REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 1212 OF 2023

PAULINE MUHANDA

T/A MUDESHI MUHANDA AND CO. ADVOCATES..... COMPLAINANT

-VERSUS-

SAFARICOM PLC.....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 AND BACKGROUND

1. 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.

2. 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.

3. 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.

4. It is on that basis that, the Office received a complaint dated 11th July, 2023 pursuant to Section 56 of the Act and Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 ('the Regulations') from the Complainants who were aggrieved data subjects.

5. The Complainant appointed the firm of Wasonga B.O & Associates Advocates through a Notice of Appointment dated 31st July 2023.

6. Pursuant to Regulation 11 of the Regulations, the Office, *vide* a letter dated 17th July, 2023, referenced ODPC/CONF/1/5/Vol 1 (338) notified the Respondent of the complaints filed against it and required its response within 21 days.

7. The Respondent, through its advocates, filed a Notice of Preliminary Objection dated 26th July 2023 and a response to the complaint *vide* a letter dated 7th August 2023.

B. NATURE OF THE COMPLAINT

8. The Complainant is an Advocate of the High Court of Kenya. As a result of proceedings in court, the Complainant allegedly discovered, through an application filed in court, that her law firm and herself have been under private investigation. These investigations led to MPESA statements relating to herself and the law firm being accessed without their consent or knowledge.

9. The Complainant attached the said M-Pesa statements to her complaint indicating various transactions between 11th and 31st December 2022.

10. As a result, both hers and her clients' information had been revealed without their consent. It is against this backdrop that the Complainant lodged the complaint with this Office.

11. It is imperative to note that the investigations and this determination is confined to the Complainant's personal data, as the data subject, and not information relating to her firm or her clients.

C. THE RESPONDENT'S CASE

12. The Respondents through their advocates put in a Notice of Preliminary Objection dated 26th July 2023 stating that:

    i. This Office does not have jurisdiction to entertain the re-filed complaint as the ODPC is now *functus officio*.

ii. The complaint offends the *res judicata* doctrine and the Respondent should not be vexed twice over the same cause.

iii. The ODPC acted in violation if Section 8 of the Act by soliciting the Complainant to lodge a complaint which had already been determined by the ODPC's finding that it had no jurisdiction.

13. The Office acknowledged receipt of the Notice of Preliminary Objection *vide* a letter dated 31st July 2023 and required the Respondent to respond to the Complaint, informing them that the preliminary objection would be considered in this determination.

14. The Respondent put in a response to the Complaint through a letter dated 7th August 2023 and stated that they have put in place technological and organisational measures to eliminate and minimize data breaches; including coming up with various policies regulating access to data and regular periodical training of its staff in respect of those policies and controls. The policies include an Acceptable Usage Policy, Disciplinary Policy and Procedure, Safaricom Data Protection Policy and Safaricom Information Security Policy. The Respondents attached the said policies to their response.

15. The Respondent stated that it has an elaborate sanction mechanism which includes undertaking disciplinary processes and/or reporting an employee who is liable for data breach to the police for prosecution for deterrence purposes.

16. The Respondent further stated that it has also put in place controls to ensure that only authorised persons have access to M-pesa statements which are in-built within its IT systems including access controls, logging, monitoring controls, quarterly audits, the Safaricom VPN which employees are required to sign into before accessing the data, and two-factor authentication.

17. Upon receipt of the complaint, the Respondent stated that it established that an employee had acted against her terms and conditions of her contract of employment and their policies by releasing the Complainant's data to a third party without a court order nor consent of the Complainant.

18. The Respondent stated that the employee was a customer care agent, who in her ordinary course of work had access to M-Pesa statements and had an obligation to provide them to data subjects upon their request or to other parties upon the production of a court order.

19. Upon discovery of the violation, the Respondent stated that it initiated disciplinary proceedings which resulted in the dismissal of the employee. The

Respondent further stated that it reported the said breach and violation to the police for prosecution under Sections 72 (4) and (5) and 73 of the Act.

Further, the Respondent averred that actions of the employee are not attributable to it as she acted outside the scope of her duties, and in furtherance of a fraudulent scheme which did not align with the measures they set up.

20. Additionally, the Respondent stated that the Complainant may pursue their former employee for the breach and if the Complainant pursues such a course, the Respondent is ready to assist the Complainant with the necessary evidence to prosecute the claim.

21. The Respondent reiterated that it did not cause the said breach and as such, is not liable as alleged by the Complainant.

22. The Respondent claimed that the complaint as filed does not disclose any legal injury, loss and damage occasioned to the Claimant as a result of the alleged breach.

23. Further, the Respondent averred that part of the data which is allegedly breached, is information which was not confidential, particularly, the Complainant's phone number which appears in the Complainant's letterhead.

24. The Respondents stated that the allegations that the said breach resulted in disclosure of the nature of work of the Complainant, communication between clients is not apparent on the said statement, and that the said allegation is without a reasonable basis. There was no evidence, according to the Respondent, that the names of persons indicated in the statement are clients of the Complainant as alleged or at all.

25. The Respondent prayed that the complaint be dismissed based on the above reasons.

D. ISSUES FOR DETERMINATION

26. Having considered the nature of the complaint, and the evidence adduced by all parties to the complaint, the following are the issues for determination of this complaint:

    i. Whether this Office has jurisdiction to hear and determine this complaint;

    ii. Whether the Respondent was vicariously liable for its employee's conduct under the Data Protection Act; and

iii. Whether the Respondent fulfilled its obligations under the provisions of the Act.

I. WHETHER THIS OFFICE HAS JURISDICTION TO HEAR AND DETERMINE THIS COMPLAINT

27. This Office received a preliminary objection by the Respondents dated 26th July 2023 setting out three issues:

    i. ODPC being *functus officio* with respect to complaints filed on 17th March 2023 and 18th March 2023 being statute barred.
    ii. ODPC lacking jurisdiction to investigate the complaints on account of *res judicata.*
    iii. ODPC acted in violation of Section 8 of Act by soliciting the Complainant to relodge the complaint.

28. On the first issue, this Office was established pursuant to Sections 5 & 6 the Act which was enacted to give effect to Article 31 (c) and (d) of the Constitution of Kenya, 2010. The objects and purpose of the Act, among others, is to protect the privacy of individuals and to provide data subjects with rights and remedies to protect their personal data from processing that is not done in accordance with the Act.

29. It is on this basis that this Office received a complaint dated 17th March 2023 and as per the Regulations, notified the Respondents of the complaint requiring them to respond within twenty-one (21) days. It is pertinent to note that the parties at this instance requested to be given a chance to conduct Alternative Dispute Resolution, which request was granted. However, the parties did not arrive at a settlement and neither was a settlement agreement recorded with this office.

30. As a result, the Office had to proceed with its investigations. However, noting the time taken by the parties in pursuing alternative dispute resolution, the 90 days statutory timeline barred this Office from rendering its decision. It is upon this basis that the Office advised the Complainant of the available options to them for the resolution of the complaint. Section 8(k) as read with Section 9(g) of the Act gives this Office the powers to perform its functions as necessary for the promotion of the objects of the Act and further to undertake any activity necessary for the fulfilment of its functions.

31. On the second issue on whether this matter is *res judicata*, this Office notes that no decision had been rendered on account of any complaint by the Complainant. The Black's law Dictionary 10th Edition defines "res judicata" as

"An issue that has been definitely settled by judicial decision...the three essentials are (1) an earlier decision on the issue, (2) a final Judgment on the merits and (3) the involvement of same parties, or parties in privity with the original parties..."

32. Similarly, in the case of **Christopher Kenyariri vs Salama Beach (2017) eKLR**, the court clearly stated the ingredients to be satisfied when determining ***res judicata*** thus;

"...the following elements must be satisfied...in conjunctive terms; a) The suit or issue was directly and substantially in issue in the former suit; b) Former suit between same parties or parties under whom they or any of them claim; c) Those parties are litigating under the same title; d) The issue was heard and finally determined; e) The court was competent to try the subsequent suit in which the suit is raised."

33. In view of the foregoing, the matter hand does not meet the threshold of cases where *res judicata* applies as aforementioned. Further, since this Office did not render any determination with regards to this complaint, then *res judicata* cannot apply in this instance as there was no finality in the resolution of the previous complaint.

34. On the last issue on the violation of section 8 of the Act, Section 8(a) of the Act provides that this Office's functions include overseeing the implementation of and being responsible for the enforcement of the Act. In so doing, the Office under Section 8(k) of the Act has powers to perform such functions as necessary for the promotion of the objects of the Act.

35. Therefore, this Office finds that it conducted itself in accordance with the powers and functions as envisaged under the Act. The Office did not solicit the complainant to re-submit her complaint. The Complainant was at liberty to decide whether or not to re-submit the Complaint. The Complainant made the independent decision to resubmit the complaint for fresh investigations in accordance with Section 56 of the Act and the attendant Regulations.

36. In view of the foregoing, this Office has the requisite jurisdiction to hear and determine the complaint as pertaining the privacy rights of the Complainant under the Act and the Regulations.

II. WHETHER THE RESPONDENT WAS VICARIOUSLY LIABLE FOR ITS EMPLOYEE'S CONDUCT UNDER THE DATA PROTECTION ACT

37. This Office notes that the Respondent does not dispute that there was a personal data breach by its employee, one Dorcas Mwaniki, as against the Complainant's

personal data. Further, that the said information was released to a third party without consent or a court order.

38. The Respondent availed its Acceptable Usage Policy which all its employees adhere to. Section 4 of the Policy provides that all its users shall comply with all the Respondent's Information Security and Privacy policies, procedures and guidelines.

39. The employee in question was a customer care agent and in her ordinary course of work had access to M-Pesa statements. However, the Respondent's policies stipulates that such information cannot be accessed by third parties unless there is a consent or a court order.

40. The Respondent further indicated that it has safeguards in place including access controls, logging, monitoring controls, quarterly audits, the Respondent VPN which employees are required to sign into before accessing the data and the two-factor authentication.

41. This Office observes that upon submission of the complaint to this Office, the Respondent conducted its own investigations and took disciplinary measures against the said customer care agent. The Respondent further reported the said personal data breach to the police.

42. Vicarious liability arises when the tortious act is done in the scope of or during the course of his employment or authority. In that regard, the Act does not prevent the imposition of vicarious liability on a data controller or data processor in circumstances where direct liability for a breach of the Act would rest with an employee in the course of their employment.

43. The Supreme Court of the United Kingdom in ***WM Morrison Supermarkets plc (Appellant) v Various Claimants (Respondents) [2020] UKSC 12*** held that the Controller was not vicariously liable for the actions of its former employee in wrongfully disclosing the payroll data of its entire workforce.

44. Consequently, the test applied by the UK Supreme Court in ***WM Morrison Supermarkets plc (Appellant) v Various Claimants (Respondents) [2020] UKSC 12*** in deciding whether an employer is vicariously liable is whether there was a sufficiently close connection between the work 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. in so doing, the two questions for consideration are:

1. What functions or "field of activities" had been entrusted by the employer to the employee?

rkt

2. Was there "sufficient connection between the position in which [the employee] was employed and his wrongful conduct to be make it right for the employer to be held liable"?

45. In the Complaint for determination by this Office, the customer care agent's role of extracting the Mpesa statements falls in her "field of activities" in which she is authorized by the Respondent. However, the Respondent has employed safeguards which ought to be followed in executing that role which should be adhered to. The fact that there was a close link between her duties and the actions she took thereafter of disclosing the complainant's personal information without the set procedure of a court order or consent from the complainant does not satisfy the close connection test.

46. Similarly, in evaluating culpability, it is notable that the customer care agent assumed the role of data controller when she accepted an unauthorized application from a third party without following the rules for accepting such applications. As a result, in carrying out the instructions, the agent failed and/or ignored the procedures established by the Respondent in circumstances of data sharing with third parties.

47. As a result, since the Office has established that there was not a sufficiently close connection between what the said customer care agent was authorized to do and her disclosure. This office finds that the fact that her employment at the Respondent company gave her the opportunity to commit the wrongful act was not sufficient to impose vicarious liability on the Respondent.

48. However, employers should not take this decision to mean that vicarious liability will never arise where an employee commits a data breach. This Office reiterates that there is nothing in the Act which excludes this possibility, and each case will turn on its facts.

49. Employers should continue to ensure that they have robust data processes and controls in place, including restrictions on who has access to personal data, to reduce the risk of data breaches occurring in the first place and limit the impact should one happen.

III. WHETHER THE RESPONDENT FULFILLED ITS OBLIGATIONS UNDER THE PROVISIONS OF THE ACT

50. A data controller as per Section 2 of the Act means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing personal data. The Respondent is a data controller with regards to the provisions of the Act with an obligation to ensure that the Complainant's personal data is processed in accordance with the right to

privacy of the data subject which includes not have data subjects' personal data disclosed to unauthorised third parties.

51. Being a data controller, the Respondent is obligated under Section 41 of the Act to implement appropriate technical and organisational measures designed to implement the data protection principles in an affective manner and to integrate necessary safeguards for that purpose into the processing,

52. Further, subsection 3 directs data controllers such as the Respondent to implement appropriate technical and organisational measures for ensuring that, ***by default***, only personal data which is necessary for each specific purpose is processed, considering the amount of personal data collected and its accessibility, among others.

53. The Respondent has demonstrated in its response that it has put in place various policies and mechanisms to ensure that the personal data of their customers is safe and secure. It provided the said policies and procedures and proof of the same. However, in this instance, despite the policies and measures in place, the Respondent's employee conducted unlawful disclosure of the complainant's personal data to a third party without a court order or consent from the complainant.

54. It is imperative to note that the Respondent is a large data handler for the personal data that it collects, processes and stores including M-Pesa Statements which is the subject of this complaint. The Respondent therefore has a greater obligation to ensure that it has in place corresponding technical and organisational measures to protect the personal data in its controllership.

55. Section 72 of the Act provides for offences of unlawful disclosure of personal data. The Respondent relied on this provision to demonstrate that it reported the breach and violation to the police.

56. That notwithstanding, Section 72 (3) provides that, a person who obtains access to personal data, or obtains any information constituting such data, without prior authority of the data controller or data processor by whom the data is kept or discloses personal data to third party, commits an offence.

57. Section 72(4) of the Act further provides that subsection (3) shall not apply to a person who is an employee or agent of a data controller or data processor acting ***within the scope of such mandate***. This Office notes that the aforementioned Customer Care agent was still an employee of the Respondent at the time she made an unauthorized disclosure of personal information to a third party. In this regard, this Office concludes that such employee's actions deviated from the

confines established by the Respondent and therefore assumes personal responsibility as outlined under section 72(3).

E. FINAL DETERMINATION

58. In consideration of all the facts of the complaint and evidence tendered, and having found the Respondent is not vicariously liable for the actions of the customer care agent, the Data Commissioner makes the following determination:

i. The complaint stands resolved against the Respondent.

ii. A recommendation is made for the prosecution of Dorcas Mwaniki under Section 72(3) of the Data Protection Act and the attendant Regulations.

iii. Parties have a right to appeal this Determination to the High Court.

DATED at **NAIROBI** this 3rd day of October. 2023.

Immaculate Kassait, MBS

DATA COMMISSIONER