REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 1766 OF 2023

JOHN ONKANGI.....COMPLAINANT

-VERSUS-

NATIONAL BANK OF KENYA LIMITED.....1ST RESPONDENT

KEYSIAN AUCTIONEERS.....2ND RESPONDENT

DETERMINATION

(Pursuant to Section 8(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 Office received a complaint on the 26th September 2023, in accordance with Section 56 of the Act and Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 (the Regulations). The Complaint relates to the alleged disclosure of the Complainant's loan statement and consequently bank account details to a third party without his consent.

B. LEGAL BACKGROUND

2. The Constitution of Kenya 2010, under Article 31 (c) and (d) 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 (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 pegged on the provisions of Regulation 14 of the 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. NATURE OF THE COMPLAINT

6. The Complainant alleged that the 1st Respondent forwarded his bank account details and loan statement to a third party without his approval. He alleged that an employee of the 1st Respondent sent the details to the third party's email address. The statement was also sent to the third party by the 2nd Respondent.

D. BACKGROUND OF THE COMPLAINT

7. This Office received a complaint from the Complainant on 26th September 2023. The complaint was lodged pursuant to Section 56 of the Act and Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 (hereinafter the 'Enforcement Regulations') from the Complainant who is the aggrieved data subject.

8. National Bank of Kenya Limited (hereinafter the '1st Respondent') is a financial services provider whose primary role is to conduct deposit taking and lending business. Keysian Auctioneers (hereinafter the '2nd Respondent') is a debt collector contracted by the 1st Respondent for its services.

9. Pursuant to Regulation 11 of the Enforcement Regulations, the Office, notified the Respondents of the complaint filed against it *vide* a letter dated 16th October, 2023 referenced ODPC/CONF/1/5 VOL 1 (490). In the notification of the complaint, the Respondents were to provide: -

    a. A response to the allegations made against them by the Complainant;
    b. Any relevant materials or evidence in support of the response;
    c. The legal basis relied upon to share the Complainant's details as per Section 30 of the Act; and
    d. A demonstration of how the institutions balances the rights and freedoms of the data subject vis-à-vis their internal policies and procedures.

10. The 1st Respondent responded to the notification of complaint via a letter dated 30th October 2023. However, the 2nd Respondent failed to respond to these allegations.

11. This determination is therefore pegged on Regulation 11 (2) of the Enforcement Regulations whereby the Data Commissioner shall proceed to determine the complaint in accordance with the Act and the Regulations the non-response of the Respondent notwithstanding.

E. SUMMARY OF EVIDENCE ADDUCED

i. THE COMPLAINANTS' CASE

12. The Complainant submitted the filled complaint form and a screenshot of an email sent from an employee of the 1st Respondent to a third party indicating his outstanding loan balance and his loan statement and his customer account statement attached to the said email.

13. *Via* an email dated 9th October 2023, the Complainant stated that the 2nd Respondent called the third party and shared his account information with her without his consent.

14. The Complainant however did not prove his case against the 2nd Respondent by providing evidence that the 2nd Respondent actually shared his personal details with the third party without his consent.

ii. THE 1ST RESPONDENT'S RESPONSE

15. The 1st Respondent stated that the Complainant is a customer of the Bank and has a loan facility with the Bank which had defaulted due to non-payment.

16. The 1st Respondent confirmed that their staff member who works as a remedial analyst, and whose role is to support collections and recovery of debts owed to the Bank was pursuing the recovery of the Complainant's debt.

17. Further, the 1st Respondent indicated that it is in contract with the 2nd Respondent to provide auctioneering services to the Bank and support the recovery of debts owed to the Bank.

18. The 1st Respondent further attached the service contract dated 14th September 2017 between itself and the 2nd Respondent. Clause 6 of the contract provides for confidentiality and sub-clause 6.5 states that:

> *"The Firm shall not divulge any information with regard to the Bank's customers/clients accounts to any third party or use any material or information acquired by virtue of this or any other agreement."*

The "Firm" in this context means the 2nd Respondent.

Further, sub-clause 6.7 provides that the provisions of Clause 6 shall remain in full force and effect notwithstanding the termination of the Agreement.

18. The 1st Respondent observes that it has clear governance structures on the handling of customer data and that all its staff are bound by organisational policies to ensure that customer data is handled with the highest level of confidentiality and in observance with the right to privacy of individuals. The policies indicated include: data classification policy, staff confidentiality policy,

code of ethical conduct and data protection and privacy policy. The 1st Respondent provided these policies as proof of the same.

19. It is noteworthy that clause 4.2 of the 1st Respondent's Staff Confidentiality Policy provides for the definition of Breach of Confidentiality as:

> *"The disclosure of information, intentionally or unintentionally, to an individual or entity that is not entitled to or authorized to receive that information."*

20. Further, Clause 5.3 of the Policy states that:

> *"Employees shall keep confidential and shall not, during the continuance of their employment or any time after the termination thereof, without the express written consent of the Bank, disclose to any person or entity, information, records and data pertaining to the Bank, its customers, suppliers or partners which they may have acquired during the course of employment."*

21. The 1st Respondent indicated that the staff member shared the Complainant's Account Statements with the third party which he had access to in his ordinary course of work. However, the Bank indicated that the staff member acted against its Code of Ethical Conduct which constituted misconduct. The 1st Respondent stated that the staff member has a duty and obligation to protect customer data and not share it with third parties without the customer's consent.

22. The 1st Respondent stated that the staff member went against its policies in his own capacity while fully cognizant of the Bank's policies on handling customer's data and as such, it should not be held liable for the actions of the staff member as alleged by the Complainant.

23. The 1st Respondent indicated that it has an elaborate Staff Disciplinary Handling Policy and was conducting a full investigation into the matter and taking necessary steps and measures to address the matter in accordance with the Policy. The Bank however did not provide proof of the said investigations and actions taken against its staff member.

24. Further, the 1st Respondent stated that it has adopted the following mitigation measures to address the complaint:

    i. Conducted and scheduled further mandatory training for staff on privacy and data protection in order to create more emphasis on protecting customer personal information.

    ii. Requirement of staff to undertake mandatory privacy, data protection and cybersecurity assessments which emphasize on staff conduct in operation of bank processes.

    iii. Its HR department has been engaged on the matter to create further awareness on adherence of Bank policies.

    iv. Staff have been informed of the strict adherence to the Bank's policies in all their operations.

    v. The Bank has implemented a Data Protection and Privacy Policy which outlines the rights of data subjects and assurance that the Bank shall provide notice to data subjects before personal data is collected informing them of their rights, the Bank's policies, purpose of collecting personal data, usage, transfer, retention and disclosure as well as the contact of the data protection officer to enable data subjects exercise their rights.

25. With regards to the contract with the 2nd Respondent, the 1st Respondent stated that the information that was shared with them in respect of the Complainant's debt and to facilitate contact with the Complainant as per its service contract with them is the Complainant's bank account name, bank account number, account ID, national ID number, postal address, employer, the defaulted amount and the last date of payment.

26. The 1st Respondent further stated that its engagement with the 2nd Respondent is governed by a contract and the service provider has a duty and obligation to uphold confidentiality and not disclose the Bank's customers' data with third parties.

27. Regarding balancing the rights of the data subject against its internal policies and procedures, the 1st Respondent stated that it values the right to privacy of individuals and continuously upholds the same through its internal policies and procedures.

28. Moreover, the Respondent indicated that its staff are required to adhere to policies and procedures in their operations that observe privacy by; having and implementing a Data Protection and Privacy Policy, training of its staff, having a HR Code of Ethical Conduct and Staff Confidentiality Policies in place, having published a Privacy Notice, and appointing a data protection and privacy resource to oversee implementation of the Act, conducting third-party data privacy risk management and due diligence and putting in place technical security measures to protect personal data.

iii. THE 2ND RESPONDENT'S RESPONSE

29. The Office observes that the 2nd Respondent did not respond to the notification sent on 16th October 2023. Nonetheless, the Office notes that the Complainant did not present any proof to support his claim that the 2nd Respondent infringed on his personal data.

F. ISSUES FOR DETERMINATION

30. The following issues fall for determination by this Office:

i. Whether the 1st Respondent is vicariously liable for its employee's conduct 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 THE 1ST RESPONDENT IS VICARIOUSLY LIABLE FOR ITS EMPLOYEE'S CONDUCT UNDER THE ACT

31. This Office notes that the 1st Respondent did not dispute that there was a personal data breach by the staff member who sent the Complainant's details to a third party without his consent.

32. The 1st Respondent availed its Staff Confidentiality Policy which prohibits employees from sharing its customer's information without authorisation or consent from the customer.

33. The employee in question was a remedial analyst who supports collections and recovery of debts owed to the Bank. Therefore, in accessing the Complainant's details, the employee was in his ordinary course of duty.

34. The United Kingdom Supreme Court in ***WM Morrison Supermarkets PLC (appellant) v Various Claimants (Respondents) (2020) UKSC 12***, in deciding whether an employer is vicariously liable applied the test of whether there was a sufficiently close connection between the work and that the employee was authorised to do and the wrongdoing carried out, so that the wrongdoing could fairly be regarded as done by the employee while acting in the ordinary course of employment.

35. In this complaint, the employee being a remedial analyst and working in the collection and recovery of debts owed to the 1st Respondent is a clear indication that he was working in the ordinary course of his duties when he sent the Complainant's details to a third party without his consent. The reason for sending those details was for purposes of debt collection which is his ordinary duty. Therefore, there was a close connection between the employee's conduct and the sending of the Complainant's details to an unauthorised third party.

36. Furthermore, the 1st Respondent admitted to its employee sharing the complainant's details with a third party in the ordinary course of business, which is a violation of the 1st Respondent's Code of Ethical Conduct and constitutes misconduct. As a result, the 1st Respondent claims to be conducting investigations into the matter. The Office does note, however, that the 1st

Respondent has not produced proof of the aforementioned investigations and steps taken against its employee.

37. Therefore, this Office finds that the 1st Respondent is vicariously liable for its employee's conduct.

II. WHETHER THE RESPONDENTS FULFILLED THEIR OBLIGATIONS UNDER THE ACT

38. The 1st Respondent is a data controller and the 2nd Respondent is a data processor within the definitions of the Act and therefore have obligations pursuant to the Act.

39. The Respondents had an obligation under Section 25 of the Act to adhere to the principles of data protection while processing the Complainant's personal data. Particularly, the Respondents were obligated under Section 25 (a) and (c) of the Act to ensure that personal data is processed in accordance with the right to privacy of the data subject and is collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes.

40. The 1st Respondent intimated that it was its staff member who shared the Complainant's details without the approval from itself and consent from the Complainant. However, because the staff member had access to the Complainant's details in his ordinary course of work, the 1st Respondent is liable for the actions of its employee. The 1st Respondent stated that it took disciplinary measures towards the employee but provided no proof of the same. This Office finds the 1st Respondent liable for breach of Section 25 (a) and (c) of the Act.

41. Section 30 of the Act gives instances where a data controller or processor can lawfully process personal data. It states that a data controller or processor **shall not** process data unless the data subject consents to the processing for one or more specified purposes or the process is necessary for the reasons given in subsection (b).

42. The Office notes that there was a data sharing agreement between the 1st and the 2nd Respondent which formed the legal basis for processing of the Complainant's personal data between themselves.

43. However, the 1st Respondent shared the Complainant's details with a third party without his consent. As a data controller, the 1st Respondent had an obligation under Section 30 of the Act to ensure that the Complainant's personal data is secure and cannot be shared with a third party without his consent. Therefore, this Office finds the 1st Respondent liable for breach of Section 30 of the Act.

44. Section 32 of the Act provides for the conditions of consent and provides that a data controller and processor shall bear the burden of proof to establish that the data subject consented to the processing of their personal data for a specified purpose. Therefore, the 1st Respondent did not discharge this burden and instead relied on the defence that it was their staff member who shared the Complainant's details without his consent. Its defence is therefore not satisfactory to this Office.

45. With regard to the 2nd Respondent, the Office observes that the Complainant made the claim but did not give the necessary proof to disprove it. Given the circumstances, this Office concludes that the Complainant failed to meet its burden of proving a viable claim against the 2nd Respondent.

46. In addition, the 1st Respondent shared information with the 2nd Respondent in respect of the Complainant's debt and to facilitate contact with the Complainant as per the service contract with the 2nd Respondent. The 1st Respondent in this regard has reiterated that the 2nd Respondent has a duty and obligation to uphold confidentiality and not to disclose the 1st Respondent's customers with third parties in the discharge of their obligations.

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

47. 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.

48. Having found that the 1st Respondent failed to fulfil their obligations under the Act, an Enforcement Notice shall be issued against the 1st Respondent pursuant to Section 58 of the Act. With regards to the 2nd Respondent, this Office determines that the Complainant failed to achieve its burden of proving a legitimate claim against it, and thus the case is dismissed in respect to the 2nd Respondent.

F. FINAL DETERMINATION

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

i. The 1st Respondent is found vicariously liable for the actions of its employee;
ii. The Complaint against the 2nd Respondent is dismissed;
iii. An Enforcement Notice to issue 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 15th day of December 2023.

IMMACULATE KASSAIT, MBS
DATA COMMISSIONER