REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 842 OF 2024

S.M.M.....COMPLAINANT

-VERSUS-

AAR INSURANCE KENYA 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 filed a complaint on 13th June 2024 alleging that the Respondent, without obtaining consent, shared his family's health insurance information with a third party, who subsequently sent him unsolicited messages about his family medical plan.

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 13th June, 2024. The complaint was lodged pursuant to Section 56 of the Act and Regulation 4 of the Enforcement Regulations by the Complainant, who was an 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 18th June 2024 and referenced ODPC/CONF/1/5 VOL 1(979). In the Notification of the Complaint, the Respondent was informed that if the allegations by the Complainant were true, it was in violation of various provisions of the Act. Further, the Respondent was asked to provide this Office with the following: -

    a. A response to the allegations made against it by the Complainant;

    b. Any relevant materials or evidence in support of the response;

    c. The legal basis relied upon to process and engage with the Complainant's personal data;

    d. Proof of consent from the Complainant or the lawful basis for sharing the Complainant's personal data with a third-party (M-TIBA);

e. A detailed description of how it fulfills the rights of a data subject;

f. 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; and

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

8. The Respondent responded to the Notification of Complaint letter *via* a letter dated 8th July 2024.

9. This determination is therefore as 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

10. The Complainant alleged that the Respondent, without obtaining consent, shared his family's health insurance information with a third party, who subsequently sent him unsolicited messages about his family medical plan.

E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

i. THE COMPLAINANT'S CASE

11. The Complainant alleged that the Respondent shared his family health information with an external entity without consent.

12. The external entity then proceeded to send engaging and intrusive SMS marketing messages without obtaining consent. The Complainant provided screenshots of the said SMS messages as proof.

13. The Complainant sought the following remedies: -

i) A written apology;

ii) Retrieval of information and documents previously shared with external parties; and

iii) Compensation for the distress inflicted by the incident.

ii. THE RESPONDENT'S RESPONSE

14. The Respondent stated that it is a provider of health insurance and other insurance services regulated by the Insurance Regulatory Authority (IRA) and as such among others develops, markets and underwrites healthcare schemes for corporate and retail clients.

15. The Respondent stated that on 1st October 2020, it entered into a Partnership Agreement (Partnership Agreement) with Carepay Limited (CarePay) and CSL Services Limited (CSL) to manage its schemes on the M-TIBA Platform.

16. It further stated that CarePay operates a mobile based healthcare infrastructure (the "M-TIBA Platform") which connects payers, patients and providers of healthcare services and enables digital administration of healthcare schemes.

17. CSL is a subsidiary of CarePay and is licensed by the Insurance Regulatory Authority ("IRA") to provide claims settlement services to insurers and as such to negotiate and settle insurance claims from healthcare providers on their behalf.

18. CarePay and CSL together offer third-party administration services for healthcare schemes of insurers, with CarePay operating the M-TIBA Platform on which the schemes are administrated and managing a network of healthcare service providers while CSL adjudicates and settles provider claims (the "Services").

19. The Partnership Agreement referenced above (paragraph 15 of the Determination) contained substantive clauses on data protection, and annexed to it was a Data Sharing Agreement setting out the manner in which personal data would be shared by the parties and the measures that would be taken to process and safeguard the same.

20. On 15th December 2023, in furtherance of their partnership, the Respondent, Carepay and CSL entered into an Agreement for Third Party Administration (TPA) Services for Medical Insurance Schemes on the M-TIBA Platform ("the Agreement") to provide claims settlement services.

21. The Respondent stated that the main purpose of the Agreement was to digitise the administration of schemes, reduce costs and reduce value leakages thereby enhancing efficiency and enabling access to affordable health insurance in Kenya.

22. In furtherance of the contract, the Respondent transferred the existing in-patient schemes to M-TIBA. Consequently, in-patient customers were upgraded from photo card to virtual access whereby the customers could view their benefits and utilization balance by dialing *253# and selecting "2.MY M-TIBA".

23. The Respondent averred that on 30th December 2023, it sent out text messages to in-patient customers informing them of the upgrade from photocard to M-TIBA virtual access. The Respondent provided samples of the messages sent to its customers as proof.

24. The Respondent stated that it only realized that the Complainant did not receive the text messages they sent in December 2023, when the complaint was served upon them. Upon receiving the complaint, the Respondent investigated the matter and established that: -

    a) The Complainant took out an AAR Insurance Kenya in-patient medical cover for himself and his family members.
    b) In December 2023, when the decision was made to outsource claims settlement to M-TIBA and change the inpatient cover mode of access from photo card to M-TIBA, the Respondent was in the process of migrating and adopting a new operating system.
    c) To facilitate communication to customers of the change in the mode of accessing the in-patient cover, the Respondent ran a system query to extract contacts of in-patient members. However, this query only picked data from the Respondent's old operating system and erroneously left out data relating to customers who had been migrated to the new system.
    d) The Complainant's contact details were hosted on the new system and hence they were not picked up by the query.

e) From 1st January 2024, M-TIBA began adding the data of all in-patient cover customers to their virtual access platform and initiated SMS messages to the customers informing them of their enrolment onto their platform. Consequently, the Complainant and his beneficiaries received the text messages that were forwarded to this Office by the Complainant. The message sent by M-TIBA to the Complainant was not an intrusive marketing SMS but a critical communication relating to the provision of services to the Complainant in furtherance of the contractual obligations.

f) It has not received any other complaint regarding the migration to M-TIBA or communication sent to customers in December 2023.

25. The Respondent stated that it relied on consent as the lawful basis to process and engage with the Complainant's personal data. It provided the Application Form signed by the Complainant in which he granted the Respondent consent to process his personal data and consent to receive communication related to his policy. As such, the Respondent asserted that, it being a registered data controller and data processor, it has lawfully been processing the Complainant's personal data and that of his beneficiaries.

26. Further, the Respondent stated that Regulation 5(1) and (2) of the Data Protection (General) Regulations 2021 states that, a data controller or data processor may process personal data without the consent of a data subject if the processing is necessary for any reason set out in Section 30(1)(b) of the Act, provided that the data controller and processor shall only rely on one legal basis for processing at a time which shall be established before the processing.

27. The Respondent stated that pursuant to Section 30(1)(b)(i) and (vii) of the Act, it shared its customers personal data with M-TIBA for two reasons: -

i) To fulfil its contractual obligations with the Complainant –

ii) In furtherance of its legitimate interests - In this case, the legitimate interests pursued were the digitization and optimization of the medical claims process for enhanced customer experience, and therefore beneficial to the Complainant. This processing of the Complainant's

personal data is not in any way unwarranted and does not result in any harm nor is it in any way prejudicial to the rights and freedoms or legitimate interests of the Complainant. As such, it meets the conditions set out in Section 30 (1) (b) (vii) of the Act.

28. The Respondent asserted that it has lawfully been processing the Complainant's personal data, and that CarePay and CSL are also lawfully processing the Complainant's personal data. There has therefore, been no breach of the Complainant's rights nor of its duties or responsibilities as envisioned under the Act and its attendant Regulations.

29. The Respondent stated that it has taken the following mitigation measures: -

a) It sent a written apology to the Complainant on 22nd and 25th June 2024 on account of the inadvertent error of not receiving the text message from the Respondent despite the fact that the processing of the personal data of the Complainant was lawful and in accordance with the principles of the Data Protection Act.
b) It met with the Complainant on 25th June 2024 in its offices, offered an apology and explained how the error occurred. The Complainant, however, did not accept its explanations.
c) It has included the Complainant's telephone number and email address in its communication data base.
d) It has sent communication on email and SMS to all its customers explaining its relationship with M-TIBA, the digitization strategy and the adoption of the inpatient virtual access mode through the M-TIBA Platform.
e) It has retrieved the Complainant's information shared with M-TIBA.
f) It has enhanced its external correspondence logging capabilities to ensure completion and remediation of any error in its communication channels.
g) It has trained all its staff and agents, on data protection.
h) It has developed and rolled out data protection policies to all staff members.

i) It has revised its member application forms and consent forms in compliance with the Data Protection Act.

j) It has appointed a Data Protection Officer.

k) It has trained and entered into data processing agreements with its data processors.

l) It has trained and entered into data sharing agreements with its joint data controllers.

30. In conclusion, the Respondent stated that the Complainant has requested for compensation, on the basis of distress inflicted by the incident. It reiterated that neither itself, CarePay or CSL has in any way contravened the provisions of the Act and that the Complainant has not furnished any proof of distress or damage arising from this incident and is consequently not entitled to any compensation.

31. The Respondent submitted the following documents to this Office: -

i) Appendix 1 - Notification to clients (30th December 2023)

ii) Appendix 2 – Apology and Invitation to Resolve Complaint

iii) Appendix 3 – Evidence of Meeting with the Complainant

iv) Appendix 4 (a) – AAR Clients' Communication by email

v) Appendix 4 (b) – AAR Clients' Communication by SMS

vi) Appendix 5 – Application Form Signed by the Complainant

vii) Appendix 6 – AAR Insurance Kenya Limited, Carepay Limited & CSL Services Limited Agreement for Third Party Administration Services for Medical Insurance Schemes on the M-TIBA Platform

viii) Appendix 7 – Data Processing Agreement between AAR Insurance Kenya Limited and Carepay Limited.

ix) Appendix 8 (a) – Data Protection Training Schedules held by the Respondent.

x) Appendix 8 (b) – Data Protection Training Attendance Register (Online Training)

xi) Appendix 8 (c) – Data Protection Training Attendance Register (physical training)

xii) Appendix 9 – Revised Application Forms.

F. INVESTIGATIONS UNDERTAKEN

32. The Office analysed the complaint as lodged, reviewed the response submitted by the Respondent and analysed all documents submitted by the parties as evidence.

33. The Office established that the Complainant had taken out a medical insurance policy for himself and his family with the Respondent.

34. The Office also established that the Complainant indeed received messages regarding his family medical plan from a third party.

G. ISSUES FOR DETERMINATION

35. It is not in contention that the Respondent shared the Complainant's personal data with a third party, who subsequently sent him messages about his family medical plan.

36. In light of the above, 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 any remedies under the Act and the attendant Regulations.

I. WHETHER THE RESPONDENT FULFILLED ITS OBLIGATIONS UNDER THE ACT

37. The Respondent is a data controller within the definition of the Act and therefore has obligations pursuant to the Act.

38. The Respondent stated that it engaged the services of a data processor, CarePay Limited, to manage its schemes on the M-TIBA Platform and signed a data sharing agreement in compliance with the Act.

39. The Respondent averred that in December 2023, it informed its customers, through text message of the upgrade from the photocard system to M-TIBA virtual access which was to take effect from 1st January 2024.

40. Further, the Respondent admitted that the Complainant's details were erroneously excluded from the above communication.

41. Section 29(d) of the Act provides for the duty to notify and states that, *"a data controller or data processor shall, before collecting personal data, in so far as practicable,* ***inform the data subject of the third parties whose personal data has been or will be transferred to, including details of safeguards adopted."***

42. A perusal of AAR's Individual and Family Application Form filled by the Complainant during the onboarding process indicates that the Complainant had consented to receive communication related to his policy. However, he had not consented to receive communication regarding his policy from third parties and he was not notified of the onboarding of M-TIBA by the Respondent to manage its schemes on the M-TIBA platform.

43. From the above, it is evident that the Complainant was not notified that his personal data will be transferred to a third party (M-TIBA) contrary to Section 29(d) of the Act.

44. The Office has however taken note of the mitigation measures taken by the Respondent to remedy this infraction, including the inclusion of the Complainant's telephone number and email addresses in their communication database, sending out communication to all customers explaining their relationship with M-TIBA and enhancing their external correspondence logging capabilities.

45. As regards the lawful basis for processing, the Respondent stated that it shared the Complainant's personal data with M-TIBA in order to fulfil its contractual obligations with the Complainant and relied on Section 30(1)(b)(i) of the Act as a lawful basis to process the Complainant's personal data.

46. The Respondent also stated that it shared the Complainant's personal data with M-TIBA in furtherance of its legitimate interests and relied on Section 30(1)(b)(vii) of the Act as the lawful basis for processing the Complainant's personal data.

47. In support of the above, the Respondent submitted a record of processing activities setting out the different personal data processed pursuant to the Data Processing Agreement between themselves and M-TIBA, and the legal basis for each processing activity.

48. The Office therefore finds that the Respondent has demonstrated the lawful basis for processing the Complainant's personal data.

49. The Complainant alleged that he received unsolicited marketing messages from the Respondent.

50. Regulation 14(1) of the Data Protection (General) Regulations, 2021 provides the interpretation of 'commercial purposes' and provides that for the purposes of Section 37(1) of the Act, *a data controller or data processor shall be considered to use personal data for commercial purposes where personal data of a data subject* ***is used to advance commercial or economic interests, including inducing another person to buy, rent, lease, join, subscribe to, provide or exchange products, property, information or services, or enabling or effecting directly or indirectly, a commercial transaction.***

51. The messages sent to the Complainant did not amount to commercial use of his personal data as they did not satisfy the ingredients above, for use of personal data for commercial purposes.

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

52. 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.

53. The Complainant prayed for a written apology, retrieval of information and documents previously shared with external parties, and compensation for the distress inflicted by the incident.

54. The Respondent offered a written apology to the Complainant *via* a letter dated 21st June 2024.

55. The Respondent, in its response stated that it had retrieved the Complainant's information shared with M-TIBA. However, the right to erasure must first be exercised with the Data Controller, before this Office's intervention. The procedure for exercising the right to erasure is as prescribed in Regulation 12 of the Data Protection (General) Regulations, 2021.

56. Section 65 of the Act provides for compensation to data subjects and states, *"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."*

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

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

59. In considering whether to issue compensation, this Office takes into consideration the fact that the Respondent did not fulfill its duty to notify as provided under Section 29 of the Act. Further, the Office considers the fact that the Respondent did not intentionally fail to fulfil its duty to notify as the Complainant's contact details were erroneously excluded from the communication notifying its customers of the change.

60. Further, this Office considers the fact that the Respondent entered into a written contract with the third parties that it shared the Complainant's personal data with in compliance with Section 42(2)(b) of the Act.

61. The Office also considers the fact that the Complainant did not demonstrate the harm or potential harm suffered by the Respondent's action of sharing his personal data with M-TIBA. The Complainant failed to demonstrate the distress suffered as a result of the Respondent's actions.

62. The upshot is that the Respondent is hereby ordered to pay the Complainant **Kenya Shillings Twenty Five thousand (KES. 25,000/=)** in nominal compensation.

H. FINAL DETERMINATION

63. The Data Commissioner therefore makes the following final determination: -

i. The Respondent is hereby found liable for failing to fulfil its duty to notify under Section 29 of the Act;

ii. The Respondent is hereby **ordered to pay the Complainant Kenya Shillings Twenty Five Thousand (KES. 25,000/=)** as compensation; and

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

DATED at **NAIROBI** this 10th day of September 2024.

IMMACULATE KASSAIT, MBS
DATA COMMISSIONER