REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO.0105 OF 2025

MWIKALI NZYOKA..... .....COMPLAINANT

-VERSUS-

KENYA WOMEN MICROFINANCE BANK (KWFT).....1ST RESPONDENT

FAMILY BANK.....2ND RESPONDENT

CO-OPERATIVE BANK OF KENYA.....3RD RESPONDENT

DETERMINATION

Under 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 on 22nd January against the 1st Respondent alleging the 1st Respondent shared unauthorized personal information containing the Complainant's loan details to the 2nd and 3rd Respondents respectively without her consent or any lawful basis.

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 22nd January 2025. The complaint was lodged pursuant to Section 56 of the Act and Regulation 4 of the Enforcement Regulations by the Complainant, the aggrieved data subject.

7. Pursuant to Regulation 11 of the Enforcement Regulations, the Office, notified the Respondent of the complaint filed against it *vide* a letter dated 14th February 2025 and referenced ODPC/CIE/CON/2 /1 (008).

8. Pursuant to regulation 12 of the Enforcement Regulations, the Office ordered that Family Bank and Co-operative Bank to be enjoined as Respondents *vide* letters dated 14th February 2025 respectively.

9. In the Notification of the Complaint, the Respondents were informed that if the allegations by the Complainant were true, it was 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 it by the Complainant;

b. A contact person who can provide further details as regards the complaint.

c. Provide any relevant materials or evidence in support of your response.

d. The legal basis relied upon to process the complainant's personal data.

e. A confirmation whether the mentioned persons are your employees.

f. A data sharing agreement/data processing agreement between the Respondents

g. An elaborate representation of how data subjects can exercise their rights in relation to data protection.

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

i. Any other relevant information it wishes the Office to consider.

10. The 1st Respondent responded to the Notification of Complaint letter *vide* a letter dated 20th February 2025.

11. The 2nd Respondent responded to the allegations levelled against it via letter dated 10th March 2025.

12. The 3rd Respondent to the notification of the Complaint via two letters dated 10th March 2025 and 28th March 2025 respectively.

13. This determination is therefore a result of analysis of the complaint as received, the response by the Respondent and investigations conducted by the Office.

D. NATURE OF THE COMPLAINT

14. The nature of the complaint involves allegations that the 1st Respondent disclosed the Complainant's personal information to the 2nd and 3rd

Respondents without obtaining her consent or having a lawful basis for doing so.

E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

i. THE COMPLAINANT'S CASE

15. The Complainant contends that the 1st Respondent unlawfully disclosed her personal data to unauthorized third parties without her consent.

16. The Complainant avers that between mid-August and November 2024, the 1st Respondent leaked her sensitive personal information, including her loan status, identification details, place of work, and phone number to multiple financial institutions and their representatives.

17. The Complainant asserts that on September 7, 2024, she was contacted by an agent purportedly from 3rd Respondent, who claimed that the 1st Respondent was selling customer loans to banks.

18. The Complainant further states that on September 12, 2024, she received a call from another agent of the 3rd Respondent, who admitted that 1st Respondent had shared the Complainant's information.

19. The Complainant purports that between 17th to 23rd September, 2024, she received additional unsolicited calls from representatives of the 3rd Respondent and 3rd Respondent who confirmed they had obtained her data from 1st Respondent.

20. The Complainant avers that on 23rd September 2024, she was contacted by someone claiming to be the Branch Manager of the 1st Respondent regarding "a case on my data," which she declined to discuss.

21. The Complainant contends that on 7th and 14th November 2024, a representative from the 1st Respondent attempted to meet with her to apologize, attributing the breach to former employees who allegedly took data after termination.

22. The Complainant asserts that 1st Respondent explanation is unacceptable as the breach resulted from inadequate data protection measures within the organization.

23. The Complainant states that she continues to experience harassment, vulnerability, and frustration due to this unauthorized disclosure of her personal information.

24. Finally, the Complainant seeks to be informed of the full extent of the data leak and the remedial measures the 1st Respondent is implementing to prevent future occurrences.

25. In light of the above, the Complainant prays for the following remedies.

a) Conduct a formal investigation into the unauthorized disclosure of her personal data.

b) A formal written apology from the 1st Respondent for the unauthorized disclosure of my personal data and the emotional distress it has caused me.

c) Compensation as a remedy for the harm suffered.

ii. THE 1ST RESPONDENT'S RESPONSE

26. The 1st Respondent submitted a response to the notification of complaint in a letter dated 20th February 2025.

27. The 1st Respondent states that the Office conducted a site visit on 29th November 2024 to investigate their records, databases, and other relevant areas, during which all requested material was provided and all questions were answered.

28. The 1st Respondent contends that a follow-up letter was sent to the Office on 2nd December 2024 addressing concerns raised by the Complainant mentioning possible data sources from which the complainant's data could have been breached, data protection measures in place, and the loan buy-off context.

29. The 1st Respondent purports that their efforts to reach the Complainant as part of their investigations had been unsuccessful.

30. The 1st Respondent states that they have taken this complaint with the utmost seriousness, conducting an internal investigation which established that the data breach did not originate from their end.

31. The 1st Respondent avers that they attempted to reach out to the Complainant as part of their internal investigation, but she deliberately declined to respond, as she has acknowledged in her re-instituted complaint letter.

32. The 1st Respondent contends that they have been closely monitoring for similar complaints from other clients regarding a potential data breach, but none have been reported.

33. Additionally, the 1st Respondent purports that the Office should confirm without reasonable doubt that the data shared originated from the 1st Respondent, taking into consideration other data sources like the Credit Reference Bureau, possible data leak via her payslip, her data held by another financial institution, and other publicly available data.

34. The 1st Respondent states that in response to the most recent Notification dated 14th February 2025, they have procedures in place for data subjects to exercise their rights through Privacy Notice Awareness, multiple channels for submitting requests, and processes for request handling and resolution.

35. Additionally, the 1st Respondent contends that they remain committed to protecting the personal data of all their customers and will fully cooperate with the ODPC throughout the process.

III. THE 2ND RESPONDENT'S RESPONSE

36. The 2nd Respondent responded to the Notification of Complaint vide a letter dated 10th March 2025.

37. The 2nd Respondent avers that their data protection policy does not authorize unlawful processing of personal data and they are actively reviewing their internal records to determine if any such engagement took place.

38. The 2nd Respondent states that the screenshot provided as evidence does not conclusively demonstrate that the alleged contact was initiated on behalf of the Bank, particularly as the Complainant is not a customer.

39. The 2nd Respondent asserts that a review of the its records suggests that the agent who contacted the Complainant is associated with the it in an employment capacity.

40. The 2nd Respondent avers that there has been no data sharing nor any contract between 2nd Respondent and 1st Respondent, and as such, no data sharing agreement has been executed between the two entities.

41. The 2nd Respondent states that they fulfill the rights of data subjects through privacy notices, pre-collection information, policy accessibility, dedicated communication channels, and data subject request forms.

42. The 2nd Respondent contends that they provide mechanisms for data subjects to exercise their rights of access, rectification, erasure, restriction of processing, data portability, and objection through dedicated channels.

43. The 2nd Respondent purports that they have a dedicated data protection officer to assist with compliance, including data subject Requests, compliance, and training.

44. The 2nd Respondent asserts that they are conducting an internal review to establish all facts in the case and are proactively enhancing their data handling measures.

45. The 2nd Respondent avers that they are taking necessary steps to be compliant with the provisions of the Data Protection Act, including registration as Data Controllers and Data Processors, appointment of a Data Protection Officer, development of Data Protection Policies, establishment of a Data Privacy Centre, and implementation of technical measures to protect data.

iii. THE 3RD RESPONDENT'S RESPONSE

46. The 3rd Respondent responded to the notification of Complaint vide a letter dated 10th March 2025 and 28th March 2025 Respectively.

47. In the letter dated 10th March the 3rd Respondent avers the 3rd Respondent states that they remain resolute in their commitment to processing personal data lawfully while upholding data subjects' privacy rights.

48. The 3rd Respondent avers that they continuously enhance their technical and organizational measures to safeguard all categories of personal data, ensuring the highest standards of data privacy and protection.

49. The 3rd Respondent contends that they became aware of the complaint through the Office and conducted investigations with preliminary findings indicating that the complainant, is not a customer of the 3rd Respondent, and there is no contractual relationship between the 3rd Respondent and the Complainant.

50. The 3rd Respondent purports that they process individuals' personal data in accordance with the lawful bases outlined in Section 30 of the Kenyan Data Protection Act, and do not engage any third party without a data processing agreement or other legally binding arrangements.

51. The 3rd Respondent asserts that they do not have sufficient information to confirm that the said individuals are their employees and request additional details for clarity.

52. The 3rd Respondent states that they have established a customer rights management process to facilitate the exercise of data rights through multiple channels, including branch visits, call centre contact, email, and social media platforms.

53. The 3rd Respondent avers that they continuously conduct internal staff training to enhance awareness and advise employees to avoid third-party engagements that do not adhere to lawful bases for processing customer information.

54. The 3rd Respondent contends that in pursuing their legitimate interests, they leverage market intelligence to drive business growth and acknowledge that the matter arose from market intelligence indicating potential loan takeover from 1st Respondent, leading to the acquisition of the complainant's data and engagement with the complainant.

55. The 3rd Respondent purports that following a thorough internal review, they have addressed gaps related to the matter by implementing organizational measures including enhanced awareness and staff training, policies governing third-party

interaction, a robust customer rights management process, and a data breach incident response plan.

56. The 3rd Respondent asserts that the Complainant has not raised any reasonable cause of action against the it and has not sought any relief or compensation from the it, as the complaint filed with the Office is against 1st Respondent.

57. The 3rd Respondent states that the remedies flowing from the complaint do not attach to the it and cannot be enforced against the it, which is not a party to the proceedings, and the complaint does not demonstrate what prejudice the complainant will suffer should the 3rd Respondent not be joined in the complaint against 1st Respondent.

58. Further, in their letter dated 28th March 2025 the Respondent reiterates that they remain resolute in their commitment to processing personal data lawfully while upholding data subjects' privacy rights.

59. The 3rd Respondent avers that they recognize compliance is a continuous journey, and remain dedicated to consistently improving processes and practices to uphold data protection standards.

60. The 3rd Respondent contends that in pursuing legitimate interests, the bank leverages market intelligence to drive business growth and acknowledges that the matter arose from market intelligence indicating potential loan takeover from the 1st Respondent, consequently acquiring the complainant's data.

61. The 3rd Respondent purports that following a thorough internal review, they have addressed gaps related to the matter by implementing organizational measures including enhanced awareness and staff training, regular committee meetings, policies governing third-party interaction, robust customer rights management process, data breach incident response plan, enhanced customer complaint handling, staff sign-off process for data privacy, and periodic compliance checks.

62. The 3rd Respondent asserts that while cognizant of the provisions of Section 8(1)(c) of the DPA, the Complainant has not raised any reasonable cause of action against the 3rd Respondent and has not sought any relief or compensation from the Bank.

63. The 3rd Respondent states that the complaint filed against it at the Office is against the 1st Respondent.

64. The 3rd Respondent avers that from a thorough perusal of the complaint, it is evident that the Complainant has not raised any reasonable cause of action against the 3rd Respondent, and the remedies flowing from the complaint filed do not attach to the 3rd Respondent.

65. The 3rd Respondent contends that the complaint does not demonstrate what prejudice the Complainant will suffer should the 3rd Respondent not be joined in the complaint against the 1st Respondent.

66. The 3rd Respondent purports that the complaint is solely against the 1st Respondent as there is no contractual relationship between the 3rd Respondent and the Complainant, and the Bank's participation, if any, would be merely peripheral, not proximate.

67. The 3rd Respondent asserts that they humbly pray not to be joined in the complaint against the 1st Respondent.

68. The 3rd Respondent states that they wish to reiterate their commitment to full compliance with the DPA, 2019, and have taken significant measures to ensure that data processing activities align with legal and regulatory requirements.

69. The 1st Respondent and the 2nd Respondent, in letters dated February 20, 2025, and March 10, 2025 respectively, requested to resolve the complaint through Alternative Dispute Resolution (ADR), a request that this Office granted. However, as indicated in a letter dated March 20, 2025, the parties were unable to settle the matter amicably as anticipated

F. INVESTIGATIONS UNDERTAKEN

70. The Office examined the complaint lodged by the Complainant, evidence adduced in support thereof, the Respondent's written responses, and all documents submitted by both parties as evidence.

G. ISSUES FOR DETERMINATION

71. 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.

ii. Whether the Respondents' fulfilled their obligations under the Act; and

iii. Whether the Complainant is entitled to any remedies under the Act and the attendant Regulations.

I. WHETHER THERE WAS A VIOLATION OF THE COMPLAINANT'S RIGHTS UNDER THE ACT

72. Section 26(a) of the Data Protection Act recognizes the right of a data subject to be informed about the purposes for which their personal data will be processed. The 1st Respondent failed to inform the Complainant that it had the intention to sell its customer loans to third parties. This omission constitutes a violation of the Complainant's right to be informed.

73. Since the 2nd and 3rd Respondent did not have any contractual relationship with the Complainant, they cannot be held responsible for upholding of the said right.

74. Based on the foregoing, this Office finds that the 1st Respondent violated the Complainant's right to be informed as required under Section 26(a) of the Act.

II. WHETHER THE RESPONDENTS' FULFILLED THEIR OBLIGATIONS UNDER THE ACT

75. By addressing this issue, the Office will address the following questions –

a. Did the Respondents establish a lawful basis for processing the Complainant's personal data?

b. Was the Complainant's data lawfully processed?

a. Did the Respondents establish a lawful basis for processing the Complainant's personal data?

74. Section 25 (b) & 30 of the Data Protection Act, 2019 impose a statutory obligation to data controllers and processors to process personal data lawfully, transparently, and fairly. Lawful bases under Section 30 include consent, performance of a contract, compliance with a legal obligation, or pursuit of legitimate interest, among other. In this case, these requirements were not observed.

75. The Complainant, alleges that the 1st Respondent unlawfully disclosed her personal data to unauthorized third parties between mid-August and November 2024 which the 1st Respondent denied.
76. Moreover, the 1st Respondent apologized and attributed the personal data breach to former employee who allegedly accessed and processed data after termination.
77. The Complainant avers that she was subsequently contacted by representatives of the 2nd and 3rd Respondents, who referenced information that could only have been accessed through the 1st Respondent, thereby linking the alleged breach to the 1st Respondent.
78. The 2nd Respondent, while denying direct responsibility, acknowledges that an agent associated with their bank did contact the Complainant. However, they claim that no data sharing occurred between them and the 1st Respondent and that the Complainant is not their customer.
79. The 3rd Respondent admits that they acquired the Complainant's data through "market intelligence" for purposes of potential loan takeover from the 1st Respondent.
80. However, the 3rd Respondent's admission that they acquired the Complainant's data through "market intelligence" for purposes of loan takeover, without the Complainant's consent, constitutes strong evidence of unauthorized data processing.
81. The 3rd Respondent's admission constitutes a clear violation of the principles of data minimization and purpose limitation and underscores the lack of a lawful basis for processing. Their actions directly contravene the requirement under Section 30 that personal data must only be processed when a lawful basis exists, and must be done in a manner that upholds the data subject's rights.

82. In light of the above the office finds that 1st Respondent's claim that the data breach did not originate from their end is not justified. Additionally, the nature of the data obtained (loan status, identification details, phone number) would typically only be known to the financial institution holding the loan.
83. Furthermore, the 2nd Respondent's own acknowledgment that the individual who contacted the Complainant was an agent affiliated with their institution

corroborates the Complainant's claim that her personal data was shared without her consent or lawful basis.

84. While the 1st Respondent claims to have security measures in place, the evidence suggests these measures were insufficient to prevent unauthorized access to or disclosure of the Complainant's personal data. Effective security measures must ensure that even former employees cannot access or extract personal data post termination.

85. The Office finds that the 1st Respondent failed to adhere to its statutory obligations under Sections 25 and 30 of the Act. The lack of proper consent, absence of a valid legal basis for the disclosure, and failure to safeguard the Complainant's personal data, collectively amount to unlawful processing.

b. Was the Complainant's data lawfully processed?

86. Section 2 of the Act defines processing as *"any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means such as:- (a) collection, recording, organization, structuring; (b) storage, adaptation or alteration; (c) retrieval, consultation or use; (d) disclosure by transmission, dissemination, or otherwise making available; or (e) alignment or combination, restriction, erasure or destruction."*

87. From this definition, it is evident that indeed the 2nd and 3rd Respondent were processing the Complainant's personal data.

88. Section 30 (1) (a) of the Act provides that a data controller or data processor shall not process personal data unless the data subject consents to the processing for one or more specified purposes.

89. The Act goes further to state the conditions of consent. It states as follows with regard to the conditions of consent:-

32. Conditions of consent

(1) A data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose.

(2) Unless otherwise provided under this Act, a data subject shall have the right to withdraw consent at any time.

(3) the withdrawal of consent under sub-section(2) shall not affect the lawfulness of processing based on prior consent before its withdrawal.

(4) In determining whether consent was freely given, account shall be taken of whether, among others, the performance of a contract, including the provision of a service, is conditional on the consent of the processing of personal data that is not necessary for the performance of that contract. (emphasis ours)

90. From the evidence adduced to this Office, it is evident that at all material times when the 2nd and 3rd Respondent was handling the Complainants' personal data, it required the Complainants' consent or a lawful basis to process the Complainant's data

91. The 2nd Respondent, while denying direct responsibility, acknowledges that an agent associated with their bank did contact the Complainant.

92. The 3rd Respondent on the other hand admits that they acquired the Complainant's data through "market intelligence" for purposes of potential loan takeover from the 1st Respondent.

93. However, the 3rd Respondent's admission that they acquired the Complainant's data through "market intelligence" for purposes of loan takeover, without the Complainant's consent or a lawful basis, constitutes unauthorized data processing. This directly contradicts the lawful bases requirement under Section 30 of the Data Protection Act.

94. This Office, therefore, finds that as far as issue no **(b)** is concerned, the 2nd and 3rd Respondent processed the Complainant's personal data unlawfully.

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

95. Pursuant to Regulation 14 (2) of the Enforcement Regulations, a determination shall state the remedy to which the complainant is entitled. The remedies are provided for in Regulation 14 (3) of the Enforcement Regulations.

96. The Complainant requested this Office to issue an award of compensation. Section 65 of the Act provides that 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. The Section indicates that damage included financial loss and damage not involving financial loss including distress.

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

98. In considering whether to issue compensation, this Office takes into consideration the fact that the Complainant's rights and whether her personal data was unlawfully processed by the Respondents.

99. In this context, the 1st Respondent is hereby ordered to pay the Complainant **Kenya Shillings Two Hundred and Fifty Thousand (KES 250,000)** for the infringement of her rights under the Act.

100. The 2nd and 3rd Respondent to each pay the Complainant **Kenya Shillings Two Hundred Thousand (KES 200,000).**

101. Furthermore, an Enforcement Notice to issue against the 1st Respondent.

H. FINAL DETERMINATION

102. The Data Commissioner therefore makes the following final determination;

i. The Respondents are found liable.

ii. The Respondents to pay the Complainant a total sum of **Kenya Shillings Six Hundred and Fifty Thousand (KES 650,000)** as compensation as follows:

1st Respondent-Kenya Shillings Two Hundred and Fifty Thousand (KES 250,000)

2nd Respondent-Kenya Shillings Two Hundred Thousand (KES 200,000)

3rd Respondent-Kenya Shillings Two Hundred Thousand (KES 200,000)

iii. An enforcement notice to hereby be issued against the 1st Respondent.

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

DATED at **NAIROBI** this 21st day of April. 2025.

IMMACULATE KASSAIT, MBS
DATA COMMISSIONER