REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 0884 OF 2025

EFK.....COMPLAINANT

-VERSUS-

QUEST HOLDINGS LIMITED.....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, through its employee, unlawfully disclosed his personal data without a lawful basis and in contravention of the principles of lawful processing.

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 20th June, 2025. 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 21st July, 2025 referenced ODPC/CIE/CON/2/1 (486). 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 detailed response to the allegations made by the Complainant;
   b) A contact person who can provide further details;
   c) Any relevant materials or evidence in support of the statement of response above;
   d) A demonstration of compliance with the principles of data protection as set out in Section 25 of the Data Protection Act;
   e) A demonstration of the technical and organizational safeguards that put in place to ensure compliance with data protection by design or by default pursuant to Section 41 of the Act;

f) The mitigation measures adopted or being adopted to address the complaint to the satisfaction of the Complainant, if any;

g) Any other relevant information.

8. The Respondent furnished the Office with its statement of response on 28th July, 2025.

D. NATURE OF THE COMPLAINT

9. The Complainant alleges that an employee of the Respondent, while acting in the course of employment, erroneously attached and disseminated a confidential file containing personal data of NCBA Bank customers including names, email addresses, and outstanding financial amounts to unintended recipients through a mail merge email, thereby causing an unlawful disclosure and breach of the principles of lawful processing and confidentiality under the Act.

E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

i. THE COMPLAINANT'S CASE

10. The Complainant alleges that on 23rd May 2025, an employee of the Respondent, acting within the scope of their employment, erroneously attached a confidential file containing sensitive personal data to a mail merge email. This file was disseminated to an undisclosed number of recipients, comprising a subset of the 461 affected NCBA customers.

11. The Complainant states that the compromised data included, but was not limited to, full names, email addresses, and outstanding financial amounts owed to NCBA.

12. The Complainant pleads that while the mail merge functionality of the email itself ensured that individual recipients only viewed their specific data within the email body, the egregious breach of data protection principles manifested in the attachment.

13. The Complainant avers that the said attachment, containing the personal information of multiple customers, was transmitted to numerous, though not all, recipients on the mailing list.

14. The Complainant further alleges that the dissemination of these emails was not a singular event but rather occurred incrementally over the course of the week.

15. The Complainant states that the Respondent's employee has formally admitted culpability for this data breach. Subsequent to the incident, an apology email was disseminated to the affected recipients.

16. The Complainant avers that NCBA Bank has provided unequivocal written confirmation acknowledging its awareness of this data breach and, in light of this serious lapse in data security, has taken the decisive step of suspending its contractual agreement with the Respondent.

17. In support of the complaint, the Complainant attached the following documents:

    i. A copy of the data breach email from the Respondent containing the excel file
    ii. A copy of the apology email from the Respondent.

iii. THE RESPONDENT'S RESPONSE

18. In its statement of response, the Respondent states, a data breach had occurred on 23rd May 2025, affecting approximately 400 customers, and avers that one of the affected individuals subsequently filed a complaint against the Respondent, as referenced in the Notification of Complaint letter.

19. The Respondent pleads that, in compliance with data protection guidelines, the incident was reported to the Office within 72 hours of its occurrence.

20. The Respondent further states that, for reference, it enclosed supporting documents, including a summary of the immediate actions taken to mitigate the breach and prevent recurrence, email threads outlining communication and reporting to the Office, and the Excel attachment that had been shared with the affected customers.

F. ISSUES FOR DETERMINATION

21. In light of the above, the complaint, the Respondent's responses and evidence adduced together with the investigations conducted, the following issue falls for determination by this Office.

    i. Whether the Respondent unlawfully disclosed personal data of the Complainant in contravention of the Act.
    ii. Whether the Complainant is entitled to any remedies under the act.

i. WHETHER THE RESPONDENT FULFILLED ITS STATUTORY DUTIES IN COMPLIANCE WITH ITS OBLIGATIONS UNDER THE

22. It is not disputed that, the Respondent's employee erroneously attached a file containing personal data of multiple NCBA Bank customers to a mail merge email, which amounts to unauthorized disclosure as defined in Section 2 of the Act.

23. Section 25(a) of the Act additionally 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.

24. The Respondent states that financial information was disclosed but emphasized that the disclosure was inadvertent and not malicious. It submitted that remedial measures were taken, including suspension of the contract by NCBA Bank, as acknowledgment of accountability. Additionally, the Respondent pleads that it complied with Section 43 of the Act by reporting the breach within 72 hours and therefore discharged its procedural obligations.

25. It is trite that the Respondent complied with Section 43 on timely reporting of a data breach, however, it does not extinguish liability for the underlying contravention of substantive obligations as a data handler.

26. Section 41 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. This provision imposes a continuous obligation. Safeguards must be designed into systems **before** processing begins (privacy by design) and maintained **throughout** processing (privacy by default).

27. The Complainant contends that the Respondent failed in its duty to safeguard personal data because the erroneous dissemination of personal and sensitive data occurred incrementally over the course of a week and that this demonstrated systemic weaknesses in monitoring and technical safeguards.

28. The fact that the dissemination occurred over the course of a week without detection shows absence of monitoring systems capable of identifying or halting irregular data flows.

This systemic lapse contravenes the duty under Section 41(1) to secure personal data against accidental or unauthorized disclosure.

29. Additionally, Section 42(4) requires a processor to take all reasonable steps to ensure employee compliance with security measures. That the breach originated from an employee's error, the Respondent failed to demonstrate that such reasonable steps were in place before the incident. The Respondent did not extinguish that adequate training, supervision, and automated safeguards had been implemented to ensure that personal data is processed in accordance with the principles set out in Section 25 of the Act.

30. In light of the above, the Office finds that the Respondent's failure was not merely a matter of isolated human error but a systemic lapse in organizational and technical measures, in access controls, staff training, and real-time monitoring. The incremental dissemination of the attachment over a week underscores the Respondent's inability to detect and arrest the breach promptly, further aggravating the violation.

31. Based on the foregoing, the Office finds that the Respondent herein failed to fulfilled its statutory duties in compliance with its obligations under the Act.

ii. WHETHER THE COMPLAINANT IS ENTITLED TO ANY REMEDIES UNDER THE ACT.

32. 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.

33. As a remedy, the Complainant prays for an order compelling the Respondent to forthwith erase all inaccurate data relating to him from its systems, to guarantee that his personal data shall not be disclosed to any third party without his express consent or a lawful basis as provided under the Act, and for an award of monetary compensation to redress the unlawful processing of his data and the attendant harm suffered.

34. Section 65(1) of the Act provides, that a person who suffers damage by reason of a contravention of a requirement of this Act is entitled to compensation for that damage from the data controller or the data processor. Section 65(2) provides, a data controller involved in processing of personal data is liable for any damage caused by the processing.

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

36. Having established that the Respondent failed to discharge its statutory obligations under Sections 25(a), 41 and Section 42 of the Act, this Office finds that the Complainant is entitled to compensation. Accordingly, the Respondent is hereby directed to pay the Complainant the sum of **Kenya Shillings Two Hundred and Fifty Thousand (KES 250,000)** as compensation.

37. In addition, having found that the Respondent failed to process the Complainant's personal data in accordance with the data protection principles and that they failed to put in place technical and organizational measures to implement data protection principles effectively, an Enforcement Notice shall issue against the Respondent pursuant to Section 58 of the Act and Regulation 16 of the Enforcement Regulations.

38. In so doing, this Office takes into account the nature and extent of violation with regard to unlawful processing of the Complainant's personal data and the failure to process personal data in accordance with the principles of personal data.

G. FINAL DETERMINATION

39. 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. An enforcement notice to issue to the Respondent.

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

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

DATED at **NAIROBI** this 17th day of September 2025

Immaculate Kassait, MBS
DATA COMMISSIONER