REPUBLIC OF KENYA

IN THE HIGH COURT AT NYERI

CIVIL APPEAL NO. E005 OF 2025

TAIFA DT SACCO SOCIETY LIMITED..... APPELLANT

VERSUS

BOSCO OTIENO..... RESPONDENT

JUDGMENT

1. This is an appeal from the decision of Immaculate Kassait, Data Commissioner, delivered on 3.1.2025 in ODPC No. 1779 of 2024.

2. The Memorandum of Appeal dated 18.12.2025 raised the following grounds:

    (i) The Honourable Commissioner of data protection misdirected herself that the information received by the Respondent from the Appellant infringed his right to privacy.

    (ii) The Honourable Commissioner of data protection misdirected herself that the Respondent was a subject whereas his personal information was received by a third party.

(iii) The Honourable Commissioner of data protection misdirected herself in holding that the respondent's personal information and/or particulars is processed by the appellant to other parties who threatens his individual privacy.

(iv) The Honourable Commissioner erred in law and fact in holding that the Appellant had obligation to protect the Respondent's personal data.

(v) The Honorable Commissioner of data protection misdirected herself in holding that the respondent's individual privacy was threatened by receiving third-party confidential information.

(vi) The Honourable Commissioner of data protection misdirected herself in failing to appreciate that the holder of an account with the Appellant, one ZWM, was the registered owner of telephone number 0721XXX416, which was allocated to the Respondent by the mobile telephone providers.

(vii) The Honourable Commissioner of data protection misdirected herself in failing to appreciate that the messages were honestly in good faith and the Respondents who apologized for these actions.

(viii) The Honorable Commissioner of data protection misdirected herself in failing to summon the original owner of telephone number 0721XXX416, and the Respondent to record a statement with the police on

the ownership of the mobile number, which is the subject of the complaint.

(ix) The Honourable Commissioner of data protection erred in holding that actions of the appellant violated the rights under Article 31 of the Constitution and therefore arrived at a wrong decision in awarding damages.

Pleadings

3. On 4.11.2024, the Respondent lodged a complaint against the Appellant with the Office of the Data Protection Commissioner, alleging violation of his privacy. It was the Respondent's case that the Appellant had consistently sent credit and debit alerts since 2022, yet he was not a member of the Appellant SACCO. The Respondent instructed the Appellant to stop sending the communication, but the Appellant continued to do so.
4. The Appellant, however, stated that they addressed the concerns of the Respondent vide their letter dated 18.11.2024, that it was discovered that the mobile phone number was initially allocated to one of its members to whom the messages were thought to be sent. The said mobile number had been transferred to the Respondent without the Appellant's knowledge, and when the Appellant learned of this, it stopped sending messages and ceased communication to the said number.

5. The Commission considered the complaint and, in its finding, ordered the Appellant to pay compensation of Ksh. 250,000/= as damages, thereby allowing the Respondent's claim. The Appellant was aggrieved with the determination, hence this appeal.

Submissions

6. The Appellant filed submissions dated 1.12.2025. It was submitted that the Respondent was not correctly classified as a subject in respect of mobile number 0721400416, which had been deactivated and given to a third party. Reliance was placed on Section 2 of the Data Protection Act.

7. It was also submitted for the Appellant that the Appellant did not violate the Respondent's right to privacy as data was processed in reference to the Appellant's customer, one Zipporah Wanjku Mathenge and so was acting through legitimate business interest. Reliance was placed on **Republic v Joe Mucheru & Others v Katiba Institute 7 Another (2021) KEHC 122** to submit that a complainant who was not a data subject could not initiate a complaint.

8. The Respondent also filed submissions dated 18.12.2025. It was submitted that the Appellant did not ensure that the data was accurate before sending to the Respondent. He cited Section 25(f), 26 and 35 of the Data Protection Act.

9. The Respondent submitted that the Appellant undertook to stop the messages, but instead continued to send the message alerts. The Respondent was, as such, a data subject under Section 2 of the Data Protection Act.

10. The Respondent submitted that he had satisfied his burden of proof under Section 107 of the Evidence Act. Reliance was placed on the case of **Hellen Wangari Wangechi v Carumera Muthoni Gathua [2015] KEHC 1758 (KLR)**, where the Judge held as follows:

> **It is a well-established rule of evidence that whoever asserts a fact is under an obligation to prove it in order to succeed.**

11. They submitted that the appeal should be dismissed with costs.

Analysis

12. This appeal emanates from Section 64 of the Data Protection Act, which grants jurisdiction to this Court as follows:

> *A person against whom any administrative action is taken by the Data Commissioner, including in enforcement and penalty notices, may appeal to the High Court.*

13. This being a first appeal, this court is under a duty to re-evaluate and assess the evidence and make its own conclusions. It must, however, keep at the back of its mind

that a trial court, unlike the appellate court, had the advantage of observing the demeanour of the witnesses and hearing their evidence first hand. In the case of *Mbogo and Another vs. Shah [1968] EA 93* the Court stated:

> *"…that this Court will not interfere with the exercise of judicial discretion by an inferior court unless it is satisfied that its decision is clearly wrong, because it has misdirected itself or because it has acted on matters on which is should not have acted or because it failed to take into consideration matters which it should have taken into consideration and in doing so arrived at a wrong conclusion."*

14. The duty of the first appellate court was discussed by Clement De Lestang, VP, Duffus and Law JJA, in the locus classicus case of **Selle and another Vs Associated Motor Board Company and Others [1968]EA 123,** where the Judges in their usual gusto, held by as follows:

> ".. this court is not bound necessarily to accept the findings of fact by the court below. An appeal to this court ... is by way of re-trial and the Court of Appeal is not bound to follow the trial Court's finding of fact if it appears either that he failed to take account of particular circumstances or probabilities or if the impression of demeanour of

> a witness is inconsistent with the evidence generally."

15. The Court is to bear in mind that it had neither seen nor heard the witnesses. It is the trial court that has observed the demeanor and truthfulness of those witnesses. However, documents still speak for themselves. The observation of documents is the same as the lower court as parties cannot read into those documents matters extrinsic to them. In the case of **Peters vs Sunday Post Limited** [1958] EA 424, court therein rendered itself as follows:-

> "It is a strong thing for an appellate court to differ from the findings on a question of fact, of the judge who had the advantage of seeing and hearing the witnesses...But the jurisdiction to review the evidence should be exercised with caution: it is not enough that the appellate court might have come to a different conclusion..."

16. On the issue as to whether the Office of the Data Protection Commissioner (the Commissioner) correctly found the Appellant liable for violating the Respondent's right to privacy under Article 31 of the Constitution and the Data Protection Act, 2019. The Appellant contended that the information was sent to the Respondent which was genuinely meant to be sent to its member, one ZWM who was the operator of the subject mobile phone number before it was deactivated and given to the Respondent, by the service provider.

17. However, the Respondent maintained that even after bringing it to the attention of the Appellant that it was the Respondent operating the subject mobile phone number, the Appellant continued to send the message alerts to the Respondent.

18. The Appellant’s evidence before the tribunal was that the Appellant stopped sending the messages on 31.10.2024, having established the mobile number had since changed and was used by the Respondent as opposed to the named Appellant’s member who used it before.

19. However, the Respondent produced the message alert of 19.12.2024, which was to the effect that the Appellant sent alerts after discovering that the mobile phone number was used by the Respondent, who was never at any time a member of the Appellant. The messages were not meant for the respondent. They were not messages meant for the Respondent. They are not unsolicited messages. These were messages, meant for the appellant’s contracted customer, who agreed to receive alerts for credits and debits. The alerts were personal to the data subject, that is, ZWM. What was being sent was not an alarm to the appellant. The mobile number is personal to ZWM. Her contact is in the appellant's banking contract.

20. Under Section 2 of the Data Protection Act, the Appellant is the data controller. However, there was no evidence that any of the Respondent's data was processed. Only ZWM's data was processed. The Appellant was not clearly privy to the deactivation and reactivation, as this was done by the service provider without involving the Appellant. Therefore, the Appellant required a reasonable time to establish such changes before concluding that indeed the line was no longer registered under its member.

21. Therefore, the Commissioner erred in not finding that the period of about one month that the Appellant used to establish the changes in registration of the subject mobile number was reasonable, and the Appellant was not bound to stop immediately without verifying such changes.

22. This matter brings out difficulties in knowing the limits of protection. The appellant is a data depository for a customer who is the owner of the impugned number. There is thus an identifiable natural person who owns the number in question, along with the full gamut of associated services. According to the appellant, the number is linked to a bank account owned by its customer. Unknown to them, the customer left the bank-linked number to fall dormant and was replaced pursuant to regulation 17 of the Kenya Information & Communication (Registration of Telecommunication Service Subscribers)

Regulation Legal Notice 90 of 2025, which provides for deactivation. It states as follows:

> **'A telecommunications operator shall deactivate a telecommunications service—**
> **(a) Where telecommunications services to the subscriber have been suspended for a period of ninety days;**
> **(b) Upon request by a subscriber; or**
> **(c) Where the telecommunications operator or the Authority establishes that the subscriber has provided false information for registration.**

23. A phone number is personal data that is protected. In arriving at the same conclusion, Mugambi L. J, in the case of **Erastus Ngura Odhiambo & Dickson Mwangi Muenene V Attorney General & Commissioner General of Prisons** posited as follows:

> 61. On assignment of numbers, the Kenya Information and Communications (Numbering) Regulations under Regulation 9 states as follows:
>
> Where an application for communication numbers or addresses is submitted to the Commission, the Commission shall, after taking into account the National Communication Numbering and Address Plan and availability of the numbers and addresses, assign and issue a certificate of assignment together with the conditions attached to the use of the communication numbers the numbers required for the communication numbers or addresses, upon payment of the prescribed fee.

> 62. The Constitution does not expressly single out digital identity as a fundamental right. However, given the elaborate legislative registration scheme that connects SIM registration to the official personal identification records of the subscriber, the mobile number is for all purposes **a digital identifier** that record provides a 'means a person can be identified directly or indirectly'.
>
> 63. Further, as ably argued by the Petitioners in the undisputed contention. A registered phone number has now become the means for authentication and verification credentials for online transactions, where security codes such as OTPs are sent to authenticate transactions. The registered mobile number thus provides link to delicate '**personal data'** that qualifies for protection under the right to privacy under Article 31 of the Constitution.

24. On the other hand, an identifiable natural person is defined in Section 2 of the Data Protection Act, 2019,

> **Means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity;**

25. Further, Personal data is defined in Section 2 of the Data Protection Act, 2019, to mean any information relating to an identified or identifiable natural person.

26. Finally, personal data breach of the Data Protection Act, 2019 provides as follows:

> "*Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;*

27. There was no accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored of the Respondent's data.

28. The appellant's case is that the specific phone number belongs to its customer. It had a duty to protect the number and related data. It received information from the respondent, who is a stranger to the bank-customer relationship, to cease sending messages to the number. It stopped, but a message was sent again in December. The information was unrelated and did not concern the Respondent. It related to the former owner of the phone number, ZWM. The question before me is whether the commissioner was right to find the applicant in breach of data privacy.

29. The first question the commissioner for data protection must consider is whether it is the appellant who sought the

number and breached privacy. In this case, that is not the case. As part of the know-your-customer requirement, a number is a prerequisite for banking. In the online banking era, data, including tax data, is linked to a phone number. For example, the Kenya Revenue Authority's personal identification number is linked to a number for each taxpayer. The one-time password is sent to this number. It is not related to the registration.

30. Secondly, banking fraud is a reality. The banks and Sacco Societies have to verify instructions from specific numbers. The appellant faces two consequences: first, if it alters banking information without informing the customer, it will constitute a personal data breach, as it will alter personal data, in this case, that of ZWM. It will also mean that the customer will be removed from online banking and alerts without instructions.

31. The appellant will be in a cul-de-sac. Therefore, there is a need to verify. However, verification cannot be done using the same phone number. This will therefore involve the bank going out of its way to deal expediently with such requests. Requiring instant removal is unrealistic. The commissioner failed to appreciate that, although now claiming ownership, the number is still an identifiable natural person, in the name of ZWM.

32. The respondent will continue to receive many more requests from all creditors of the customer, ZWM. This will include being added to extended-family WhatsApp groups and other groups the customer was in. This cannot be considered a breach of personal data. The respondent needed an unburdened number from a service provider. The data commissioner placed an insurmountable and usurious burden on the data controllers and processors.

33. It must be remembered that Data Protection Act is an Act of Parliament to give effect to Article 31(c) and (d) of the Constitution; to establish the Office of the Data Protection Commissioner; to make provision for the regulation of the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors; and for connected purposes. The rights of the data subjects set out in section 26 of the Act are:

a. to be informed of the use to which their personal data is to be put;
b. to access their personal data in custody of data controller or data processor;
c. to object to the processing of all or part of their personal data;
d. to correction of false or misleading data; and
e. to deletion of false or misleading data about them.

34. None of the rights under section 26 of the Data Protection Act was breached. Where the commissioner of data protection must protect data, is where personal data is released or accessed by a third party, who then sends messages. It cannot apply where the number is already burdened and linked to service providers. There was nothing to delete as no data related to the Respondent was released.

35. The Respondent can only go back to his service provider on how to opt out of burdens that belong to other individual owners. What the commissioner did was to re-write a contract between the appellant and ZWM. In the case of **National Bank of Kenya Ltd v Pipeplastic Samkolit (K) Ltd & another** [2001] KECA 362 (KLR) [Tunoi, Shah & Keiwua JJ A] held as follows: -

> A Court of law cannot re-write a contract between the parties. The parties are bound by the terms of their contract, unless coercion, fraud or undue influence are pleaded and proved. There was not the remotest suggestion of coercion, fraud or undue influence in regard to the terms of the charge.
>
> As was stated by Shah JA in the case of *Fina Bank Limited vs Spares & Industries Limited* (Civil Appeal No 51 of 2000) (unreported):
>
> "It is clear beyond peradventure that save for those special cases where equity might be prepared to relieve a party from a bad bargain, it is ordinarily no part of equity's function to allow a party to escape from a bad bargain.

36. By requiring the appellant to breach a contract with ZWM, the commissioner of data protection was breaching both the rights of ZWM and banking regulations and anti-money laundering regulations. Indeed the principles of data protection are set out in Section 25 of the Data Protection Act as follows:

> Every data controller or data processor shall ensure that personal data is
>
> a. processed in accordance with the right to privacy of the data subject;
> b. processed lawfully, fairly and in a transparent manner in relation to any data subject;
> c. collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
> d. adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
> e. collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
> f. accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
> g. kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
> h. not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

37. The principles require reasonable steps to be taken to ensure accuracy of the information related to ZWM's banking. Further, under section 40 of the Act, a data subject may request a data controller or data processor:

a. to rectify without undue delay personal data in its possession or under its control that is inaccurate, out-dated, incomplete or misleading; or

b. to erase or destroy without undue delay personal data that the data controller or data processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

2. Where the data controller has shared the personal data with a third party for processing purposes, the data controller or data processor shall take all reasonable steps to inform third parties processing such data, that the data subject has requested

a)the rectification of such personal data in their possession or under their control that is inaccurate, out-dated, incomplete or misleading; or

(b)the erasure or destruction of such personal data that the data controller is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

(3)Where a data controller or data processor is required to rectify or erase personal data under subsection (1), but the personal data is required for the purposes of evidence, the data controller or data processor shall, instead of erasing or rectifying,

restrict its processing and inform the data subject within a reasonable time.

38. It is true that false and misleading information must be deleted. However, this was not false or misleading information. This was current information required by the appellant and the account owner. The appellant had a duty to verify and inform the other data subject whose number had been deactivated that it had been given away. There was no direct evidence from the respondent that the number was his. There are no mechanisms for verifying numbers, other than through a court order. There is no data sharing agreement between data controllers and mobile service providers.

39. I therefore find that the appellant is entitled to take a reasonable time to ascertain from the other data subject that the number has changed ownership. A period of three months is, in the circumstances, not too long. There is no maximum statutory period within which a bank may verify information from its customer. For the purposes of ease of doing business, the Data Protection Act should not be used as a cash cow. It will encourage parties to replace idle numbers and then sue. Data processors will collapse.

40. The circumstances are different from a scenario where data is stolen and used to harass customers. This used to happen in the olden days, when bankers sent documents to the last

known address. Sending messages to the last known user of the phone number is not a breach of personal data.

41. This explains why the court in **Erastus Ngura Odhiambo & Dickson Mwangi Muenene V Attorney General & Commissioner General of Prisons**(Supra), held as follows regarding personal numbers:

> 71. Though deactivation is provided after a prolonged period of non-use or inactivity, specifically 90 days, the regulations are silent on how the reassignment or recycling of the deactivated telephone number is undertaken. It is left to the unregulated discretion of the Network Providers. Further, the deactivation of the registered telephone numbers for non-use is done without any regard as whether there exists any reasonable justification for the non-use. It does not give the subscriber the opportunity to explain or retain the digital identity once the 90 days of non-use have been confirmed, yet the registered phone number as a digital identifier, already provides vital link to delicate personal data. The provision is so mechanical that it fails to appreciate that a non-use may in fact be justified, like in the case of prisoners serving a sentence as in the instant case. A person may also have left the country for treatment in a country that does not have 'roaming services.' A student in a boarding school where the use of phones is prohibited could similarly suffer the same fate.

42. I agree with my brother that, though the number may have been deactivated, there are no regulations on delinking or transferring services linked to the mobile phone number. This calls for legislative intervention; the banking services will be brought to a halt by the mechanical application of Regulation 17 of the Kenya Information & Communication (Registration of Telecommunication Service Subscribers) Regulation Legal Notice 90 of 2025.

43. What then is the way forward? The appellant has a duty to contact the client and ascertain whether the person now using his or her number has fraudulently obtained it. Secondly, the new subscriber may have to contend with inconveniences associated with services linked to the number. Failing to delete the information promptly is not a breach of data protection.

44. The Data Commissioner, therefore, erred in punishing the appellant for endeavoring to verify data. Having found that the Appellant was not liable, I set aside the damages awarded as they were not justified. The appeal succeeds.

45. This leaves the issue of costs, which is governed by Section 27 of the Civil Procedure Act, which provides as follows:

> **(1) Subject to such conditions and limitations as may be prescribed, and to the provisions of any law for the time being in force, the costs**

of and incidental to all suits shall be in the discretion of the court or judge, and the court or judge shall have full power to determine by whom and out of what property and to what extent such costs are to be paid, and to give all necessary directions for the purposes aforesaid; and the fact that the court or judge has no jurisdiction to try the suit shall be no bar to the exercise of those powers: Provided that the costs of any action, cause or other matter or issue shall follow the event unless the court or judge shall for good reason otherwise order.

(2) The court or judge may give interest on costs at any rate not exceeding fourteen per cent per annum, and such interest shall be added to the costs and shall be recoverable as such.

46. Costs are generally discretionary. However, the discretion is not arbitrary. The Court of Appeal in the case of **Farah Awad Gullet v CMC Motors Group Limited [2018] KECA 158 (KLR)** had this to say:

> **It is our finding that the position in law is that costs are at the discretion of the court seized up of the matter with the usual caveat being that such discretion should be exercised judiciously meaning without caprice or whim and on sound reasoning secondly that a court can only withhold costs either partially or wholly from a successful party for good cause to be shown.**

47. The Supreme Court set forth guiding principles applicable in the exercise of that discretion in the case of **Rai & 3 others v Rai & 4 others [2014] KESC 31 (KLR),** as follows:

> 18.It emerges that the award of costs would normally be guided by the principle that "costs follow the event": the effect being that the party who calls forth the event by instituting suit, will bear the costs if the suit fails; but if this party shows legitimate occasion, by successful suit, then the defendant or respondent will bear the costs. However, the vital factor in setting the preference, is the judiciously-exercised discretion of the Court, accommodating the special circumstances of the case, while being guided by ends of justice. The claims of the public interest will be a relevant factor, in the exercise of such discretion, as will also be the motivations and conduct of the parties, prior-to, during, and subsequent-to the actual process of litigation
>
> 22. Although there is eminent good sense in the basic rule of costs - that costs follow the event- it is not an invariable rule and, indeed, the ultimate factor on award or non-award of costs is the judicial discretion. It follows, therefore, that costs do not, in law, constitute an unchanging consequence of legal proceedings - a position well illustrated by the considered opinions of this Court in other cases. The relevant question in this particular matter must be, whether or not the circumstances merit an award of costs to the Applicant.

Determination

48. In the upshot, I make the following orders:

a) The appeal is merited and is accordingly allowed.

b) The Decision of the Data Protection Commissioner delivered on 3.1.2025 in ODPC No. 1779 of 2024 is set aside. In lieu thereof, the complaint is dismissed.

c) The Appellant shall have costs of Ksh. 55,000/=.

d) 30 days stay of execution.

DELIVERED, DATED and **SIGNED** at **NYERI** on this **15th** day of **April, 2026.** Judgment delivered through Microsoft Teams Online Platform.

KIZITO MAGARE

JUDGE

In the presence of:-

Wachira Muturi for the Appellant

Mr. Odongo for the Respondent

Court Assistant – Michael/Martin