REPUBLIC OF KENYA

**OFFICE OF THE DATA PROTECTION COMMISSIONER**

**ODPC COMPLAINT NO. 0658 OF 2025**

**IMMACULATE NDUNGE KINYUNGU.....COMPLAINANT**

**-VERSUS-**

**KENYA WOMEN MICROFINANCE BANK.....RESPONDENT**

**DETERMINATION**

*(Pursuant to Section 8(1)(f) and 56 of the Data Protection Act, 2019 and Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021)*

## A. INTRODUCTION

1. The Complainant lodged a complaint against the Respondent, alleging that a loan was irregularly applied for and linked to her payslip without her knowledge, consent, or any prior relationship with the Respondent.

## B. LEGAL BASIS

2. Article 31(c) and (d) of the Constitution of Kenya provides for the right to privacy. Consequently, as an effort to further guarantee the same, the Data Protection Act, 2019 (hereinafter known as 'the Act') was enacted.
3. The Office of the Data Protection Commissioner (hereinafter as 'this Office' and/or 'the Office') was established pursuant to Section 5 of the Act and is mandated with the responsibility of regulating the processing of personal data; ensuring that the processing of personal data of a data subject is guided by the principles set out in Section 25 of the Act; protecting the privacy of individuals; establishing the legal and institutional mechanism to protect personal data and providing data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act.

4. Section 8(1)(f) of the Act provides that the Office can receive and investigate any complaint by any person on infringements of the rights under the Act. Furthermore, Section 56(1) of the Act provides that a data subject who is aggrieved by a decision of any person under the Act may lodge a complaint with the Data Commissioner in accordance with the Act.

5. This determination is premised on the provisions of Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 (hereinafter as 'the Enforcement Regulations'), which states that the Data Commissioner shall, upon the conclusion of the investigations, make a determination based on the findings of the investigations.

## C. BACKGROUND OF THE COMPLAINT

6. This Office received a complaint from the Complainant on 8th May 2025. The complaint was lodged pursuant to Section 56 of the Act and Regulation 4 of the Enforcement Regulations by the Complainant, who was an aggrieved data subject.

7. Pursuant to Regulation 11 of the Enforcement Regulations, the Office notified the Respondents of the complaint filed against them *vide* a letter dated 11th June 2025 and referenced ODPC/CIE/CON/2/1 (360). In the Notification of the Complaint, the Respondents were informed that if the allegations by the Complainant were true, they were in violation of various provisions of the Act. Further, the Respondents were asked to provide this Office with the following:

    a. A response to the allegations made against you by the Complainant;

    b. Any relevant materials or evidence in support for your response above,

    c. How you obtained the Complainant's personal data,

    d. The legal basis relied upon to use the Complainant's employment data to process a loan.

    e. The application forms that were used to secure the loan

    f. Whether the Complainant was notified, and whether she consented to loan application,

g. The mitigation measures adopted or being adopted to address the Complaint to the satisfaction of the Complainant, if any

h. The mitigation measures adopted or being adopted to ensure that such occurrence mentioned in the complaint does not take place again; and

i. Any other relevant information they wish the Office to consider.

8. The Respondent submitted a response to the allegation vide a letter dated 18th June 2025.

9. This determination is therefore as a result of analysis of the complaint as received and investigations conducted by the Office.

## D. NATURE OF THE COMPLAINT

10. This complaint concerns the unauthorized application and attachment of a loan to the Complainant's payslip. The Complainant alleges that the said loan was applied for and processed without her knowledge or consent, and despite having no prior relationship with the Respondent. She only became aware of the issue upon noticing unexplained deductions on her payslip, prompting her to seek clarification from the relevant authorities, which confirmed the existence of the loan in her name.

## E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

### i. THE COMPLAINANT'S CASE

11. The Complainant avers that in or about November 2022, a loan amounting to KES 1,368,500 was irregularly applied for and subsequently attached to her payslip by the Respondent, without her knowledge, consent, or prior engagement with the institution. She contends that the said action resulted in unauthorized deductions from her salary, beginning with a sum of KES 11,500.

12. Following the discovery of the said deductions, the Complainant purports to have visited the Respondent's offices to make inquiries regarding the origin of the loan, the process through which it was applied for, and the source of her personal data. However, despite these efforts, the Respondent failed or refused to furnish any meaningful explanation, merely stating that she did not have an account with them.

13. Moreover, the Complainant further avers that upon requesting to be informed of the purported guarantors of the said loan—information that could have shed light on who may have been in possession of her personal documents—the Respondent declined to check or disclose the same from their system, thereby frustrating her attempts to trace the source of the alleged fraud.

### ii. THE RESPONDENTS' RESPONSE

14. The Respondent avers that following internal investigations, it was established that the Complainant's personal data had, indeed, been unlawfully accessed and misused in the processing of a fraudulent loan application. The Respondent contends that the breach was allegedly orchestrated by a rogue staff member working in collusion with a colleague of the Complainant within the National Police Service, who is suspected to have facilitated unauthorized access to the Complainant's personal information.
15. The Respondent further purports that upon detecting the suspicious activity, it took immediate and corrective action. These included halting any further processing of the impugned loan, reversing all related loan transactions to eliminate any financial liability, and refunding the sum of KES 11,500 that had already been deducted from the Complainant's payslip. Additionally, a stop order was issued to prevent further deductions, and the Complainant's bank account was closed to avoid any continued exposure to risk.
16. Moreover, the Respondent states that it initiated an internal audit with the objective of tracing the source of the fraudulent activity and to establish whether similar breaches had occurred in other branches. It notes that this audit formed part of a broader strategy aimed at strengthening internal processes and accountability mechanisms.
17. In conclusion, the Respondent expresses regret over the incident and reaffirms its commitment to the principles of data protection as outlined in the Data Protection Act, 2019. It further states that it is undertaking ongoing efforts to enhance internal controls, improve staff training, and tighten access restrictions across its systems, with a view to preventing recurrence of similar incidents.

### iii. COMPLAINANT'S REJOINDER

18. The Complainant submitted an additional response through a letter dated 24th July 2025, in which she states as follows:

19. That The Complainant, in response to the Respondent's submissions, contends that the allegations therein are not only misleading but also devoid of material truth. She avers that the process of obtaining a loan through the National Police Service payroll is governed by an elaborate and stringent protocol, which, in her case, was never followed.

20. She states that, as a serving police officer, she is well aware of the procedural requirements for accessing credit facilities through payroll. The process requires the officer to physically present herself at the financial institution's banking hall, open a bank account (where one does not exist), and submit a duly completed loan application form. In addition, the officer must provide extensive and sensitive personal data, including but not limited to: a copy of the National Identity Card, Kenya Revenue Authority (KRA) PIN, biometric data such as passport-sized photographs, mobile phone number, bank account details, payslip (which is only accessible with a password), marital status, next of kin information, and her signature.

21. The Complainant further notes that the process mandates the submission of at least two guarantors, who must also be serving police officers stationed at the same workplace, and who are similarly required to appear physically and provide sensitive personal information. The final stage involves a mandatory visit by the bank's loan officer to the officer's place of work, where written confirmation and approval from the Officer Commanding Station (OCS) or immediate supervisor must be obtained before any disbursement.

22. However, the Complainant avers that she was never approached, never submitted any application, nor was she notified or involved in any step of the loan application process. She states that she was shocked to discover in November 2022 that her salary had been subjected to deductions in repayment of a loan she had neither applied for nor authorized. Upon realizing the irregular deductions, she promptly initiated personal efforts to uncover the source of the

alleged loan and to understand how her personal data may have been accessed and used without her consent.

23. Despite her efforts, she contends that the Respondent failed to provide adequate information regarding the identity of the individuals involved in the loan processing, and repeatedly denied her access to crucial records, contrary to her rights under Section 26 of the Data Protection Act. She maintains that the Respondent's refusal to disclose the details of the impugned transaction severely hampered her ability to trace and pursue the perpetrators of the identity fraud.
24. She avers that she was denied even the right to access the banking hall and one of the tellers was sent to refund her the amount deducted in cash. Additionally, she asserts that indeed the Respondent during the arbitration admitted the fact that someone impersonated the Complainant and duped the Respondent, but however it was noteworthy that they took immediate remedial actions after it became aware of the breach.
25. Moreover, the Complainant avers that the response from the Respondent raises many questions such as why the Respondent is unwilling to reveal the true identity of the impersonator? And yet it had CCTV cameras within its premises? What will stop the impersonator from using the Complainants personal information to commit more atrocious crimes against the Complainant etc.
26. She further avers that, by processing her personal data without her knowledge, consent, or involvement and in the absence of the required supervisory confirmations the Respondent not only breached the data protection principles under Section 25 of the Act, but also facilitated an act of identity fraud. She contends that the Respondent's failure to detect the irregularities or subject the application to proper scrutiny is indicative of gross negligence and a failure of institutional safeguards.
27. Consequently, the Complainant argues that she suffered reputational harm, emotional distress, and financial loss, and thus seeks redress. She prays that the Office imposes appropriate administrative sanctions under Section 63 of the Act and awards her compensation under Section 65, broken down as follows:

i. KES 2,000,000 for violation of her right to privacy under Article 31(c) of the Constitution;
ii. KES 1,000,000 in general damages for negligence;
iii. KES 500,000 in exemplary damages for stress, trauma and emotional suffering; and
iv. KES 500,000 for legal and incidental costs

## F. ISSUES FOR DETERMINATION

28. In light of the above, the following issues fall for determination by this Office:
    i. Whether there was a violation of the Complainant's rights under the Act and attendant regulations.
    ii. Whether the Respondent fulfilled its obligation under the Act.
    iii. Whether the Complainant is entitled to any remedies under the Act and the attendant Regulations.

## I. WHETHER THERE WAS A VIOLATION OF THE COMPLAIANT'S RIGHT UNDER THE ACT.

29. Section 26(a) of the Data Protection Act, 2019 grants every data subject the right to be informed of the use to which their personal data is to be put. This provision places a proactive duty on data controllers to ensure transparency and clarity in their data handling practices, especially at the point of collection or processing.
30. In the present case, the Complainant maintains that she was unaware of the loan application and had never authorized the use of her personal data for that purpose. She avers that she did not have any prior relationship with the Respondent and only became aware of the transaction after detecting an unexplained deduction from her payslip.
31. Investigations later revealed that an individual had impersonated the Complainant and used a fraudulently completed account opening form to facilitate the loan application. The Respondent, in its response, admitted that the Complainant's data had been unlawfully accessed by one of its staff members, allegedly acting in collusion with an officer of the National Police

Service. These facts reinforce the conclusion that the Complainant was neither notified nor involved in the use of her personal data—thereby breaching her right to be informed under Section 26(a).

32. That said, it is noteworthy that once the fraud was detected, the Respondent took a number of corrective actions: it halted further deductions, reversed the financial transactions, refunded the sum already deducted, and closed the account linked to the fraudulent loan. While these measures demonstrate a degree of responsiveness and willingness to mitigate harm, they were reactive rather than preventive, and do not negate the fact that the Complainant's data was used without her knowledge or consent.
33. Therefore, while the remedial steps taken by the Respondent are acknowledged and commendable, they do not cure the initial failure to inform the Complainant of the purpose for which her personal data was being used. That failure, which occurred at the point of collection and processing, constitutes a violation of Section 26(a) of the Act.
34. Section 26(b) of the Data Protection Act, 2019 grants every data subject the right to access their personal data in the custody of a data controller or data processor. This includes the right to request and receive details on:
    i. What personal data is being held,
    ii. How it was collected or processed,
    iii. The purpose for which it is being used, and
    iv. Any third parties with whom it has been shared.
35. In this case, the Complainant avers that upon discovering deductions from her payslip, she visited the Respondent's offices to seek clarity on the origin of the loan and how her personal information had been used. Despite these inquiries, the Respondent allegedly failed to provide any documentation or explanation on how her personal data was obtained and processed. This omission directly undermined her ability to understand the circumstances surrounding the unauthorized processing of her data.
36. The failure to facilitate timely and meaningful access to her personal data constitutes a breach of her statutory right. It deprived her of the opportunity to respond effectively to the misuse of her data and limited her ability to assess

and mitigate the impact of the breach. While the Respondent eventually took corrective measures including closure of the fraudulent account and refund of deductions these steps were only taken after the Complainant had experienced undue anxiety and financial inconvenience, which could have been minimized had access been granted at the initial stage.

37. This demonstrates non-compliance with Section 26(b), which requires a data controller to be transparent and responsive in facilitating access to personal data upon request by the data subject.
38. In view of the foregoing, the Respondent violated Section the Complainant's right to be informed and right of access under 26 (a) and (b) of the Act.

## II. WHETHER THE RESPONDENT FULFILLED ITS OBLIGATIONS UNDER THE ACT.

39. In addressing this issue, the Office will address the following question –
    a) Did the Respondent's processing of the Complainant's data comply with the principles outlined in the Act?
40. The Respondent, as a data controller or processor, was under a duty to ensure that the Complainant's personal data was handled in a manner that aligned with the core data protection principles set out in Section 25 of the Act. However, several key principles appear to have been violated:
41. Section 25(b) provides that every data controller or data processor shall ensure that personal data is processed lawfully, fairly and in a transparent manner in relation to any data subject;
42. In this case the processing of the Complainant's personal data namely, its use to apply for and process a loan was done without her knowledge, consent, or any form of notification. The Respondent admitted that the data was unlawfully accessed by a rogue staff member in collusion with an officer of the National Police Service. There was no transparency in how the data was obtained or used, and no lawful basis appears to have existed for the processing in the first place. As such, the Respondent failed to meet the standard of lawful, fair, and transparent processing required under the Act.

43. In addition to Section 25(f) imposes obligation on data controllers and processors to ensure that data collected is accurate and up to date. Investigations revealed that an account opening form was fraudulently filled by someone impersonating the Complainant. The use of impersonated or forged documents in the loan process, and failure to cross-check these against official employment records, indicates that the data used was not verified for accuracy. No steps appear to have been taken to authenticate the information or confirm the identity of the alleged applicant, thereby violating the requirement that personal data be accurate and kept up to date.
44. From the foregoing, it is evident that the Respondent did not fulfill its obligations under Section 25 (b) and (f) of the Data Protection Act. The processing of the Complainant's data lacked lawfulness, transparency, and no safeguards were in place to ensure accuracy and prevent misuse. These lapses collectively point to non-compliance with the core principles of data protection.
45. However, it's noteworthy that the investigations revealed that the Respondent undertook several remedial actions upon confirming the complaint. These included halting any further processing of the impugned loan, reversing all related transactions to eliminate financial liability on the part of the Complainant, and refunding a total of KES 11,500 that had already been deducted from her payslip. Furthermore, a stop order was promptly issued to prevent any additional deductions, and the Complainant's bank account opened fraudulently in her name was closed to eliminate any continued exposure to financial or reputational risk.

## III. WHETHER THE COMPLAINANT IS ENTITLED TO ANY REMEDIES UNDER THE ACT AND THE ATTENDANT REGULATIONS.

46. Pursuant to Regulation 14(2) of the Enforcement Regulations, a determination shall state the remedy to which the Complainant is entitled. Further, the remedies are provided for in Regulation 14(3) of the Enforcement Regulations.
47. The Complainant seeks compensation for the breach of her personal data
48. With regards to the award of compensation, Section 65 of the Act provides for compensation to data subjects and states, *"a person who suffers damage by*

*reason of a contravention of a requirement of the Act is entitled to compensation for that damage from the data controller."*

49. Section 65(4) of the Act states that, "*damage includes financial loss and damage not involving financial loss, including distress.*"

50. Further, Regulation 14(3)(e) provides that the Data Commissioner may make an order for compensation to the data subject by the Respondent.

51. Notably, in assessing the award for compensation, the Office takes into account the violation of the right to be informed under Section 26(a) and the right to access under section 26 (c).

52. In view of the foregoing, the Office hereby orders the Respondent to pay the Complainant **Kenya Shillings Five Hundred Thousand (KES. 500,000/=)** as compensation.

53. Having found that the Respondent failed to fulfill its obligations under the Act and attendant regulations, **an Enforcement Notice shall issue against the Respondent** pursuant to Section 58 of the Act and Regulation 16 of the Enforcement Regulations.

## G. FINAL DETERMINATION

54. The Data Commissioner therefore makes the following final determination:

i. The Respondent is hereby found liable.

ii. The Respondent is hereby **ordered to pay the Complainant Kenya Shillings Five Hundred thousand (KES 500,000/=)** as compensation;

iii. An Enforcement Notice to hereby be issued to the Respondent.

iv. Parties have the right to appeal this determination to the High Court of Kenya within thirty (30) days.

**DATED** at **NAIROBI** this 5th day of August 2025.

**IMMACULATE KASSAIT, MBS**
**DATA COMMISSIONER**