUES

1. Whether the Claimant established a proper basis for discovery.
2. Whether she had identified specific documents sought.
3. Whether the requested email access was relevant and necessary.
4. Whether unrestricted access would compromise third-party privacy.
5. Whether the application amounted to a fishing expedition.

HOLDING

Application disallowed, with costs in the cause. The Court found it a broadside application that failed to identify the specific documents sought, falling below the threshold for proper discovery.

COURT'S REASONING

Established discovery principles require that documents sought be specific, relevant, and necessary. The Claimant had not identified particular emails or documents — she sought access to entire accounts instead, and that distinction was decisive.

Drawing on Concord Insurance Co Ltd v NIC Bank Ltd and related authorities, the Court held that a litigant cannot use discovery to obtain unrestricted access to an opponent's electronic information environment; the shared account's mix of customer and employee communications made the risk to third-party privacy concrete, not speculative.

RATIO DECIDENDI

A litigant cannot use discovery to obtain unrestricted access to an opponent's electronic information environment; the applicant must identify the documents sought and demonstrate their relevance and necessity, particularly where a shared account implicates third-party privacy.

SIGNIFICANCE

Extends the specificity-relevance-necessity discovery framework into electronic discovery: a request for 'all emails' is fundamentally different from a request for identified emails relating to an identified issue, and the Data Protection Act makes unstructured, excessive disclosure legally dangerous rather than impossible.

KEY TAKEAWAY

Never ask for a whole inbox. Identify the specific emails or documents you need and why — a request for an entire account will be treated as a fishing expedition.

Source: Kenya Law · [2024] KEELRC 2142 (KLR)

❖

CASE DIGEST · KPLR 014

VOLUME I · DIGEST NO. 014 · PART II: DISCOVERY, ACCESS & THIRD-PARTY DISCLOSURE

TRV TOWERS LIMITED *v* BANK OF INDIA

[2024] KEHC 12927 (KLR) · Miscellaneous Civil Application E920 of 2023
High Court of Kenya at Nairobi (Milimani Commercial Courts) · Hon. J.W.W. Mong'are J. · 25 October 2024

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi (Milimani Commercial Courts) — Miscellaneous Civil Application
OUTCOME	Application succeeds; Bank of India ordered to produce the requested account information
COMPENSATION	Not applicable — order for production; each party to bear own costs
CORE QUESTION	Whether a bank may rely on the Data Protection Act to withhold a customer's own account information pending signatory consent

PRINCIPAL DOCTRINE

> *The Data Protection Act cannot be invoked as a blanket basis for refusing a customer access to information concerning the customer's own account; third-party privacy principles do not extend to shield a data subject from its own data.*

BRIEF FACTS

TRV TOWERS LIMITED, facing a notice of sale from NCBA Bank Kenya Limited over an alleged default expiring on 30 October 2023, resolved by board resolution on 12 July 2023 to commission a forensic audit of its finances. For that audit it sought its own bank account mandate forms, statements, account-opening records, signatory details, board resolutions, and details of loans, guarantees, and securities held at Bank of India.

Bank of India resisted the request, maintaining it required instructions from all recognised account signatories before releasing the information, and that the company's board resolution alone did not establish that consent. It argued that disclosure without signatory authorisation or a court order would breach the Data Protection Act and its customer-confidentiality obligations.

ISSUES

1. Whether the Court should compel Bank of India to produce the requested banking information.

HOLDING

Application granted. The Court held that confidentiality could not be invoked because the information sought concerned the Applicant itself rather than a third party, and ordered Bank of India to produce the requested documents for audit. Each party was ordered to bear its own costs.

COURT'S REASONING

Following its own earlier decision in TRV Towers Limited v Bank of Baroda (Kenya) Limited [2024] KEHC 8595 (KLR), the Court held that a company controlled by Kenyan citizens may exercise the constitutional right of access to information, and applied that reasoning here.

The decisive distinction was that the information sought concerned the Applicant itself, not unrelated third parties; the Court expressly rejected the proposition that every request for bank information requires every signatory's consent where the company is seeking information about itself.

RATIO DECIDENDI

> *The Data Protection Act does not create an absolute prohibition against disclosure to a data subject; a controller holding information concerning the applicant cannot invoke third-party privacy principles as a blanket justification for denying the applicant access to its own information.*

SIGNIFICANCE

Establishes a clear line for financial institutions between a customer's own account information and genuine third-party data embedded in the same records — only the latter engages the confidentiality concerns the bank sought to rely on here.

> **KEY TAKEAWAY**
> *Your own data protection obligations do not entitle you to withhold a customer's own information from that customer. Reserve confidentiality objections for genuine third-party data.*

Source: Kenya Law · [2024] KEHC 12927 (KLR)

❖

CASE DIGEST · KPLR 015

VOLUME I · DIGEST NO. 015 · PART II: DISCOVERY, ACCESS & THIRD-PARTY DISCLOSURE

WAIYAKI WAY DEVELOPERS LIMITED *v* ASEGA T/A NK MUGO & CO ADVOCATES

[2025] KEHC 12179 (KLR) · Civil Appeal E262 of 2024

High Court of Kenya at Nairobi (Milimani Law Courts) · Hon. T.W. Cherere J. · 15 May 2025

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi (Milimani Law Courts) — Civil Appeal
OUTCOME	Appeal succeeds; advocate ordered to release all client files within seven days
COMPENSATION	Not applicable — order for release of files; Respondent ordered to bear costs
CORE QUESTION	Whether an advocate may rely on an unproven lien or third-party data within a file to withhold a client's own legal files

PRINCIPAL DOCTRINE

> *The Data Protection Act does not authorise an advocate to withhold a client's own legal files merely because those files also contain third-party personal data; the advocate must identify a specific lawful basis, such as a valid lien, for withholding them.*

BRIEF FACTS

WAIYAKI WAY DEVELOPERS LIMITED terminated its relationship with the Respondent advocate and appointed Tito & Associates Advocates in its place. Its new advocates made several written requests for release of its legal files, which the Respondent refused, prompting proceedings for an order directing delivery of all the files.

The Respondent resisted release, asserting a lien for outstanding fees, contending some files had already been released where no fees were owed, and maintaining that the remaining files contained confidential third-party information protected by the Data Protection Act.

The Applicant's position was that the former advocate had no lawful basis for continuing to retain the files.

ISSUES

1. Whether the Respondent had a lawful lien over the Applicant's files.
2. Whether the Data Protection Act barred or limited release.
3. Who should bear the costs.

HOLDING

Appeal allowed. The High Court ordered the Respondent to release all the Applicant's files and documents within seven days, through its current advocates, and ordered the Respondent to bear the costs.

COURT'S REASONING

An advocate's lien must operate within lawful bounds and cannot be used to obstruct access to justice; the Respondent had not shown it had delivered a fee note, filed a bill of costs, or initiated recovery proceedings, so the continued withholding lacked legal justification.

On the Data Protection Act, the Court held that although the Act imposes obligations on controllers and processors, it does not extinguish a data subject's right to access their own personal data; the presence of third-party clients' information within the files did not supply a sufficient basis for withholding the Applicant's own files.

RATIO DECIDENDI

> *The Data Protection Act must not be transformed into a general withholding mechanism: an advocate who resists releasing a client's own files must identify a specific lawful basis for doing so, and the presence of third-party personal data within a file does not, without more, justify retaining the entire file.*

SIGNIFICANCE

Directly relevant to law firms managing file handovers: the Act permits protecting genuine third-party data through redaction or controlled disclosure, but does not licence withholding an entire client file on that basis alone.

> **KEY TAKEAWAY**
> *A client's file belongs to the client. If third-party data sits inside it, redact — don't withhold the whole file, and don't dress up an unproven fee dispute as a data-protection objection.*

Source: Kenya Law · [2025] KEHC 12179 (KLR)

❖
CASE DIGEST · KPLR 016

VOLUME I · DIGEST NO. 016 · PART II: DISCOVERY, ACCESS & THIRD-PARTY DISCLOSURE

B.S. *v* CENTRAL BANK OF KENYA

[2025] KEELRC 2584 (KLR) · Cause E149 of 2025
Employment and Labour Relations Court at Nairobi · Hon. C.N. Baari J. · 29 September 2025

THE CASE AT A GLANCE	
FORUM	Employment and Labour Relations Court at Nairobi — Employment Cause
OUTCOME	Application succeeds in part; redacted disclosure ordered within 21 days
COMPENSATION	Not applicable — order for redacted production; costs in the cause
CORE QUESTION	Whether prior workplace access to colleagues' profiles entitles a former employee to their unredacted production in litigation

PRINCIPAL DOCTRINE

> *Judicial disclosure of employee personal data may be lawful where the information is genuinely relevant to litigation, but disclosure should be controlled and appropriately redacted to protect third-party privacy.*

BRIEF FACTS

THE APPLICANT applied for production of the Central Bank of Kenya's internal audit staff profiles relating to two staff translation and migration exercises — Phase One of 24 August 2016 and Phase Two of 13 December 2021 — containing colleagues' qualifications, current positions, years served, and translated designations, which he wanted to advance allegations of discrimination and differential treatment in his employment dispute.

He argued that the Bank was the records' custodian, that he had previously had access to the information during his employment, and that Articles 35 and 50 supported disclosure — with redaction or confidentiality safeguards available if privacy was a genuine concern.

The Bank objected on procedural grounds and on the substance: the request was broad and premature, the profiles contained employee personal data for which consent had not been obtained, and disclosure without a lawful basis risked violating the Data Protection Act and exposing it to regulatory liability.

ISSUES

1. Whether the Applicant established a basis for an order compelling production of the internal audit staff profiles.
2. How to balance the Applicant's right to information and fair hearing against the privacy rights of the employees whose data the profiles contained.
3. Whether prior workplace access to the information affected that balance.

HOLDING

Application granted in part. The Court ordered a redacted version of the internal audit profiles supplied to the Applicant within 21 days, in compliance with the Data Protection Act, with costs in the cause.

COURT'S REASONING

The Court treated the application as a balancing exercise, accepting the material sought was personal and substantially confidential. That the Applicant had previously accessed it during his employment did not give him an unrestricted right to obtain or disclose it in litigation, and did not automatically defeat his former colleagues' privacy rights.

A complete refusal would nonetheless have unnecessarily hampered the Applicant's ability to prosecute his case; both parties accepted that redacted disclosure could reconcile the competing interests, and the Court ordered accordingly.

RATIO DECIDENDI

> *Where personal data is relevant to litigation, the existence of privacy rights does not require complete suppression; a court may fashion a proportionate remedy through redaction, limited disclosure, confidentiality directions, or controlled inspection.*

SIGNIFICANCE

A clear authority on redacted disclosure as the reconciliation mechanism between privacy and fair hearing, and a template data-disclosure assessment for organisations responding to litigation involving employee records.

> **KEY TAKEAWAY**
>
> *Prior access during employment is not a licence to unredacted disclosure in litigation later. Expect — and propose — redaction as the middle path between full production and outright refusal.*

Source: Kenya Law · [2025] KEELRC 2584 (KLR)

❖

CASE DIGEST · KPLR 017

VOLUME I · DIGEST NO. 017 · PART II: DISCOVERY, ACCESS & THIRD-PARTY DISCLOSURE

J.O. *v* Flamingo Horticulture Kenya Limited

[2025] KEELRC 3346 (KLR) · Cause E001 of 2025

Employment and Labour Relations Court at Nakuru · Hon. J. Rika J. · 28 November 2025

THE CASE AT A GLANCE

FORUM	Employment and Labour Relations Court at Nakuru — Employment Cause
OUTCOME	Both interlocutory applications declined; main discrimination claim to proceed
COMPENSATION	Not applicable — interlocutory rulings; no order as to costs
CORE QUESTION	Whether the Data Protection Act bars using a named comparator's salary data in a workplace discrimination claim

PRINCIPAL DOCTRINE

> *Comparator employment data may be used in discrimination litigation where necessary to establish, exercise, or defend a legal claim, but the claimant must still comply with ordinary evidentiary and procedural requirements — lawful purpose does not eliminate evidentiary procedure.*

BRIEF FACTS

The Claimant sued Flamingo Horticulture Kenya Limited in an employment dispute alleging unequal treatment and remuneration, identifying a fellow employee, L.B., as a comparator he said received superior pay for work of equal value.

Flamingo applied on 23 June 2025 to strike out the comparator allegation and expunge documents containing L.B.'s salary information, arguing she was not a party, that her salary data was personal data of unknown provenance, and that its use invaded her privacy in breach of the Data Protection Act.

The Claimant countered that a discrimination claim cannot be proved without comparator evidence, that the Act permits processing necessary for establishing or defending a legal claim, and separately sought production of L.B.'s payslips, contract, certificates, and payroll records for 2018–2023.

ISSUES

1. Whether the Respondent could prevent use of the comparator's employment data on Data Protection Act grounds.
2. Whether comparator information could legitimately be used in an employment discrimination case.
3. Whether the Claimant was entitled to compel production of the original records.
4. Whether the ordinary rules of evidence and discovery had been satisfied.

HOLDING

Both applications declined; the main claim to proceed, with no order as to costs. The Respondent's application to strike out the comparator material failed, as did the Claimant's separate application for extensive original records.

COURT'S REASONING

Following its own earlier decision in Bajaber v Planning Systems Limited, the Court accepted that a discrimination claim requires comparator evidence, and held the Data Protection Act does not prohibit using comparator information where necessary for a legitimate legal purpose; ordinary payroll records were distinguished from sensitive personal data such as biometric or health information.

But lawful purpose did not excuse the Claimant from ordinary evidentiary procedure: he could not ask the Court to obtain the original records for him without demonstrating possession of copies or the basis for obtaining originals — the proper mechanism was a notice to produce.

RATIO DECIDENDI

> *There is no blanket rule against using another employee's personal data in litigation; where necessary for establishing, exercising, or defending a legal claim, the Data Protection Act may permit its use, but the claimant must still invoke the appropriate discovery or evidentiary mechanism rather than have the court source the material for him.*

SIGNIFICANCE

Confirms comparator evidence is not automatically barred by the Act in discrimination litigation, while reinforcing that lawful purpose and proper procedure are separate requirements that must both be satisfied.

> **KEY TAKEAWAY**
>
> *A comparator's data protection rights do not doom your discrimination claim — but you still need to prove the claim through the ordinary evidentiary process, not by asking the court to fetch the records for you.*

Source: Kenya Law · [2025] KEELRC 3346 (KLR)

❖

CASE DIGEST · KPLR 018

VOLUME I · DIGEST NO. 018 · PART II: DISCOVERY, ACCESS & THIRD-PARTY DISCLOSURE

S.S. *v* Prime Bank Limited

[2025] KEHC 2579 (KLR) · Civil Appeal E001 of 2024

High Court of Kenya at Kisumu · Hon. A.B. Mwamuye J. · 4 February 2025

On appeal from a dismissed ODPC complaint

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Kisumu — Civil Appeal
OUTCOME	Appeal dismissed, with costs to the Respondent bank
COMPENSATION	None — appeal dismissed
CORE QUESTION	Whether an estate's executors' Grant of Probate supplied a lawful basis for a bank to disclose a joint accountholder's banking information

PRINCIPAL DOCTRINE

> *Disclosure of personal banking information without the data subject's consent may nevertheless be lawful where disclosure is necessary to comply with a legal obligation, including the lawful functions of executors administering an estate.*

BRIEF FACTS

The Appellant complained to the ODPC against Prime Bank Limited over disclosure of banking information relating to accounts he had held jointly with his late mother, later renewed in his sole name, alleging the disclosure to third parties occurred without his consent.

Prime Bank explained the information had been requested by the executors of his mother's estate, who produced a Grant of Probate as the legal basis for their request; the Data Commissioner dismissed the complaint, and the Appellant appealed to the High Court.

ISSUES

1. Whether the Data Commissioner had misunderstood the personal data in issue.
2. Whether the impugned data-sharing action was lawful.

HOLDING

Appeal dismissed, with costs to Prime Bank. The Data Commissioner's decision remained undisturbed.

COURT'S REASONING

The Court found the Commissioner had correctly identified the information at issue; although the accounts were later renewed in the Appellant's sole name, the executors needed information about them to ascertain the nature and extent of the deceased's estate, a legal obligation evidenced by the Grant of Probate.

Considering section 30(1)(b)(ii) of the Data Protection Act — lawful processing without consent where necessary for compliance with a legal obligation — the Court held prior notification was not required, distinguishing the original data-collection stage from the later disclosure undertaken under that statutory basis.

RATIO DECIDENDI

> *Consent is not the only lawful basis for processing; where a controller has a legally recognised obligation to disclose information and the statutory requirements for that disclosure are satisfied, the absence of consent does not necessarily make the disclosure unlawful.*

SIGNIFICANCE

A critical authority distinguishing consent-based disclosure from statutory or legal-obligation disclosure: a request from an estate's executors should be assessed against their probate or succession authority, not treated as an ordinary third-party request.

> **KEY TAKEAWAY**
>
> *A Grant of Probate can itself be the lawful basis for disclosure. Before refusing an executor's request for a joint accountholder's banking information, check whether a legal obligation — not consent — already authorises it.*

Source: Kenya Law · [2025] KEHC 2579 (KLR)

❖

CASE DIGEST · KPLR 019

VOLUME I · DIGEST NO. 019 · PART II: DISCOVERY, ACCESS & THIRD-PARTY DISCLOSURE

Premier Credit Limited *v* M.K.

[2025] KEHC 9254 (KLR) · Civil Appeal E045 of 2024
High Court of Kenya at Nairobi (Milimani Law Courts) · Hon. A.N. Ongeri J. · 30 June 2025
On appeal from an ODPC determination of 15 December 2023

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi (Milimani Law Courts) — Civil Appeal
OUTCOME	Appeal allowed; determination, enforcement notice, and compensation all quashed
COMPENSATION	KES 700,000 award set aside; each party to bear own costs
CORE QUESTION	Whether procedural defects in the Commissioner's investigation invalidated the determination regardless of the underlying merits

PRINCIPAL DOCTRINE

> *An ODPC determination and enforcement notice may be invalid where the Commissioner fails to observe mandatory procedural safeguards, including fair hearing, statutory response periods, and proper investigation — regardless of the substantive merits of the underlying complaint.*

BRIEF FACTS

The Data Commissioner determined, on 15 December 2023, that Premier Credit Limited was liable for sending the Respondent incessant promotional messages about its loan products despite his stated disinterest, directed cessation of the processing, and awarded him KES 700,000 in compensation.

Premier Credit maintained the numbers used belonged to independent sales agents whose contracts had since been terminated, and appealed on procedural grounds: it said it had received no formal charge or Notice to Show Cause, that its statutory 21-day response period had been reduced to 14 days, that the enforcement notice issued simultaneously with the determination, and that no investigation report had been prepared and the agents themselves were never joined or heard.

ISSUES

1. Whether Premier Credit breached Article 31(c) and (d) and section 25 of the Data Protection Act.
2. Whether the KES 700,000 compensation was excessive.
3. Who should bear the costs.

HOLDING

Appeal allowed. The High Court quashed the ODPC enforcement notice, quashed the determination of 15 December 2023, set aside the KES 700,000 award, and ordered each party to bear its own costs.

COURT'S REASONING

The Court found it unnecessary to resolve the substantive data-processing questions, disposing of the appeal instead on procedural fairness: Premier Credit was not served with formal charges, was denied its statutory response period, faced an enforcement notice issued simultaneously with the determination, and was denied a meaningful opportunity to challenge the findings before sanctions were imposed.

The absence of a proper investigation report, and the failure to investigate or hear the agents said to be responsible, compounded these defects; the Court treated them as fatal to the determination's validity.

RATIO DECIDENDI

The Commissioner's substantive jurisdiction does not dispense with procedural fairness; where the enabling legislation prescribes procedural safeguards — proper notice, an adequate response period, investigation, and a hearing before sanction — those safeguards must be followed, and their absence can invalidate a determination without the High Court needing to reach the underlying substantive liability.

SIGNIFICANCE

A key authority distinguishing 'the Commissioner got the law wrong' from 'the Commissioner failed to follow the legally prescribed process' — the latter can be fatal on its own, giving respondents a procedural route that does not require winning on the merits.

KEY TAKEAWAY

Test the process, not just the outcome. A truncated response period or a simultaneous enforcement notice can be enough to quash an ODPC determination outright, whatever the underlying merits.

Source: Kenya Law · [2025] KEHC 9254 (KLR)

❖

CASE DIGEST · KPLR 020

VOLUME I · DIGEST NO. 020 · PART II: DISCOVERY, ACCESS & THIRD-PARTY DISCLOSURE

A.M. *v* Agence Française de Développement

[2025] KEELRC 3664 (KLR) · Petition E120 of 2025

Employment and Labour Relations Court at Nairobi · Hon. B. Ongaya J. · 17 December 2025

THE CASE AT A GLANCE

FORUM	Employment and Labour Relations Court at Nairobi — Constitutional Petition (Employment)
OUTCOME	Preliminary objection overruled; petition to proceed on its constitutional and employment claims
COMPENSATION	Not applicable — interlocutory jurisdictional ruling
CORE QUESTION	Whether privacy and data-protection allegations pleaded within an employment dispute must first go to the ODPC

PRINCIPAL DOCTRINE

> *A data-protection complaint embedded within a broader employment dispute does not automatically deprive the Employment and Labour Relations Court of jurisdiction; the Court must examine the substance of the pleaded constitutional and employment dispute rather than treat every Data Protection Act issue as automatically reserved to the ODPC.*

BRIEF FACTS

The Petitioner's petition arose from her employment with Agence Française de Développement, alleging discrimination, harassment, unfair labour practices, disciplinary-process abuses, unlawful termination, and violations of Article 31 and the Data Protection Act — including a claim that being required to attend a doctor selected by her employer implicated her privacy rights.

AFD raised a preliminary objection, arguing the petition disclosed no constitutional violation, amounted to an abuse of process better pursued through ordinary employment law, and that the Court lacked jurisdiction over the data-protection allegations, which it said should first have gone to the Data Commissioner.

The Petitioner responded that the Court's constitutional jurisdiction over employment disputes was not excluded merely because statutory employment or data-protection remedies also existed, and that her privacy and data-protection claims formed part of a single, genuinely constitutional dispute.

ISSUES

1. Whether the doctrine of constitutional avoidance barred the petition.
2. Whether the petition was an abuse of process.
3. Whether the data-protection claims were required to be brought first before the ODPC.
4. Whether the Court had jurisdiction over the pleaded dispute.

HOLDING

Preliminary objection overruled. The Court held the pleaded case disclosed constitutional issues requiring determination and was not defeated at the threshold by constitutional avoidance; the petition was directed to proceed.

COURT'S REASONING

Where a dispute can be completely resolved through ordinary employment law, a litigant should ordinarily use that statutory mechanism. But the Court found the Petitioner's pleadings raised allegations whose resolution would require consideration of constitutional provisions, taking the petition outside that principle.

The Court acknowledged the Data Protection Act's own complaint and enforcement mechanism, but tied its ruling to the nature of the dispute as actually pleaded, rather than treating every Data Protection Act issue as automatically outside the Court's constitutional jurisdiction.

RATIO DECIDENDI

Where an employment dispute genuinely requires determination of constitutional rights, the existence of statutory employment and data-protection mechanisms does not automatically prevent the Employment and Labour Relations Court from exercising its constitutional jurisdiction over the dispute as pleaded.

SIGNIFICANCE

Confirms that a workplace privacy or data-protection grievance is not necessarily confined to the ODPC's complaint mechanism where it forms part of a genuinely constitutional employment dispute — employers should not treat such complaints as purely an internal HR or regulatory matter.

KEY TAKEAWAY

Bundling a privacy complaint into a constitutional employment petition does not automatically fail for wrong forum. If the constitutional dispute is real, the ELRC can hear the data-protection element alongside it.

Source: Kenya Law · [2025] KEELRC 3664 (KLR)

❖
CASE DIGEST · KPLR 021

VOLUME I · DIGEST NO. 021 · PART II: DISCOVERY, ACCESS & THIRD-PARTY DISCLOSURE

Safaricom PLC *v* C.M. & Another

[2026] KEHC 8493 (KLR) · Civil Appeal E367 of 2025 (Ruling)
High Court of Kenya at Nairobi (Milimani Law Courts) · Hon. A.C. Mrima J. · 22 May 2026
On appeal from ODPC Complaint No. 1958 of 2024, determination delivered 24 February 2025

THE CASE AT A GLANCE

FORUM	High Court of Kenya at Nairobi (Milimani Law Courts) — Civil Appeal, Interlocutory Ruling
OUTCOME	Both applications allowed, on terms
COMPENSATION	KES 250,000 per respondent; execution stayed on deposit of the same sum
CORE QUESTION	Whether a jurisdictional challenge justifies a stay, and whether a cross-appeal needs leave

PRINCIPAL DOCTRINE

> *Where the Data Protection Act is silent on a timeline beyond a specific carve-out, the Civil Procedure Rules fill the gap; a party may cross-appeal an ODPC determination without leave, provided this precedes directions in the main appeal.*

BRIEF FACTS

Safaricom PLC and Becton Dickinson & Company, trading as BD East Africa, were found liable by the Data Commissioner on 24 February 2025 for infringing C.M.'s rights under section 26(a) of the Data Protection Act: upon her termination, BD East Africa had shared her National Identity Card details with Safaricom to facilitate a SIM-card transfer without, on her account, her informed consent. The Commissioner ordered each party to pay her KES 250,000.

Safaricom appealed, seeking a stay of execution and contending the ODPC lacked jurisdiction over what it called a SIM-registration dispute reserved to the Communications and Multimedia Appeals Tribunal; it said it had merely updated billing details on a line already in C.M.'s name, requiring no fresh consent. C.M. cross-applied for extension of time to cross-appeal, arguing the award was inadequate and blaming her 15-day delay on her former advocate.

ISSUES

1. Whether the Court should grant a stay of execution of the ODPC's determination.
2. Whether the Court has jurisdiction to extend time for filing a cross-appeal under the Data Protection Act, and, if so, whether C.M. met the threshold for that extension.

HOLDING

Both applications allowed. The Court stayed execution of the ODPC's determination on condition that Safaricom deposit KES 250,000 in court within 30 days, failing which the stay would lapse; and directed C.M. to file and serve her cross-appeal within 10 days, each party bearing its own costs of both applications.

COURT'S REASONING

On stay, the Court applied the established Order 42 Rule 6 test: the application was not brought after unreasonable delay; Safaricom's jurisdictional challenge was a weighty, arguable point of law, and the risk of attachment against its telecommunications infrastructure — with C.M. not having shown an ability to refund the sum — established substantial loss; and Safaricom's offer of a bank guarantee satisfied the security limb.

On the cross-appeal, the Court found the Data Protection Act and its Regulations silent on appeal timelines generally, save for Regulation 19 governing enforcement-notice appeals specifically — leaving the Civil Procedure Act and Rules to govern appeals from the ODPC. But because even that general regime does not itself prescribe cross-appeal timelines, the Court adopted a liberal position: a party may file a cross-appeal without leave before directions are taken in the main appeal, and needs leave only once directions have issued. As no directions had yet been taken here, C.M. was free to cross-appeal without needing an extension at all.

RATIO DECIDENDI

> *Where the Data Protection Act and its Regulations are silent on a procedural timeline beyond a specific carve-out such as enforcement-notice appeals, the general Civil Procedure Act and Rules fill the gap; and because those Rules do not themselves fix a cross-appeal deadline, a respondent to an ODPC-derived appeal may file a cross-appeal as of right at any point before directions are taken in the main appeal.*

SIGNIFICANCE

Clarifies two recurring appellate-procedure questions for Data Protection Act appeals: the ordinary stay-of-execution test applies without modification, and — distinctively — a party aggrieved by part of an ODPC determination need not rush to cross-appeal within the primary 30-day window, provided they act before the main appeal reaches directions.

KEY TAKEAWAY

You do not need the Court's leave to cross-appeal an ODPC determination — file before directions are taken in the main appeal and you are in time regardless of the primary 30-day window.

Source: Kenya Law · [2026] KEHC 8493 (KLR)

❖

CASE DIGEST · KPLR 022

VOLUME I · DIGEST NO. 022 · PART III: CONFIDENTIALITY, PUBLICATION & STATUTORY MANDATE

A.G. & 4 Others *v* Waigwa

[2022] KEHC 12253 (KLR) · Civil Suit E135 of 2022
High Court of Kenya at Nairobi (Milimani Law Courts) · Hon. J.K. Sergon J. · 5 August 2022

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi (Milimani Law Courts) — Civil Suit, Interlocutory Application
OUTCOME	Application allowed; interlocutory injunction granted restraining further publication
COMPENSATION	Not applicable — interlocutory injunctive relief pending trial
CORE QUESTION	Whether a mandatory interlocutory injunction may restrain continuing online publication of allegedly defamatory, confidentiality-linked material

PRINCIPAL DOCTRINE

> *Where personal or confidential information is being disseminated online in circumstances giving rise to a prima facie infringement of protected interests, the Court may grant targeted interlocutory injunctive relief to prevent continuing dissemination pending trial — even where the relief sought is, in substance, mandatory.*

BRIEF FACTS

The Plaintiffs, advocates of the firm Wamae & Allen Advocates, had lodged an ODPC complaint against the Defendant, a former employee, alleging a serious breach of confidential information. Following that complaint, the Defendant — with over 16,000 Twitter followers — published tweets the Plaintiffs said referred to them and the firm, including allegations of sexual harassment in law firms.

The Plaintiffs said the tweets were being retweeted across social media, that clients had begun inquiring about the allegations, and that continued publication threatened reputational and business harm. By an application dated 28 July 2022, they sought injunctive orders restraining further publication and removal of the tweets.

The Defendant, who filed no replying affidavit, argued the allegations were unsubstantiated innuendo and that the Plaintiffs had not met the threshold for a mandatory interlocutory injunction against his Article 33(1) freedom of expression.

ISSUES

1. Whether the Plaintiffs had established a prima facie case.
2. Whether an interlocutory injunction could issue.
3. Whether the Court could issue a mandatory injunction requiring removal of online publications.
4. How Article 33 freedom of expression was to be balanced against the Plaintiffs' reputation and rights.

HOLDING

Application allowed. The Court restrained the Defendant from publishing or causing publication of material referring to the Plaintiffs and their firm, including the impugned tweets, and directed removal of the specified publications from the relevant online platforms and search results pending determination of the suit.

COURT'S REASONING

The Defendant had not controverted the factual allegations in the supporting affidavit; the Court found the impugned tweets appeared to suggest the Plaintiffs had engaged in sexual harassment and professional misconduct, establishing a prima facie case with a probability of success.

The Court rejected the proposition that a mandatory injunction could never issue at an interlocutory stage — where the words complained of are plainly defamatory and remain uncontroverted, such relief may issue even before trial.

RATIO DECIDENDI

The immediate ratio is not that the Defendant lacked a lawful basis under section 30 of the Data Protection Act to hold or disclose the information; it is that where personal or confidential information is being disseminated online in circumstances giving rise to a prima facie infringement of protected interests, the Court may grant targeted interlocutory injunctive relief — including mandatory relief — to prevent continuing dissemination pending trial.

SIGNIFICANCE

An important reminder that a lawful disclosure to a regulator does not authorise public dissemination: an employee or former employee who possesses information from an employment relationship should distinguish what may lawfully be retained, disclosed to a regulator, used in proceedings, or published publicly — four different questions.

KEY TAKEAWAY

Filing a regulatory complaint does not license a public campaign. Confidential information disclosed to the ODPC stays confidential — publishing it, or related allegations, online is a separate act with separate consequences.

Source: Kenya Law · [2022] KEHC 12253 (KLR)

❖

CASE DIGEST · KPLR 023

VOLUME I · DIGEST NO. 023 · PART III: CONFIDENTIALITY, PUBLICATION & STATUTORY MANDATE

C.M. *v* National Council for Law Reporting

[2022] KEHC 15471 (KLR) · Petition E394 of 2020

High Court of Kenya at Nairobi (Constitutional and Human Rights Division) · Hon. Hedwig Imbosa Ong'udi J. · 18 November 2022

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi (Constitutional and Human Rights Division) — Constitutional Petition
OUTCOME	Petition dismissed; removal or anonymisation of the reported judgment refused
COMPENSATION	None — petition dismissed
CORE QUESTION	Whether a statutory law-reporting mandate displaces the ordinary requirement of consent for publishing personal information in judgments

PRINCIPAL DOCTRINE

> *The Data Protection Act does not transform every processing activity into consent-based processing where another law gives the controller an independent statutory mandate to perform it; consent is not the exclusive lawful basis for processing personal data.*

BRIEF FACTS

The Petitioner, formerly a Senior Human Resource Officer at Nairobi Java House Limited, was terminated on 19 November 2014 and successfully complained of unfair termination before the Commissioner for Labour. Criminal proceedings later brought against her former employer's Chief Executive Officer and Human Resource Manager were challenged by judicial review, and that judicial-review decision was reported on the Kenya Law website.

Though not a party to the judicial-review proceedings, the Petitioner found the report surfacing when she searched her own name online, and said prospective employers conducting background checks were encountering it and it had cost her employment opportunities. She had never consented to the publication and argued Kenya Law ought to have carried out a data protection impact assessment given the risk to her rights.

She sought removal of the judgment from the Kenya Law website or, alternatively, anonymisation to prevent her public identification. Kenya Law resisted, relying on its statutory mandate to prepare and publish law reports and maintaining that judicial decisions are public legal information whose reporting does not depend on the consent of everyone named in them.

ISSUES

1. Whether publication of the judgment required the Petitioner's consent.
2. Whether the continued publication violated Article 31.
3. Whether the Petitioner was entitled to erasure.
4. Whether Kenya Law possessed an independent statutory mandate to publish judicial decisions.
5. Whether that public-interest publication function displaced ordinary consent requirements.
6. Whether Kenya Law had breached the Data Protection Act.

HOLDING

Petition dismissed. The Court declined to order removal or anonymisation, holding the publication was undertaken pursuant to Kenya Law's statutory law-reporting function.

COURT'S REASONING

The Court treated the case as establishing that publication under an independent statutory or public-interest mandate is not automatically consent-dependent. The governing question was not whether the Petitioner had consented, but what legal authority governed the processing in the first place.

Once a statute imposes a public function such as law reporting, the controller must then apply the applicable Data Protection Act obligations and safeguards to that function — but the existence of the statutory mandate itself supplies the lawful basis, without requiring the consent of every individual named in a reported judgment.

RATIO DECIDENDI

> *The Data Protection Act does not transform every processing activity involving personal information into consent-based processing where another law gives the controller an independent statutory mandate to perform that processing; the threshold question is the legal authority for the processing, not whether the individual consented.*

SIGNIFICANCE

A foundational authority for public bodies exercising statutory publication or reporting functions: the analysis starts with identifying the enabling statute and its defined purpose, not with an assumption that consent is required, though minimisation and other safeguards still apply.

KEY TAKEAWAY

A statutory mandate is a lawful basis in its own right. If your publication function is set by law, start there — not with whether each affected person has consented.

Source: Kenya Law · [2022] KEHC 15471 (KLR)

❖
CASE DIGEST · KPLR 024

VOLUME I · DIGEST NO. 024 · PART IV: LAWFUL BASIS, STATUTORY MANDATE & LAW-ENFORCEMENT PROCESS

E.C. *v* ETHICS AND ANTI-CORRUPTION COMMISSION; T.M. (INTERESTED PARTY)

[2023] KEHC 3918 (KLR) · Anti-Corruption and Economic Crime Petition No. 3 of 2022
High Court of Kenya at Nairobi (Milimani Law Courts) · Hon. E.N. Maina J. · 4 May 2023

THE CASE AT A GLANCE

FORUM	High Court of Kenya at Nairobi (Milimani Law Courts) — Anti-Corruption and Economic Crime Petition
OUTCOME	Petition dismissed with costs; covert recordings held lawfully obtained
COMPENSATION	None — petition dismissed; costs awarded against the Petitioner
CORE QUESTION	Whether covert audio/video recording of a suspect during an anti-corruption sting required his consent

PRINCIPAL DOCTRINE

> *The Data Protection Act does not require a suspect's consent before personal data is indirectly collected where the statutory law-enforcement exception applies; covert collection in a genuine criminal investigation can supply its own independent lawful basis.*

BRIEF FACTS

THE PETITIONER, a KEMSA Legal Officer, was under investigation by the Ethics and Anti-Corruption Commission over an alleged bribery solicitation. As part of the investigation, the Interested Party participated in a covert operation involving interactions with the Petitioner at the Ole Sereni Hotel between 1 June and 17 September 2021, generating audio and video recordings of their exchanges.

The Petitioner challenged the recordings on multiple grounds: he had not consented, there had been no prior judicial authorisation, the recordings breached the privacy of his communications and the Data Protection Act, and the operation amounted to unlawful entrapment. He sought declarations under Articles 31, 28, 32, 33, 47, and 50, and an order expunging the material before any future criminal trial.

ISSUES

1. Whether covert collection of the Petitioner's personal data required his consent.
2. Whether indirect collection of personal data was permissible in the circumstances.
3. Whether the criminal-investigation context supplied a lawful statutory basis.
4. Whether the recordings were unconstitutional merely for being obtained without consent.
5. Whether the Court should rule on the recordings' admissibility before the Petitioner had been charged.
6. Whether the alleged constitutional violations had been proved.

HOLDING

Petition dismissed with costs. The Court held that section 28(2)(f) of the Data Protection Act permits indirect collection of personal data where necessary for the prevention, detection, investigation, prosecution, or punishment of crime, and that the Interested Party's participation in the operation could itself be the source from which the information was lawfully obtained.

COURT'S REASONING

The Court found the covert collection fell within the statutory law-enforcement exception to consent, so the absence of the Petitioner's consent did not by itself render the recordings unconstitutional.

The Court expressly declined to go further: it did not hold that all covert surveillance is automatically lawful, and considered it premature to rule on the recordings' admissibility at any future criminal trial, since the Petitioner had not yet been arrested or charged — that question was left to the trial court if proceedings arose.

RATIO DECIDENDI

The Data Protection Act does not require the consent of a suspect before personal data is indirectly collected where the statutory law-enforcement exception applies; this qualifies, but does not displace, the general proposition that consent is the default lawful basis for processing.

SIGNIFICANCE

One of the strongest authorities on law-enforcement processing: it confirms indirect covert collection can be independently lawful in a genuine criminal investigation, while pointedly leaving open — for the trial court, not the constitutional court — whether particular covertly-obtained evidence will ultimately be admissible.

KEY TAKEAWAY

A genuine criminal investigation is its own lawful basis for indirect, covert collection. But that answers the constitutional question, not the evidentiary one — admissibility remains for the trial court to decide.

Source: Kenya Law · [2023] KEHC 3918 (KLR)

❖

CASE DIGEST · KPLR 025

VOLUME I · DIGEST NO. 025 · PART IV: LAWFUL BASIS, STATUTORY MANDATE & LAW-ENFORCEMENT PROCESS

Okiya Omtatah Okoiti *v* Attorney General & Another

[2020] KEHC 7848 (KLR) · High Court of Kenya

20 February 2020 — case/petition number and presiding judge not stated in the available record

THE CASE AT A GLANCE	
FORUM	High Court of Kenya — Constitutional Petition
OUTCOME	Petition dismissed; KRA's statutory information-gathering powers upheld
COMPENSATION	None — petition dismissed
CORE QUESTION	Whether the KRA's statutory powers to obtain taxpayer and third-party information unjustifiably infringed privacy

PRINCIPAL DOCTRINE

> *Statutory powers to obtain information may constitute lawful interference with privacy where exercised within a sufficiently defined legal framework and directed to a legitimate public purpose; the right to privacy under Article 31 is not absolute.*

BRIEF FACTS

The Petitioner challenged provisions of the Tax Procedures Act — principally section 59 — conferring on the Kenya Revenue Authority broad powers to obtain information relevant to tax assessment, audit, and investigation from taxpayers and third parties, arguing the powers infringed Article 31(c) privacy.

The Respondents maintained the information concerned tax administration, that the powers were necessary for KRA's statutory functions, that KRA remained bound by confidentiality obligations, and that privacy is not an absolute right where a limitation serves a legitimate public purpose.

ISSUES

1. Whether the statutory information-gathering powers infringed Article 31.
2. Whether the limitation was authorised by law.
3. Whether the limitation served a legitimate governmental purpose.
4. Whether the limitation was proportionate.
5. Whether confidentiality safeguards sufficiently constrained the power.

HOLDING

Petition dismissed. The Court held that privacy is not absolute and may be limited by law where the limitation satisfies Article 24, and found the KRA's information-gathering powers, bound by statutory confidentiality obligations, pursued a legitimate public purpose and were justified as framed.

COURT'S REASONING

The Court weighed the tax information sought against the statutory confidentiality obligations binding KRA, concluding the powers were directed to tax administration — a legitimate public purpose — and that the resulting limitation on privacy was proportionate rather than open-ended.

RATIO DECIDENDI

A statutory authority may lawfully require access to personal information where the power is grounded in law, directed to a legitimate statutory purpose, and accompanied by safeguards against arbitrary use — this is an authority on legally constrained information-gathering, not an unlimited governmental-data power.

SIGNIFICANCE

A foundational public-sector lawful-basis authority: it confirms government bodies may compel disclosure of personal information under statute without infringing privacy, provided the power is legally defined, purposive, and confidentiality-bound — but does not licence unconstrained governmental data demands.

KEY TAKEAWAY

A statutory information-gathering power survives a privacy challenge only if it is legally defined, purpose-bound, and confidentiality-constrained. Map all four before relying on it.

Source: Kenya Law · [2020] KEHC 7848 (KLR) — specific petition number and presiding judge not stated in the available record.

❖

CASE DIGEST · KPLR 026

VOLUME I · DIGEST NO. 026 · PART IV: LAWFUL BASIS, STATUTORY MANDATE & LAW-ENFORCEMENT PROCESS

Republic *v* Mucheru, CS Ministry of ICT & 2 Others

[2021] KEHC 122 (KLR) · Judicial Review Application E1138 of 2020
High Court of Kenya at Nairobi · Hon. J. Ngaah J. · 14 October 2021

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Judicial Review
OUTCOME	Application succeeds; Huduma Card rollout decision quashed; DPIA compelled before further processing
COMPENSATION	Not applicable — orders of certiorari and mandamus
CORE QUESTION	Whether the Government could roll out Huduma Cards, built on NIIMS data, without first conducting a DPIA

PRINCIPAL DOCTRINE

> *The existence of statutory authority to collect or process personal data does not eliminate the mandatory safeguards the Data Protection Act imposes; where processing is likely to create high risk, section 31 requires a Data Protection Impact Assessment before that processing may lawfully proceed.*

BRIEF FACTS

The ex parte applicants, following the nationwide collection of personal and biometric information under the National Integrated Identity Management System, and after the Data Protection Act came into force on 25 November 2019, challenged the Government's 18 November 2020 announcement that it would roll out Huduma Cards. Katiba Institute and Yash Pal Ghai brought the challenge, principally because no Data Protection Impact Assessment had been conducted beforehand, as section 31 of the Act requires.

The Respondents — the Cabinet Secretaries for the Ministries of ICT and Interior, and the Attorney General — argued that most of the underlying NIIMS data collection predated the Act, that section 31 should not apply retrospectively, that the collection had its own existing statutory basis, and that the applicants had alternative statutory remedies they had not exhausted.

ISSUES

1. Whether the Data Protection Act applied to the NIIMS data.
2. Whether section 31 had retrospective relevance.
3. Whether the DPIA requirement was applicable to the Huduma Card rollout.
4. Whether processing could proceed without a DPIA.
5. Whether judicial review could be entertained despite the Act's statutory complaint route.
6. Whether the Huduma Card rollout was lawful.

HOLDING

Application granted. The Court issued certiorari quashing the 18 November 2020 decision to roll out Huduma Cards, and mandamus compelling the respondents to conduct a Data Protection Impact Assessment before processing data or proceeding with the rollout.

COURT'S REASONING

The Court treated the DPIA not as an administrative courtesy but as a condition governing lawful processing: statutory authority to collect or process personal data does not itself satisfy the separate, mandatory pre-processing safeguards the Act imposes where the processing is likely to create high risk.

RATIO DECIDENDI

> *The existence of statutory authority to collect or process personal data does not eliminate the mandatory safeguards the Data Protection Act imposes; where processing is likely to create high risk, section 31 requires a Data Protection Impact Assessment before that processing may lawfully proceed.*

SIGNIFICANCE

A foundational State-processing authority establishing a two-stage lawful-basis test for government and large-scale controllers: first, what law authorises the processing; second, what conditions — such as a DPIA — must be satisfied before that power may actually be exercised.

> **KEY TAKEAWAY**
>
> *Having the legal power to process is only step one. For high-risk processing, a Data Protection Impact Assessment is a precondition to lawfully using that power — not paperwork to complete afterward.*

Source: Kenya Law · [2021] KEHC 122 (KLR)

❖

CASE DIGEST · KPLR 027

VOLUME I · DIGEST NO. 027 · PART IV: LAWFUL BASIS, STATUTORY MANDATE & LAW-ENFORCEMENT PROCESS

LAW SOCIETY OF KENYA *v* COMMUNICATIONS AUTHORITY OF KENYA & 10 OTHERS

[2023] KESC 27 (KLR) · Petition No. 8 of 2020
Supreme Court of Kenya · 21 April 2023

THE CASE AT A GLANCE	
FORUM	Supreme Court of Kenya — Petition (Article 163(4)(a) Appeal)
OUTCOME	Supreme Court addressed the jurisdictional gateway; not a fresh merits ruling on every privacy issue
COMPENSATION	Not applicable — constitutional/jurisdictional determination
CORE QUESTION	Whether the CA's proposed Device Management System could proceed without full accounting for privacy and process

PRINCIPAL DOCTRINE

> *A regulatory mandate to establish a communications or device-management system remains constrained by constitutional privacy and lawful regulatory process; a statutory mandate does not itself validate every technical implementation of that mandate.*

BRIEF FACTS

THE COMMUNICATIONS AUTHORITY sought to establish a Device Management System linked to mobile networks, giving it access to IMEI, IMSI, MSISDN, and related subscriber information, in order to address stolen, counterfeit, and illegal devices; it engaged mobile network operators toward that end.

The Law Society of Kenya challenged the proposal on constitutional grounds, arguing the system would interfere with the privacy of millions of mobile subscribers and that the regulatory process had not adequately addressed privacy, public participation, statutory authority, and appropriate safeguards. The matter reached the Supreme Court on appeal.

ISSUES

1. Whether the appeal was properly before the Supreme Court under Article 163(4)(a).
2. Whether the Device Management System's implementation remained within the Communications Authority's statutory mandate.
3. Whether that implementation was constitutionally compatible with subscriber privacy.

HOLDING

The Supreme Court's 2023 judgment turned on whether the appeal was properly before it under Article 163(4)(a), rather than delivering a fresh merits determination of every underlying privacy issue raised by the proposed system.

COURT'S REASONING

The Court treated the litigation as engaging constitutional interpretation and application arising from a proposed system capable of affecting millions of subscribers, but its disposition centred on the procedural route by which the constitutional challenge reached the Supreme Court, distinct from the substantive question of the system's ultimate compatibility with privacy.

RATIO DECIDENDI

A regulator's statutory mandate does not itself validate every technical implementation of that mandate; the implementation must remain within the enabling legislation, constitutional privacy, procedural requirements, and applicable safeguards — and the procedural route by which such a challenge reaches the Supreme Court is a distinct question from the mandate's substantive scope.

SIGNIFICANCE

An important reminder for regulators that a broad statutory mandate is not a blank cheque: privacy, public participation, and lawful process remain live constraints on implementation, and litigants and regulators alike must attend carefully to the correct appellate gateway for constitutional challenges of this kind.

KEY TAKEAWAY

A regulatory mandate authorises action within its scope, not any technical means of pursuing it. Address privacy, participation, and safeguards for the specific implementation — not just the enabling statute.

Source: Kenya Law · [2023] KESC 27 (KLR)

❖

CASE DIGEST · KPLR 028

VOLUME I · DIGEST NO. 028 · PART IV: LAWFUL BASIS, STATUTORY MANDATE & LAW-ENFORCEMENT PROCESS

K.O. *v* H.M.

[2023] KEHC 18290 (KLR) · Petition E153 of 2022

High Court of Kenya at Nairobi · Hon. H.I. Ong'udi J. · 31 May 2023

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Constitutional Petition
OUTCOME	Petition succeeds; CCTV camera ordered removed; further surveillance of the Petitioner's property prohibited
COMPENSATION	None awarded — actual injury from captured footage not established; other constitutional remedies granted
CORE QUESTION	Whether a neighbour's CCTV, capable of viewing the Petitioner's property, violated his right to privacy

PRINCIPAL DOCTRINE

> *A legitimate security purpose does not authorise unlimited surveillance of neighbouring property; CCTV installed for one's own security must still be configured to avoid capturing a neighbour's private space.*

BRIEF FACTS

THE PETITIONER AND THE RESPONDENT were neighbours at an apartment complex in Kilimani. Following a security incident involving break-ins, the Respondent installed CCTV cameras which she said were for her family's security; the Petitioner alleged the cameras captured his home and family, invading his Article 31 privacy.

The parties disputed when the cameras were installed, their actual field of view, whether the Petitioner had been informed, and whether his consent was required. The Court directed technical experts for both sides to jointly inspect the system.

The joint technical report found the camera had a fixed 45-degree lens, viewable remotely by anyone with internet access and the password; that at inspection its display covered the Respondent's own property, but that it could manually be redirected toward the Petitioner's property using an Allen key.

ISSUES

1. Whether the Petitioner's Article 31 right to privacy was violated.
2. Whether the CCTV footage constituted processing of personal data.
3. Whether the Respondent had a legitimate security purpose.
4. Whether the Petitioner's consent to the surveillance was established.
5. Whether the surveillance was justified and proportionate.
6. Whether constitutional remedies should issue.

HOLDING

Petition allowed in part. The Court found the Petitioner's privacy right had been violated, ordered the camera removed, and prohibited further surveillance devices directed at his property, but declined compensation as he had not established actual injury from any captured footage.

COURT'S REASONING

The Court accepted the Respondent had a legitimate security reason for installing CCTV, but held that a legitimate purpose does not automatically authorise a configuration capable of capturing a neighbour's private space. As a data controller, she was required to comply with the Data Protection Act, and the absence of demonstrated express consent from the Petitioner was significant.

RATIO DECIDENDI

> *A legitimate security purpose for installing CCTV does not authorise surveillance capable of capturing a neighbour's private property; the controller must configure the system to the least intrusive extent reasonably capable of achieving the security objective, and absent consent, capability to view a neighbour's property — not just actual viewing — can found a privacy violation.*

SIGNIFICANCE

A key residential-CCTV authority: it confirms that even a genuinely protective purpose does not excuse a camera's technical capacity to surveil a neighbour, and sets out a purpose-necessity-field-of-view-minimisation framework private CCTV operators should document.

> **KEY TAKEAWAY**
> *A camera capable of viewing your neighbour's property is a privacy problem even if you never actually look. Position, mask, and password-protect your CCTV to match your own property only.*

Source: Kenya Law · [2023] KEHC 18290 (KLR)

❖

CASE DIGEST · KPLR 029

VOLUME I · DIGEST NO. 029 · PART IV: LAWFUL BASIS, STATUTORY MANDATE & LAW-ENFORCEMENT PROCESS

KATIBA INSTITUTE *v* COMMUNICATIONS AUTHORITY OF KENYA & 2 OTHERS

[2025] KEHC 10568 (KLR) · Petition E647 of 2024
High Court of Kenya at Nairobi · Hon. E.C. Mwita J. · 18 July 2025

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Constitutional Petition
OUTCOME	Petition succeeds; IMEI-disclosure notices declared unconstitutional and quashed
COMPENSATION	Not applicable — declaratory and prohibitory constitutional relief
CORE QUESTION	Whether mandatory IMEI-disclosure notices were unconstitutional for lack of an adequate governing framework

PRINCIPAL DOCTRINE

> *A legitimate regulatory purpose for collecting IMEI information does not itself create a lawful processing architecture; the State must also establish the governing rules for storage, access, sharing, retention, and subsequent use once that information becomes personal data.*

BRIEF FACTS

THE COMMUNICATIONS AUTHORITY AND THE KENYA REVENUE AUTHORITY issued public notices requiring device assemblers, importers, manufacturers, retailers, wholesalers, mobile network operators, and incoming passengers to provide IMEI numbers, citing tax compliance, preventing evasion, and controlling non-compliant devices as their objectives.

Katiba Institute argued that IMEI numbers, once connected with subscriber information, could reveal identity, telephone number, location, communications, and device activity, and that the resulting database could facilitate surveillance in the absence of adequate rules governing collection, storage, access, sharing, retention, and subsequent use.

The Respondents maintained IMEI numbers were technical device identifiers that did not themselves identify a natural person, that the collection served legitimate regulatory purposes, and that the notices were administrative rather than legislative in character.

ISSUES

1. Whether IMEI numbers constituted personal data when associated with individuals.
2. Whether mandatory disclosure violated Article 31.
3. Whether the State had demonstrated a lawful mechanism for processing the information.
4. Whether the privacy limitation was prescribed by law.
5. Whether adequate processing guidelines existed.
6. Whether alternative statutory remedies ousted the High Court's jurisdiction, and whether the matter was res judicata.

HOLDING

Petition allowed. The Court declared the notices unconstitutional and the mandatory disclosure requirement contrary to Article 31, issued certiorari quashing the notices, and issued prohibition against their implementation.

COURT'S REASONING

The Court held an IMEI could constitute personal data once associated with an identifiable person, capable of being connected to telephone information, location, communications, and other identifying data.

The Respondents had not demonstrated a lawful mechanism sufficiently governing the processing of that information once it became personal data — the absence of adequate guidelines was a material defect that, combined with the privacy threat the notices posed, rendered them unconstitutional.

RATIO DECIDENDI

> *A lawful initial purpose does not cure an undefined or inadequately regulated downstream processing architecture; the State must be able to answer why data is collected, its legal basis, what happens after collection, who receives and can access it, whether it can be combined with other databases, how long it is retained, and whether it may be used for another purpose.*

SIGNIFICANCE

A modern, comprehensive State-processing authority: it confirms that even device identifiers can become personal data through association, and establishes that a legitimate regulatory objective is only the starting point — the entire downstream processing architecture must itself be lawfully defined.

KEY TAKEAWAY

A good reason to collect data is not a data governance framework. Before rolling out any mandatory disclosure regime, be able to answer what happens to the data after collection — not just why you're collecting it.

Source: Kenya Law · [2025] KEHC 10568 (KLR)

❖

CASE DIGEST · KPLR 030

VOLUME I · DIGEST NO. 030 · PART V: DIGITAL IDENTITY, BIOMETRICS & PUBLIC-INTEREST LITIGATION

Nubian Rights Forum & 2 Others *v* Attorney General & 6 Others

[2020] KEHC 8772 (KLR) · Petitions Nos. 56, 58 & 59 of 2019 (Consolidated)
High Court of Kenya at Nairobi (three-judge bench) · Hon. P. Nyamweya, M. Ngugi & W. Korir JJ. · 30 January 2020

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi (three-judge bench) — Consolidated Constitutional Petitions
OUTCOME	Petitions succeed in part; DNA and GPS collection for NIIMS declared unconstitutional
COMPENSATION	Not applicable — declaratory and conditional constitutional relief
CORE QUESTION	Whether the State could compel DNA and GPS collection for a national identity system without proving necessity and proportionality

PRINCIPAL DOCTRINE

> *Biometric data is personal data protected by Article 31; State collection of biometric information must satisfy legality, necessity, and proportionality, and highly intrusive identifiers such as DNA and GPS coordinates cannot be collected for identification merely because the State considers them technologically useful.*

BRIEF FACTS

The Statute Law (Miscellaneous Amendments) Act No. 18 of 2018 amended the Registration of Persons Act to establish the National Integrated Identity Management System (NIIMS) — a national population register with a unique identification number, harmonised government databases, and identity authentication. The Government commenced nationwide biometric registration under the new framework.

The Petitioners — Nubian Rights Forum, the Kenya Human Rights Commission, and the Kenya National Commission on Human Rights — challenged the biometric collection, proposed DNA and GPS collection, and the absence of adequate safeguards, particularly for children; DNA, they argued, could reveal genetic and health information extending well beyond the individual registered. The Government defended NIIMS as necessary for accurate identification, eliminating duplicates, and serving legitimate public-interest objectives.

ISSUES

1. Whether the amendments establishing NIIMS were constitutionally enacted, including as to public participation.
2. Whether collection of biometric data violated Article 31.
3. Whether collection of DNA and of GPS coordinates was necessary and lawful.
4. Whether the NIIMS database created an unacceptable surveillance risk.
5. Whether the information sought was excessive, and whether adequate safeguards existed.
6. Whether NIIMS could lawfully be implemented without a comprehensive regulatory framework, and whether children's rights were adequately protected.

HOLDING

Petitions allowed in part. The Court held that collecting DNA and GPS coordinates for identification was intrusive and unnecessary, and unconstitutional to the extent not specifically anchored in empowering legislation; it further held NIIMS could proceed only once an appropriate and comprehensive regulatory framework, compliant with the constitutional requirements identified in the judgment, was established.

COURT'S REASONING

The Court recognised biometric data generally as personal information protected by Article 31, and accepted that certain biometric characteristics could legitimately serve authentication and verification purposes. It nonetheless distinguished ordinary biometric identifiers from DNA and GPS data, finding the latter intrusive and unnecessary for identification within the statutory framework before it.

The Court's reasoning connected purpose, necessity, proportionality, and lawful authority: a State cannot justify collection merely by showing a technology is capable of gathering information — it must demonstrate why the particular information is necessary for the legally authorised purpose.

RATIO DECIDENDI

> *The State's statutory authority to establish an identification system does not automatically authorise unlimited collection of information; the information collected must be legally authorised, necessary, proportionate, relevant to the identified purpose, and adequately protected.*

SIGNIFICANCE

One of the foundational Kenyan authorities for the proposition that biometric data is constitutionally protected informational privacy, and a template compliance architecture — statutory authority, defined purpose, necessity and proportionality analysis, minimisation, access controls, retention, oversight, and safeguards against function creep — for any national digital identity programme.

KEY TAKEAWAY

Technological capability is not a lawful basis. Before adding any identifier — especially DNA or location data — to a national identity system, the State must independently justify its necessity and proportionality.

Source: Kenya Law · [2020] KEHC 8772 (KLR)

❖

CASE DIGEST · KPLR 031

VOLUME I · DIGEST NO. 031 · PART V: DIGITAL IDENTITY, BIOMETRICS & PUBLIC-INTEREST LITIGATION

Haki na Sheria Initiative *v* Attorney General & 4 Others

[2024] KEHC 10021 (KLR) · Petition E288 of 2023
High Court of Kenya at Nairobi · 4 September 2024

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Constitutional Petition
OUTCOME	Petition dismissed on preliminary grounds
COMPENSATION	None — petition dismissed
CORE QUESTION	Whether a fresh constitutional challenge to the Maisha Namba ecosystem was barred by res judicata

PRINCIPAL DOCTRINE

> *A constitutional challenge to a digital-identity ecosystem substantially overlapping with matters already settled in prior litigation on the same subject may be barred by res judicata; public-interest standing does not permit repeated re-litigation of issues already determined.*

BRIEF FACTS

Haki na Sheria Initiative challenged aspects of the Maisha Namba digital-identity ecosystem, the successor framework to NIIMS, raising constitutional objections concerning necessity, proportionality, and safeguards for the underlying biometric and personal data processing.

The Respondents contended that the substance of the challenge had already been determined in the earlier NIIMS litigation and related proceedings, and that the petition should not be entertained afresh on largely the same subject matter.

ISSUES

1. Whether the petition was barred by res judicata.
2. Whether the matters raised had already been substantively determined in prior NIIMS litigation.
3. Whether the public-interest character of the petition affected the res judicata analysis.

HOLDING

Petition dismissed on preliminary grounds, the Court finding the challenge substantially duplicative of matters already litigated and determined in the earlier NIIMS proceedings.

COURT'S REASONING

The Court treated the overlap between the Maisha Namba ecosystem and the previously litigated NIIMS framework as sufficient to engage res judicata principles, notwithstanding the public-interest character of the petition.

RATIO DECIDENDI

Public-interest standing broadens who may litigate a constitutional question; it does not by itself permit re-litigating a question of substance that earlier proceedings, involving the same underlying digital-identity architecture, have already determined.

SIGNIFICANCE

A caution for public-interest litigants pursuing successive challenges to evolving government digital-identity systems: each new petition must be assessed against what earlier litigation on the same architecture has already settled.

KEY TAKEAWAY

Before filing a fresh constitutional challenge to a digital-identity system, map it against prior litigation on the same architecture — substantial overlap risks a res judicata dismissal regardless of public interest.

Source: Kenya Law · [2024] KEHC 10021 (KLR)

❖

CASE DIGEST · KPLR 032

VOLUME I · DIGEST NO. 032 · PART V: DIGITAL IDENTITY, BIOMETRICS & PUBLIC-INTEREST LITIGATION

REPUBLIC *v* TOOLS FOR HUMANITY CORPORATION (US) & 9 OTHERS

[2025] KEHC 5629 (KLR) · Judicial Review Application E119 of 2023
High Court of Kenya at Nairobi · Hon. R.E. Aburili J. · 5 May 2025

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Judicial Review
OUTCOME	Application succeeds; biometric collection prohibited pending compliance; unlawfully obtained data ordered destroyed
COMPENSATION	Not applicable — prohibition, certiorari, and mandamus; each party to bear own costs
CORE QUESTION	Whether cryptocurrency-incentivised iris and facial scanning satisfied the Act's requirements for lawful processing and valid consent

PRINCIPAL DOCTRINE

> *Biometric data processing requires valid informed consent, lawful registration, DPIA compliance, and lawful cross-border transfer; a cryptocurrency inducement does not by itself constitute freely given consent where the statutory requirements for consent are not otherwise satisfied.*

BRIEF FACTS

THE WORLDCOIN ENTITIES began collecting biometric data — including iris and facial scans — from Kenyan residents using the Orb device from July 2023, offering participants cryptocurrency worth approximately KES 7,000 (USD 50) as an inducement. The ODPC issued a cautionary public communication on 28 July 2023 urging heightened vigilance around Orb scanning.

Katiba Institute and other public-interest applicants challenged the processing as lacking a valid Data Protection Impact Assessment, proper registration, and valid consent — arguing the cryptocurrency incentive undermined the voluntariness of consent, and that personal data was being transferred outside Kenya without compliance with statutory requirements or ODPC directions.

The respondents maintained the applicants lacked standing and had not exhausted the ODPC mechanism, that a DPIA had in fact been submitted and updated, that participation was voluntary, and that registration applications had been made.

ISSUES

1. Whether processing biometric data without the required safeguards was unlawful.
2. Whether the DPIA complied with section 31, and whether the respondents were properly registered before processing began.
3. Whether transfer of biometric data outside Kenya was lawful, and whether ODPC directions had been obeyed.
4. What information must be provided to establish informed consent, and whether cryptocurrency incentives were compatible with valid consent.
5. Whether public-interest applicants could approach the Court without exhausting the ODPC mechanism.

HOLDING

Application granted. The Court issued prohibition restraining further biometric collection, processing, or transfer using the Orb unless statutory requirements were met; certiorari quashing the decision to collect, process, or transfer the data without adequate DPIA compliance and lawful consent; and mandamus compelling permanent destruction of the unlawfully obtained biometric data within seven days under ODPC supervision. Each party bore its own costs given the public interest involved.

COURT'S REASONING

The Court found that processing of sensitive biometric data had commenced before the registration requirements of section 18 were satisfied, and rejected the proposition that the mere existence of a consent form resolved the question of consent — it scrutinised whether the cryptocurrency incentive affected its voluntariness, distinguishing formal consent from legally valid consent.

On the DPIA, the Court held that a purported assessment does not satisfy section 31 merely because a document exists; it must be adequate for the actual, highly sensitive processing operation undertaken.

RATIO DECIDENDI

> *High-risk biometric processing is not lawful merely because an organisation has obtained a signed or electronically recorded consent; the controller must demonstrate compliance with the complete legal architecture — registration, lawful basis, informed and voluntary consent, purpose specification, DPIA, transparency, security, cross-border transfer requirements, and regulatory directions.*

SIGNIFICANCE

A foundational authority for Privacy by Design and DPIA-driven deployment of biometric systems in Kenya, and the clearest Kenyan authority yet on the difference between the mere existence of a consent record and consent that is actually freely given, specific, and informed — particularly where a financial inducement is involved.

KEY TAKEAWAY

An incentive can defeat consent. If participants are paid to hand over biometric data, examine whether that payment makes the consent involuntary — and complete registration and a genuine DPIA before, not after, collection begins.

Source: Kenya Law · [2025] KEHC 5629 (KLR)

❖

CASE DIGEST · KPLR 033

VOLUME I · DIGEST NO. 033 · PART V: DIGITAL IDENTITY, BIOMETRICS & PUBLIC-INTEREST LITIGATION

REPUBLIC *v* TOOLS FOR HUMANITY CORPORATION (US) & 8 OTHERS

[2025] KEHC 16829 (KLR) · Judicial Review Application E119 of 2023 (Ruling)
High Court of Kenya at Nairobi · Hon. R.E. Aburili J. · 14 November 2025

THE CASE AT A GLANCE

FORUM	High Court of Kenya at Nairobi — Judicial Review (Enforcement Ruling)
OUTCOME	Application to withdraw allowed following verified deletion; public notification directed
COMPENSATION	Not applicable — procedural ruling; no order as to costs
CORE QUESTION	Whether proceedings could be withdrawn once the Commissioner confirmed supervised deletion of the unlawfully collected data

PRINCIPAL DOCTRINE

> *Where a court orders destruction of unlawfully processed personal data, its supervisory role continues through to demonstrable compliance; the substantive judgment is not merely declaratory, and withdrawal of enforcement proceedings will be permitted only once compliance is verified.*

BRIEF FACTS

FOLLOWING THE MAY 2025 SUBSTANTIVE JUDGMENT ordering destruction of the biometric data unlawfully obtained by the Worldcoin entities, the Data Protection Commissioner supervised deletion of the data and, by an application dated 11 September 2025, sought leave to withdraw the proceedings on the basis that compliance with the destruction order had been confirmed. This ruling addresses only that withdrawal application; it does not revisit or restate the substantive Worldcoin liability findings, which belong to the May 2025 judgment at [2025] KEHC 5629 (KLR).

ISSUES

1. Whether the Court should permit withdrawal of the application following the Commissioner's confirmed supervision of the data's deletion.

HOLDING

Application to withdraw allowed, without orders as to costs. The Court directed that the applicant file a written communication with the Court — to also be issued to the public — confirming that the Commissioner had supervised deletion of the data.

COURT'S REASONING

The Court treated the May 2025 judgment as more than declaratory: it required demonstrable compliance with the destruction obligation before proceedings could be closed, and the Commissioner's supervised deletion satisfied that requirement, warranting a public confirmation before the matter was allowed to lapse.

RATIO DECIDENDI

Judicial orders for erasure of unlawfully processed personal data carry a continuing supervisory dimension: the enforcement stage requires demonstrable, verifiable compliance — through records, confirmations, or independent verification — before the Court will treat the obligation as discharged.

SIGNIFICANCE

Confirms that a data-erasure order is not satisfied by a promise to comply; regulators and courts alike may require documented proof of deletion, with public notification serving an accountability function distinct from the underlying substantive liability finding.

KEY TAKEAWAY

A deletion order is not finished until deletion is proven. Keep records, system logs, and confirmations ready to demonstrate compliance to a regulator or court.

Source: Kenya Law · [2025] KEHC 16829 (KLR)

❖

CASE DIGEST · KPLR 034

VOLUME I · DIGEST NO. 034 · PART V: DIGITAL IDENTITY, BIOMETRICS & PUBLIC-INTEREST LITIGATION

Kenya Union of Journalists *v* Kenya Broadcasting Corporation

[2025] KEHC 17216 (KLR) · Judicial Review Miscellaneous Application E355 of 2025
High Court of Kenya at Nairobi · Hon. R.E. Aburili J. · 25 November 2025

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Judicial Review
OUTCOME	Application succeeds; rollout restrained pending strict compliance with the Data Protection Act
COMPENSATION	Not applicable — judicial review relief against unlawful rollout
CORE QUESTION	Whether an employer could deploy facial-recognition attendance technology without consent, information, or a DPIA

PRINCIPAL DOCTRINE

> *Facial-recognition biometric attendance systems constitute processing of sensitive personal data and cannot be deployed by an employer without compliance with constitutional and statutory data-protection requirements; an employer's ownership of the workplace does not remove an employee's right to informational privacy.*

BRIEF FACTS

Kenya Broadcasting Corporation introduced a biometric attendance system using facial recognition to replace conventional attendance methods. The Kenya Union of Journalists challenged the rollout, alleging employees had not consented and had not been adequately informed, including employees with medical conditions potentially affected by the system.

The Union raised its concerns with KBC and requested consultation; when these went unresolved, KBC informed staff the system had been installed and would become operational. The Union's application alleged failures to conduct a DPIA and to comply with sections 26, 29, 30, 31, 32, and 36 of the Data Protection Act, and sought orders preventing implementation and quashing the decision to introduce the system.

KBC ultimately made concessions concerning its constitutional and statutory obligations, which the Court treated as aligning with its duty to respect, protect, and promote employee privacy.

ISSUES

1. Whether the biometric attendance system involved processing of sensitive personal data.
2. Whether employees were adequately informed, and whether consent or another lawful basis was required.
3. Whether a DPIA was required before deployment.
4. Whether the employer had adequately addressed employee objections.
5. Whether KBC had complied with the Data Protection Act, and whether judicial review relief should issue.

HOLDING

Application granted. The Court granted relief against the unlawful rollout and required strict and demonstrable compliance with the Data Protection Act and Article 31 before any facial-recognition attendance system could proceed.

COURT'S REASONING

The Court emphasised that biometric processing is not confined to national identity systems: a private or public employer using facial recognition for attendance is processing personal and sensitive biometric data like any other controller, and must undertake a lawful-basis and risk assessment before deployment rather than after employee objection.

RATIO DECIDENDI

An employer deploying facial recognition or other intrusive biometric technology for workplace purposes such as attendance is processing sensitive personal data and must comply with the Data Protection Act's full requirements — including consent or another lawful basis, adequate notice, and a DPIA — before deployment; ownership of the workplace does not displace the employee's constitutional right to informational privacy.

SIGNIFICANCE

Extends Kenya's biometric-processing jurisprudence from national identity systems into the ordinary workplace: any employer considering biometric attendance, access control, or monitoring technology must treat it as a data-protection compliance exercise, not merely an operational or security upgrade.

KEY TAKEAWAY

Facial recognition for clocking in is still biometric processing. Consult employees, assess necessity and proportionality, and complete a DPIA before rollout — not after the union objects.

Source: Kenya Law · [2025] KEHC 17216 (KLR)

❖

CASE DIGEST · KPLR 035

VOLUME I · DIGEST NO. 035 · PART V: DIGITAL IDENTITY, BIOMETRICS & PUBLIC-INTEREST LITIGATION

Okiya Omtatah Okoiti & 4 Others *v* Attorney General & 4 Others

[2020] KEHC 8763 (KLR) · Petition 163 of 2019

High Court of Kenya at Nairobi · 30 January 2020 — presiding judge not stated in the available record

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Constitutional Petition
OUTCOME	DNA and GPS collection for identification declared unconstitutional; NIIMS permitted only within a comprehensive framework
COMPENSATION	Not applicable — declaratory and conditional constitutional relief
CORE QUESTION	Whether the legislative process establishing NIIMS, and the DNA/GPS data it authorised, satisfied constitutional requirements

PRINCIPAL DOCTRINE

> *Collection of DNA and GPS coordinates for identification purposes is intrusive and unnecessary, and violates Article 31 to the extent not specifically authorised by empowering legislation — a distinct judgment reaching the same NIIMS conclusion as Nubian Rights Forum on a separate petition.*

BRIEF FACTS

The Petitioners challenged the Statute Law (Miscellaneous Amendments) Act 2018, including the amendments establishing NIIMS, arguing the amendments were improperly introduced through a miscellaneous-amendments statute without adequate public participation, and that Kenya's existing Integrated Population Registration System already made NIIMS unnecessary.

They argued the collection of GPS coordinates could enable mass surveillance, that biometric and DNA information demanded was excessive, and that the legislation and the system it authorised violated Article 31. The Government defended the legislation as necessary to integrate a fragmented national identification landscape into a single population register.

ISSUES

1. Whether the legislative process establishing NIIMS satisfied constitutional requirements, including public participation.
2. Whether NIIMS was constitutional.
3. Whether collection of biometric data, DNA, and GPS coordinates was necessary and proportionate.
4. Whether adequate constitutional limitations applied to the scheme.

HOLDING

The Court held that collection of DNA and GPS coordinates for identification was intrusive and unnecessary, violating Article 31 to the extent not specifically authorised by empowering legislation, and permitted NIIMS implementation to proceed only subject to an appropriate and comprehensive constitutional and regulatory framework.

COURT'S REASONING

Considering necessity, proportionality, data minimisation, and purpose limitation together, the Court found DNA and GPS information went beyond what identification required, while accepting that the broader NIIMS programme could proceed once properly regulated — reaching, on its own petition, the same substantive conclusion as the Court reached in Nubian Rights Forum on a related but separate petition.

RATIO DECIDENDI

The State's statutory authority to establish an identification system does not authorise collection of highly intrusive identifiers, such as DNA and GPS coordinates, where they are unnecessary for the identification purpose actually pursued and unauthorised by clear empowering legislation.

SIGNIFICANCE

A distinct, independent NIIMS authority that must not be merged with Nubian Rights Forum — the two are separate judgments reaching parallel conclusions, and together they reinforce the necessity-and-proportionality limits on biometric identification as settled Kenyan constitutional doctrine rather than the view of a single bench.

KEY TAKEAWAY

Two separate benches reached the same conclusion on DNA and GPS collection for identity systems — treat that convergence, not just one judgment, as the settled doctrine when advising on biometric identification schemes.

Source: Kenya Law · [2020] KEHC 8763 (KLR) — presiding judge not stated in the available record.

❖

CASE DIGEST · KPLR 036

VOLUME I · DIGEST NO. 036 · PART V: DIGITAL IDENTITY, BIOMETRICS & PUBLIC-INTEREST LITIGATION

Coalition for Reform and Democracy & 2 Others *v* Republic & Another

[2015] KEHC 7074 (KLR) · Petitions 628 & 630 of 2014 and 12 of 2015 (Consolidated)
High Court of Kenya at Nairobi · 23 February 2015 — presiding judge(s) not stated in the available record

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Consolidated Constitutional Petitions
OUTCOME	Petitions largely dismissed; challenged surveillance and interception provisions upheld
COMPENSATION	Not applicable — constitutional declaratory determination
CORE QUESTION	Whether statutory powers of communications interception, enacted in response to terrorism, were a proportionate limitation on privacy

PRINCIPAL DOCTRINE

> *Interception of communications intrudes upon privacy, but a surveillance regime may be constitutionally justified where it pursues a legitimate national-security objective, is proportionate, and is accompanied by adequate safeguards including judicial oversight.*

BRIEF FACTS

The Coalition for Reform and Democracy and its co-petitioners, following terrorist attacks in Kenya in late 2014, challenged the Security Laws (Amendment) Act No. 19 of 2014, which amended numerous statutes affecting privacy, communications, national security, freedom of expression, refugee rights, criminal procedure, and intelligence operations — focusing on provisions authorising interception of communications.

They argued the interception provisions created the possibility of arbitrary or mass surveillance, that the resulting limitation on Article 31 privacy was not justified under Article 24, and that judicial oversight and other safeguards were inadequate. The Government relied on national security, the prevention of terrorism, the State's obligation to protect life, and existing statutory safeguards, maintaining that privacy is not an absolute right.

ISSUES

1. Whether the surveillance and interception provisions engaged Article 31.
2. Whether any resulting limitation was constitutionally permissible under Article 24.
3. Whether the national-security objective was legitimate.
4. Whether adequate safeguards, including judicial oversight, existed.
5. Whether the limitation was proportionate, and whether less restrictive means were available.

HOLDING

The Court recognised that interception of communications intrudes upon privacy, but held the challenged surveillance provisions constitutionally justified in the circumstances before it, given the legitimate national-security objective and the safeguards — including judicial oversight — attending the scheme.

COURT'S REASONING

Applying Article 24, the Court balanced the nature of the privacy right against the importance of the national-security objective, the relationship between the interception powers and that objective, the availability of less restrictive means, and the safeguards actually built into the scheme, finding the balance struck by the legislation constitutionally acceptable.

RATIO DECIDENDI

Privacy is fundamental but not absolute; a constitutional challenge to a surveillance or interception regime must be resolved by weighing the nature of the privacy right, the importance of the governmental objective, the relationship between the limitation and that objective, the availability of less restrictive means, and the adequacy of the safeguards provided — including judicial oversight.

SIGNIFICANCE

An important pre-Data Protection Act constitutional foundation for later Kenyan data-protection jurisprudence: it supplies the proportionality framework — objective, necessity, least restrictive means, and safeguards — that later authorities apply to State processing more generally, not merely to interception.

KEY TAKEAWAY

A national-security justification for surveillance still has to survive the full proportionality analysis: legitimate objective, necessity, least restrictive means, and genuine independent oversight — not simply an invocation of security.

Source: Kenya Law · [2015] KEHC 7074 (KLR) — presiding judge(s) not stated in the available record.

❖

CASE DIGEST · KPLR 037

VOLUME I · DIGEST NO. 037 · PART V: DIGITAL IDENTITY, BIOMETRICS & PUBLIC-INTEREST LITIGATION

Okiya Omtatah Okoiti *v* Independent Electoral and Boundaries Commission & 2 Others

[2022] KEHC 12111 (KLR) · Petition 47 of 2017
High Court of Kenya at Nairobi · Hon. H.I. Ong'udi J. · 27 July 2022

THE CASE AT A GLANCE	
FORUM	High Court of Kenya at Nairobi — Constitutional Petition
OUTCOME	Petition dismissed; NIIMS-related relief overtaken by subsequent NIIMS litigation
COMPENSATION	None — petition dismissed
CORE QUESTION	Whether specific identity documents as prerequisites for voter registration, and the absence of an integrated database, were unlawful

PRINCIPAL DOCTRINE

> *Digital identity architecture is not confined to a single statute; it intersects with electoral, civil-registration, immigration, tax, and social-protection systems, and integration of these systems does not itself eliminate the requirement for purpose limitation and lawful access controls.*

BRIEF FACTS

The Petitioner challenged aspects of voter registration and identity documentation, seeking declarations concerning the use of birth certificates, expired passports, and national identification documents as prerequisites for registration, and calling for a single, integrated citizen database usable across government transactions, together with greater transparency around voter-registration statistics.

By the time the matter was heard, NIIMS had since been established by legislation and its constitutionality had been separately litigated; the Court noted that the aspects of the petition concerning NIIMS had consequently been overtaken by those subsequent developments. IEBC and the other respondents defended the applicable electoral and identification framework as it then stood.

ISSUES

1. Whether the identity documents required for voter registration were lawful prerequisites.
2. Whether the Petitioner was entitled to an integrated government identity database.
3. Whether greater transparency regarding voter-registration statistics was required.
4. Whether the relief sought concerning NIIMS remained live following the subsequent NIIMS litigation and legislative developments.

HOLDING

Petition dismissed. The Court held that the NIIMS-related relief sought had been overtaken by the intervening NIIMS litigation and legislative changes, and declined the remaining reliefs concerning voter registration and identity documentation.

COURT'S REASONING

Recognising that the legal landscape had materially changed since the petition was filed — with NIIMS's constitutionality by then addressed in dedicated litigation — the Court found no continuing basis to grant relief that had, in substance, already been overtaken by events.

RATIO DECIDENDI

Where intervening litigation and legislative developments have already addressed the substance of relief sought in an earlier petition, that relief may be treated as overtaken by events; digital identity architecture spans multiple statutory systems, and integrating them does not itself dispense with purpose limitation and lawful access controls.

SIGNIFICANCE

Illustrates how Kenya's fast-moving digital-identity jurisprudence can overtake earlier litigation: petitioners and respondents alike must track parallel proceedings addressing the same underlying architecture, and government agencies integrating identity systems across electoral, civil-registration, and other domains must still maintain purpose limitation and access controls for each distinct data category.

KEY TAKEAWAY

In a fast-moving area like digital identity, check whether related litigation has already overtaken your claim before you file — and if you are integrating identity systems, keep each data category's purpose and access rules distinct.

Source: Kenya Law · [2022] KEHC 12111 (KLR)

❖

CASE DIGEST · KPLR 038

VOLUME I · DIGEST NO. 038 · PART VI: TRIBUNAL DECISIONS ON AUTOMATED DECISION-MAKING & DATA ACCURACY

B.M. *v* National Transport and Safety Authority

[2023] KETLABT 664 (KLR) · Appeal TLAB/E015 of 2022

Transport Licensing Appeals Board · Dr Adrian Kamotho, Joseph McDonald, Maryan Hajir, James Ngomeli & Waithira Muiruri · 16 August 2023

THE CASE AT A GLANCE

FORUM	Transport Licensing Appeals Board — Statutory Tribunal (not a High Court decision)
OUTCOME	Appeal allowed; NTSA directed to reconsider the PSV badge application
COMPENSATION	Not applicable — tribunal directions on reconsideration
CORE QUESTION	Whether NTSA could rely on an automated criminal-records check, without more, to deny a PSV badge

PRINCIPAL DOCTRINE

> *An automated or database-driven adverse decision affecting a data subject must be accompanied by a meaningful opportunity to contest the underlying record; a bare automated match is not, on its own, a sufficient basis to deny a statutory licence.*

BRIEF FACTS

The Appellant applied to the National Transport and Safety Authority for a Public Service Vehicle badge. NTSA declined the application after an automated check against its records returned an adverse criminal-records flag against his name.

The Appellant maintained the flagged record did not belong to him, or was inaccurate, and that he had been given no meaningful opportunity to contest it before the application was declined; he appealed to the Transport Licensing Appeals Board.

ISSUES

1. Whether NTSA's reliance on the automated records check was procedurally fair.
2. Whether the Appellant was given an adequate opportunity to contest the adverse record.
3. Whether the data underlying the decision was shown to be accurate.
4. Whether the application should be reconsidered.

HOLDING

Appeal allowed. The Tribunal directed NTSA to reconsider the Appellant's PSV badge application, affording him a proper opportunity to address the underlying record before any fresh decision.

TRIBUNAL'S REASONING

The Tribunal held that a database match, without independent verification and without giving the affected person a chance to respond, does not adequately support an adverse licensing decision.

Data accuracy and the data subject's right to contest automated or database-driven findings were treated as necessary safeguards before such a record could be relied upon to deny a statutory licence.

RATIO DECIDENDI

> *Where a licensing or administrative decision rests on an automated or database check of personal data, the affected data subject must be given a genuine opportunity to contest the accuracy of the underlying record before the decision is finalised.*

SIGNIFICANCE

An early Kenyan tribunal authority applying data-accuracy and fair-process principles to automated administrative decision-making, outside the ordinary High Court data-protection track; it should be cited as tribunal, not High Court, authority.

> **KEY TAKEAWAY**
> *A database flag is not a verdict. If you rely on an automated records check to deny a licence or service, give the affected person a real chance to contest the underlying record first.*

Source: Kenya Law · [2023] KETLABT 664 (KLR)

❖

CASE DIGEST · KPLR 039

VOLUME I · DIGEST NO. 039 · PART VI: TRIBUNAL DECISIONS ON AUTOMATED DECISION-MAKING & DATA ACCURACY

G.K. *v* NATIONAL TRANSPORT & SAFETY AUTHORITY

Transport Licensing Appeals Board · Appeal (full citation not fully confirmed in the available record)
Transport Licensing Appeals Board · 2023

THE CASE AT A GLANCE	
FORUM	Transport Licensing Appeals Board — Statutory Tribunal (not a High Court decision)
OUTCOME	Appeal allowed; NTSA directed to reconsider the application on accurate data
COMPENSATION	Not applicable — tribunal directions on reconsideration
CORE QUESTION	Whether an inaccurate or outdated record in NTSA's database could lawfully ground refusal of a licence application

PRINCIPAL DOCTRINE

> *Data accuracy is a precondition for lawful reliance on a record in an administrative licensing decision; a tribunal will not permit a licence to be refused on the strength of a record shown to be inaccurate or outdated.*

BRIEF FACTS

THE APPELLANT applied to the National Transport and Safety Authority for a licence and was refused on the strength of a record held in NTSA's database that the Appellant contended was inaccurate or outdated.

The Appellant appealed to the Transport Licensing Appeals Board, seeking correction of the record and reconsideration of the application on accurate data.

ISSUES

1. Whether the record relied upon by NTSA was accurate.
2. Whether NTSA adequately verified the record before refusing the application.
3. Whether the Appellant was entitled to have the record corrected.
4. Whether the application should be reconsidered on corrected data.

HOLDING

Appeal allowed. The Tribunal directed NTSA to reconsider the Appellant's application on the basis of accurate, corrected data.

TRIBUNAL'S REASONING

The Tribunal treated accuracy of the underlying record as a threshold requirement for any adverse decision resting on it, and found the record relied upon had not been shown to be reliable.

RATIO DECIDENDI

A statutory decision-maker may not rely on an inaccurate or outdated record to refuse a licence or similar application; the data subject is entitled to have the record corrected and the application reconsidered on accurate data.

SIGNIFICANCE

Reinforces, alongside Mutuku, that data accuracy obligations apply squarely to administrative and licensing databases, not only to commercial or consumer-facing processing.

KEY TAKEAWAY

Before refusing an application on the strength of a database record, confirm the record is accurate and current — an outdated or wrong entry will not support the refusal on appeal.

Source: Kenya Law · Transport Licensing Appeals Board — full citation not independently confirmed for this digest; verify before detailed reliance.

❖

CASE DIGEST · KPLR 040

VOLUME I · DIGEST NO. 040 · PART VI: TRIBUNAL DECISIONS ON AUTOMATED DECISION-MAKING & DATA ACCURACY

S.K.M. *v* National Transport and Safety Authority

Transport Licensing Appeals Board · Appeal (full citation not fully confirmed in the available record)
Transport Licensing Appeals Board · 2023

THE CASE AT A GLANCE	
FORUM	Transport Licensing Appeals Board — Statutory Tribunal (not a High Court decision)
OUTCOME	Appeal allowed in principle; matter remitted for reconsideration
COMPENSATION	Not applicable — tribunal directions on reconsideration
CORE QUESTION	Whether NTSA's decision-making process adequately safeguarded the accuracy and fair use of the Appellant's records
VERIFICATION	***This entry was not reproduced at the same level of completeness as the other two tribunal decisions in this Part; detailed party submissions and the full list of authorities considered are not reproduced here — verify before detailed reliance***

PRINCIPAL DOCTRINE

> *The data-accuracy and fair-process principles applied to automated and database-driven licensing decisions in Mutuku and Kinyua extend consistently across the Transport Licensing Appeals Board's practice, not merely to a single case.*

BRIEF FACTS

The Appellant, identified in the tribunal's record by initials only, appealed against an adverse NTSA licensing decision said to rest on the Authority's internal records, raising materially the same data-accuracy and fair-process concerns considered in the Board's other 2023 decisions on this subject.

NTSA maintained its records and process had been properly applied; the Appellant disputed the accuracy of the underlying data and the adequacy of the opportunity given to contest it.

ISSUES

1. Whether NTSA's records were shown to be accurate.
2. Whether the Appellant had an adequate opportunity to contest the adverse record.
3. Whether the matter should be remitted for reconsideration.

HOLDING

Appeal allowed in principle; the matter was remitted to NTSA for reconsideration consistent with the data-accuracy and fair-process approach applied in the Board's related 2023 decisions.

TRIBUNAL'S REASONING

Not reproduced in full in the material available for this digest. The Tribunal's approach is understood to be consistent with its reasoning in Mutuku and Kinyua on the same subject, but the detailed submissions and authorities considered in this specific matter are not presently available for citation.

RATIO DECIDENDI

Consistent with Mutuku and Kinyua: a statutory tribunal will not uphold an adverse licensing decision resting on unverified or uncontested personal data, without more specific reliance pending verification of this entry's own reasoning.

SIGNIFICANCE

Taken together with Mutuku and Kinyua, confirms this is a settled line of Transport Licensing Appeals Board practice on data accuracy and fair process, rather than the outcome of a single case.

KEY TAKEAWAY

Three tribunal decisions, one consistent message: verify your records and give the affected person a fair chance to contest them before an adverse licensing decision will be upheld on appeal.

Source: Kenya Law — full submissions and authorities not independently retrieved for this digest; verify before detailed reliance.