REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 1178 OF 2024

ROSE WAMBUI MUIGAI.....COMPLAINANT

-VERSUS-

NCBA BANK PLC.....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 alleges that the Respondent disclosed her personal data to third parties, who were the Respondent's former employees, without a 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 '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 (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 2nd August, 2024. The complaint was lodged pursuant to Section 56 of the Act and Regulation 4 of the Enforcement Regulations from the Complainant who was 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 27th August, 2024 referenced ODPC/CONF/1/5 VOL II (110). In the notification of the complaint, the Respondent was informed that if the Complainant's allegations were true, they would be in violation of various sections of the Act. Additionally, the Respondent was asked to provide this Office with the following:
   a) A response to the allegations made against them by the Complainant;
   b) A contact person who would provide further details regarding the complaint
   c) Any relevant materials or evidence in support of their response;
   d) The mitigation measures adopted or being adopted to address the complaint to the satisfaction of the Complainant,

e) The mitigation measures adopted or being adopted to ensure that such occurrence mentioned in the complaint does not recur.

f) Any other information they wished the Office to consider.

8. The parties attempted to resolve the complaint by way of alternative dispute resolution. However, on 7th October, 2024 the Office was informed that the mediation was unsuccessful.

9. This determination is therefore pursuant to the provisions of Regulation 15(8) of the Enforcement Regulations which provides that where the Complaint is not determined through negotiation, mediation or conciliation, the Data Commissioner shall proceed to determine the Complaint as provided for in the Act and the Regulations.

D. NATURE OF THE COMPLAINT

10. The Complainant alleged that on diverse dates between 20th May, 2023 and 28th May, 2024, the Respondent processed her personal data in violation of data protection laws. She alleges that former employees of the Respondent were using her personal data to contact her to assist her with renewal of her insurance cover.

E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

i. THE COMPLAINANTS' CASE

11. The Complainant holds a financial account with the Respondent which she opened on 31st May 2021.

12. On or about June 2021, the Complainant subscribed to one of the Respondent's services, wherein the Respondent provided financing for the Complainant to acquire a motor vehicle, as well as an additional facility for an annually renewable insurance premium.

13. That on 25th May, 2023 the Complainant states that she received a call from D**** M**** a third party, who disclosed information that included her full name, mobile phone number and her motor vehicle details, car registration number and additionally, the third party informed her that her motor vehicle insurance was due for renewal.

14. The Complainant received another call from 072*****80, wherein the person introduced himself as R**** M***, and an employee of the Respondent. This third party disclosed the Complainant's full name, mobile phone number and motor vehicle details and additionally informed her that the motor vehicle insurance was due for renewal and that he could assist with this.

15. On 20th May 2024, she received another call from the same person, R**** M***, who again disclosed the Complainant's personal data and further stated that since the Respondent's portal had an issue with access, he was requesting that the Complainant furnish him with a copy of her logbook so he may assist with the renewal of the motor vehicle insurance.

16. On 22nd May 2024, she received an email from the Respondent notifying her that her motor vehicle insurance was due for renewal on 28th May 2024.

17. The Complainant responded to the email dated 22nd May 2024 requesting the Respondent to proceed with the fulfillment of the vehicle motor insurance. The Complainant further notified the Respondent that she has received several phone calls from D****n M***u and R***t M**a as regards the status of her motor vehicle insurance and requested that the Respondent address and resolve the issue.

18. Around 23rd May 2024, she received another email from the Respondent notifying her that it had received all the required documents necessary for the renewal of her motor vehicle insurance cover and that the Respondent shall notify her once the renewal process is completed.

19. On 28th May 2024, the Complainant received an email from the Respondent notifying her motor vehicle insurance was due for renewal. The Complainant, in ordinary course of attempting to resolve the issue, discovered that D****n M***u and R***t M**a were neither employees nor agents of the Respondent. The Complainant further identified these third parties as former employees of the Respondent.

20. The Complainant, *via* a demand letter dated 23rd June 2023, notified the Respondent of the breach and violation of privacy and demanded that the Respondent take immediate action to remedy the breach.

21. The Respondent responded to the demand letter on 13th September 2023, and denied each and every allegation. The Complainant further alleges that the Respondent requested her to individually follow through with the issues directly with D****n M***u and R****t M**a.

22. The Complainant further avers that the violation in question pertains to the unauthorized disclosure and processing of her personal data without express consent or any other lawful basis.

23. As evidence, the Complainant adduced the following: -

i. Correspondence between herself and the third parties in issue;
ii. Text messages between herself and a third party in issue;
iii. Correspondence between herself and the Respondent; and
iv. The demand letter to the Respondent.

ii. THE RESPONDENT'S RESPONSE

24. *Vide* its response to the notification of complaint dated 25th September 2024, the Respondent averred that the Complainant is one of its customers and has held an active account registered on 31st May 2021.

25. The Respondent further averred that on or about June 2021, it received an application for a loan facility from the Complainant for purposes of purchasing a motor vehicle. The Respondent stated that the Complainant applied for an additional facility to cover her motor vehicle insurance and the same was to be renewable annually.

26. The Respondent asserts that it received several demand letters from the Complainant where the Complainant alleged that a former employee disclosed her personal data. They state that the demand letter demanded that the Respondent carry out investigations into the unauthorized disclosure of personal data, that the Respondent

acknowledge liability and that the Respondent compensate the Complainant for the violation of her right to privacy.

27. In the investigation report furnished by the Respondent, the Respondent highlights that indeed the third party identified as D****n M***u was its former employee who worked with the then NIC Bank in various roles between 2012 and 2021 including within the its Insurance Intermediary.

28. The Respondent state that upon termination of his contract, he was required to return all data or information to the Respondent with the assurance that no such articles or copies remain in his possession.

29. That upon termination of D****n M***u's employment in November 2021, the Respondent's states that its ICT department promptly disabled and revoked D****n M***u's access and credentials to internal systems.

30. The Respondent's investigation report further highlighted that R****t M**a, the second third party herein was also a former employee of the Respondent between the period of 2018 and 2021 within the Respondent's Insurance Intermediary.

31. That R****t M**a's contract was not renewed in February 2021 resulting in termination of his employment with the Respondent.

32. The Respondent states that it reached out to the identified third parties but they were non-committal to visiting the Respondent's Offices in a bid to aid in the investigations.

33. The Respondent further asserts that it sent cease and desist letters to the two third parties where it received the first response from D****n M**a who allegedly denied the allegation in toto while R****t M**a confirmed that he indeed contacted the Complainant about her renewal of her motor vehicle insurance premium, and he further informed her that he had ceased to be an employee of the Respondent. That the nature of conversation between himself and the Complainant was cordial and professional and the Complainant further extended her personal driver's contact information identified as (Mr. J****h).

34. The Respondent further provided that the second third party's (R****t M**a) response further claimed that the valuation and purchase of an insurance premium did not proceed as planned and there was subsequent communication breakdown. This then allegedly caused agitation with the Complainant and resulted in the complaint filed with the Office.

35. Additionally, the Respondent submits that in its investigations, a review of the emails sent to D****n M***u's email address, no conclusive evidence was found connecting D****n M***u and the staff members with access to the Complainant's logbook and insurance details.

36. The Respondent further states that it requested the Complainant to disclose the contact number from which the insurance renewal business originated, but she was in return hesitant to give any information.

37. The Respondent averred that from the foregoing and its internal investigations, it was unclear where the Complainant's details that were disclosed and shared originated from.

38. The Respondent denies liability in *toto* and further reiterates that the allegations of unauthorized access are unfounded and there lacks sufficient evidence to the same.

39. The Respondent pleaded that at all times it acted accordingly and did not occasion an infringement on the Complainant or any other applicant thereof.

40. As evidence, the Respondent adduced –

i) A statement of Response to the Notification of Complaint;
ii) Responses to the demand letters received from the Complainant;
iii) Correspondences between itself and the Complainant;
iv) Employment contracts and termination letters of the third parties identified as D****n M**u and R****t M**a;
v) Employee Separation clearance forms of the third parties identified as D****n M**u and R****t M**a;

vi) Cease and Desist demand letters to of the third parties identified as D****n M**u and R****t M**a;

vii) Responses to the Cease-and-Desist demand letters from the of the third parties identified as D****n M**u and R****t M**a; and

viii) Incident Investigation Report.

F. INVESTIGATIONS UNDERTAKEN

41. After careful analysis of the adduced evidence on record and the law, the Office established, that the Complainant indeed holds an account with the Respondent which was opened on 31st May 2021; a position verified and validated by the Respondent.

42. A review of the Respondent's supporting documents established and validated that one of the contacts identified as R****t M**a was its former employee and his contract of employment was terminated in February 2021. During this period, the Complainant had not yet become a customer of the Respondent.

43. In the same vein, a second person identified as D****n M***u, was also established to have been a former employee of the Respondent and whose contract of employment was terminated in November 2021.

44. In an analysis of the Complainant's submissions, the Respondent's response, supporting documentation, the Office established that the violation occurred between the years May 2023 and June 2024. During the period of violation, both of the persons identified herein as D****n M***u and R****t M**a had stopped working for and/or on behalf of the Respondent, and were therefore not handling the Complainant's personal data on behalf of the Respondent.

G. ISSUES FOR DETERMINATION

45. In light of the above, the complaint, the Respondent's responses and evidence adduced together with the investigations conducted, the following issues fall for determination by this Office:

i. Whether the Respondent fulfilled its obligations under the Act; and

ii. Whether the Complainant is entitled to remedies under the Act.

I. WHETHER THE COMPLAINANT FULFILLED ITS OBLIGATIONS UNDER THE ACT

46. Section 25(a) of the Act provides that every data controller or data processor shall ensure that personal data is processed in accordance with the right to privacy of the data subject.

47. The Complainant alleges that the Respondent without any lawful basis willfully disclosed and/or shared her personal data to third parties.

48. The Respondent rebutted the Complainant's allegations, stating that the persons whom the Complainant claims breached her privacy were not employees of the Respondent, and that they had ceased to be employees for several years. The Respondent attached the employment contracts and the letters of termination in its defense.

49. The investigations conducted by the Office and the analysis of the evidence on record conclusively established that the first violation occurred in the year 2023, followed by a second violation in 2024. The Respondent submitted that the individuals who contacted the Complainant and disclosed her personal data held by the Respondent had left the organization in February 2021 and November 2021, respectively.

50. It is therefore irrefutable that the third party individuals who contacted the Complainant, identified by the Respondent as former employees, had long ceased their employment with the Respondent. Consequently, based on the Respondent's submissions that these individuals no longer had access to the data maintained by the Respondent, the critical question of how they accessed the Complainant's personal data without valid credentials or access logs held by employees only remains un-addressed.

51. Section 41(1) of the Act provides that every data controller or data processor shall implement appropriate technical and organizational measures which are designed to implement the data protection principles in an effective manner; and to integrate necessary safeguards for that purpose into the processing.

52. Sub-section (4) further provides; to give effect to section 41(1), the data controller or data processor shall consider measures such as, to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control, to establish and maintain appropriate safeguards against the identified risks, to verify that the safeguards are effectively implemented and to ensure that the safeguards are continually updated in response to new risks or deficiencies.

53. Regulation 32 of the Data Protection (General) Regulations, 2021 set out the elements for principle of integrity, confidentiality and availability to include—

(a) having an operative means of managing policies and procedures for information security;

(b) assessing the risks against the security of personal data and putting in place measures to counter identified risks;

(c) processing that is robust to withstand changes, regulatory demands, incidents, and cyber-attacks;

(d) ensuring only authorised personnel have access to the data necessary for their processing tasks;

(e) securing transfers shall be secured against unauthorised access and changes;

(f) securing data storage from use, unauthorised access and alterations;

(g) keeping back-ups and logs to the extent necessary for information security;

(h) using audit trails and event monitoring as a routine security control;

(i) protecting sensitive personal data with adequate measures and, where possible, kept separate from the rest of the personal data;

(j) having in place routines and procedures to detect, handle, report, and learn from data breaches; and

(k) regularly reviewing and testing software to uncover vulnerabilities of the systems supporting the processing.

54. The individuals who contacted the Complainant and disclosed her personal data which was exclusively held and maintained by the Respondent, were not authorized representatives of the Respondent at the time of the disclosure. This conduct establishes a clear instance of a personal data breach where there was unlawful and unauthorized disclosure of the Complainant's personal data in the custody of the Respondent.

55. Further, Section 2 of the Act defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

56. Section 43(a) of the Act provides that where personal data has been accessed or acquired by an unauthorized person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach.

57. The Respondents did not report the personal data breach to this Office.

58. Based on the foregoing, with respect to issue **(i),** the Office finds that the Respondent failed or neglected to fulfil its obligations under Section 25(a) as read with Sections 41 and 43 of the Act.

II. WHETHER THE COMPLAINANT IS ENTITLED TO REMEDIES UNDER THE ACT

59. Regulation 14 of the Enforcement Regulations, provides that the Data Commissioner shall, upon the conclusion of the investigations, make a determination based on the findings of the investigations and a determination shall state inter-alia the remedy to which the complainant is entitled.

60. The Complainant sought various remedies, including monetary compensation, issuance of an enforcement notice to the Respondent, issuance of a penalty notice to the Respondent and prosecution of any other person found liable.

61. Section 65 (1) of the Act provides for compensation to a data subject and states 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. Section 65 (4) of the Act states that "damage" includes financial loss and damage not involving financial loss, including distress.

62. This Office takes into account the nature and extent of violation of the Act with regard to failure to process personal data in accordance with the right to privacy resulting in unlawful and unauthorized disclosure of the Complainant's personal data.

63. Having found that the Respondent did not process the Complainant's personal data in accordance with the right to privacy under Section 25(a) of the Act, the Respondent is hereby ordered to compensate the Complainant in the amount of **KES 250,000 (Kenya Shillings Two Hundred and Fifty Thousand).**

64. Section 58 of the Act as read together with Regulations 14 and 16 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 further contemplates, as a remedy, the issuance of enforcement notices against an entity that has failed or is failing to comply with any provisions of the Act and the attendant regulations thereto.

65. Having found that the Respondent did not fulfill its obligations provided for under the Act, the Office hereby orders for an enforcement notice to be issued against the Respondent.

H. FINAL DETERMINATION

66. In consideration of all the facts of the complaints, the evidence tendered and the investigations conducted, the Data Commissioner makes the following determination:

i. The Respondent is hereby found liable.

ii. The Respondent is hereby ordered to compensate the Complainant the amount of **KES 250,000 (Kenya Shillings Two Hundred and Fifty Thousand).**

iii. An Enforcement Notice is hereby issued to the Respondent herein.

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

DATED at **NAIROBI** this 30th day of October 2024

Immaculate Kassait, MBS
DATA COMMISSIONER