REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 0072 OF 2024

KIPLIMO KIPTUI.....COMPLAINANT

-VERSUS-

MULLA PRIDE LIMITED T/A KE CREDIT.....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 Office received a complaint on 11th January 2024 alleging that the Respondent unlawfully obtained the Complainant's salary information, sent him threatening messages and calls even after loan repayments were made, tracked his location, including that of his child, to the extent of monitoring school drop-offs, and sent him marketing messages without obtaining consent.

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 (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 11th January 2024. The complaint was lodged pursuant to Section 56 of the Act and Regulation 4 of the Enforcement Regulations from 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 30th January 2024 and referenced ODPC/CONF/1/5 VOL 1 (770). 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. Details of how it obtained the Complainant's personal data;
    d. The legal basis relied upon to process and engage with the Complainant's personal data and whether or how it fulfills the duty to notify under Section 29 of the Act;

e. Whether the Complainant consented to the processing of their personal data; and

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;

8. The Respondent filed its response to the complaint via a letter dated 9th February 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 unlawfully obtained his salary details, sent him threatening messages and calls even after loan repayments were made, tracked his location, including that of his child, to the extent of monitoring school drop-offs, and sent him marketing messages without obtaining consent.

E. SUMMARY OF EVIDENCE ADDUCED

i. THE COMPLAINANTS' CASE

11. The Complainant alleged that he received a call from the Respondent informing him of his employer and salary details. He further stated that he did not consent to having the Respondent access his salary details.

12. The Complainant also alleged that he received a message with details of his child's school drop-off details, indicating that the Respondent was tracking him. He provided a screenshot of the said message as proof of the allegations made.

13. The Complainant alleged that he received threatening messages and calls even after making loan repayments. He went further and deleted his account on 11th January 2024 after making payments but still received threatening messages from the Respondent. He provided screenshots of the messages received as proof.

14. Additionally, the Complainant alleged that he received promotional messages from the Respondent without his consent. No evidence was availed to prove this.

15. Finally, the Complainant sought for the deletion of all his data in the possession of the Respondent.

ii. THE RESPONDENTS' RESPONSE

16. The Respondent stated that the information collected during the customer onboarding process consists of:
    i) **Personal details** – Name, ID number, date of birth, nationality, salary bracket and employment status.
    ii) **Personal contact details** – Includes residential addresses, mailing addresses, and contact information such as phone numbers and email addresses.
    iii) **Location data** – It seeks access or permission to track location-based information from mobile devices while using its mobile application to offer specific location-based services. Customers have the option to modify these permissions in their device settings.
17. The Respondent stated that the Complainant was contacted as his loan was overdue and he had not responded to its agents' text messages or picked up calls. No evidence was adduced to indicate that the loan was overdue or that the Complainant had not responded to the agents' messages and calls.
18. Concerning the issue of the Complainant receiving text messages even after clearing his loan, the Respondent stated that the problem arose from a customer error in providing the correct account details. It further stated that it offers two repayment channels – online and offline (using the Paybill). In this particular case, the customer made an offline payment but mistakenly omitted the correct account number. Once this was brought to its attention, the matter was promptly resolved and the customer's data was expunged from its system as per the Complainant's request.
19. The Respondent stated that every customer is granted access to its data privacy notice subsequent to downloading the loan application and prior to initiating the

loan application process. The Respondent provided a link to the privacy notice as well as a copy of the said privacy notice.

20. Regarding the issue of obtaining of the Complainant's salary details, the Respondent stated that, upon investigating the matter, it discovered that the collection agent accessed the customer data by using social media platforms like LinkedIn and that it strongly condemns such unlawful activities and emphasizes that it does not provide information about workplaces and salaries to its agents. It further stated that this breach of privacy goes against its ethical standards and that it is taking immediate corrective actions to address the issue.
21. The Respondent also stated that communication has been made to the outsourced company to be firm in ensuring debt collection agents have customer privacy policies and information processing certificates from the Office of the Data Protection Commissioner. No evidence was availed to prove that the above was done.
22. The Respondent stated that it had deleted the Complainant's data from its records. It provided a screenshot of its database as proof of the same.
23. In addition, the Respondent stated that it had issued an apology to the Complainant for the alleged data breach. It provided screenshots as proof that it had issued an apology.

F. INVESTIGATIONS UNDERTAKEN

24. The Office analysed the documents provided by both the Complainant and Respondent.
25. The Office also scheduled a site visit at the Respondent's premises on 2nd April 2024 to conduct further investigations on the matter. The Respondent was notified of the said visit via a letter dated 26th March 2024 and served upon it on 27th March 2024.
26. On 2nd April 2024, Investigation Officers from the Office visited the Respondent's premises located at Top Plaza, Kindaruma Road, and found the Office closed. The Investigation Officers knocked on the door but no one opened. There was

movement inside the Office thereby indicating a choreographed move to intentionally derail the investigations.

27. The Investigation Officers left and noted the efforts put by the Respondent to obstruct investigations.

G. ISSUES FOR DETERMINATION

28. In light of the above, the following issues fall for determination by this Office:
    i. Whether there was a violation of Complainant's rights 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 THERE WAS A VIOLATION OF COMPLAINANT'S RIGHTS UNDER THE ACT

29. Section 26 of the Act provides for the rights of a data subject under the Act. As such, the Complainant had the right to be informed of the use to which his personal data was to be put.

30. The Respondent did not inform the Complainant that it was going to collect his location details for purposes of tracking him, to the extent of monitoring school drop-offs of his child. The Respondent in its Privacy Policy only informed the Complainant that it will collect his Geo location for customer risk assessment. The Respondent also stated in its response to the complaint that it accesses location-based information to offer specific location-based services. It did not explicitly state what 'specific location-based services' it offers. Further, the Respondent did not state in its Privacy Policy that it would access the location details of the Complainant for purposes of tracking him and knowing his location in real time.

31. The Respondent by not informing the Complainant that his location details were going to be used to track him together with his child, violated his right to be informed.

II. WHETHER THE RESPONDENTS FULFILLED THEIR OBLIGATIONS UNDER THE ACT

32. The Respondent is a data controller within the definitions of the Act and therefore has obligations pursuant to the Act.
33. 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).
34. The Respondent in its response admitted to having obtained the Complainant's salary details unlawfully as it had not sought prior consent from the Complainant to access such details.
35. Further, Section 28(1) of the Act states that a data controller or a data processor shall collect personal data directly from the data subject. Section 28(2) provides for instances where personal data may be collected indirectly. The Respondent stated that it accessed the Complainant's salary details by using social media platforms like LinkedIn. It did not provide any evidence to show that the Complainant had deliberately made the data public by sharing his salary on his LinkedIn profile. The Respondent did not also provide proof of exactly where it obtained the salary details of the Complainant.
36. From the foregoing it is evident that the Respondent obtained the Complainant's salary details in an unlawful manner as it neither collected the personal data directly from the Complainant nor sought his consent to process his salary details.
37. Section 29(c) 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 purpose for which the data is being collected. The Respondent failed to fulfil this obligation by not informing the Complainant that his location data was going to be used to track him together with his child.

38. Section 44 of the Act imposes specific restrictions on handling of sensitive personal data and states that no category of sensitive personal data shall be processed unless the principles of data protection apply to that processing. The Respondent unlawfully processed the family details of the Complainant by tracking where the Complainant's child goes to School and the time that the child is dropped off at School.
39. Further, Section 25(c) requires every data controller or data processor to ensure that personal data is collected for explicit, specified, and legitimate purposes and not further processed in a manner incompatible with those purposes.
40. The Respondent's Privacy Policy states that the Respondent collects geo-location information for the purpose of customer risk assessment. The Respondent by tracking the Complainant to an extent of knowing when he has dropped off his child in school and where the child Schools, violated the principle of purpose limitation. The Respondent processed the personal data of the Complainant in a manner incompatible to the initial purpose of collection.
41. Section 25(f) requires every data controller or data processor to ensure that personal data is accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay.
42. The Complainant alleged that he received threatening messages and calls even after making loan repayment. On the other hand, the Respondent admitted to having sent messages to the Complainant even after making loan repayment. It stated that the problem arose from a customer error in providing the correct account details. No evidence was adduced by the Respondent to prove that the Complainant provided the wrong account number. Additionally, the Respondent stated that once this matter was brought to its attention, it expunged the Complainant's details from its system. The screenshots provided by the Respondent do not clearly demonstrate that the Complainant's details were deleted from its database.

43. The Respondent did not uphold the principle of accuracy by not updating its records promptly so as to avoid sending messages to the Complainant when he had repaid the loan. The Respondent had an obligation to ensure that the personal data in its custody is reliable and kept up to date.

44. The Respondent in its response alluded to the fact that it outsources debt collection services. Section 42(2)(b) mandates data controllers who are using the services of a data processor to enter into written contracts with all data processors processing personal data on their instructions. No evidence of the written agreements was availed to this Office by the Respondent thereby it did not fulfil its obligation of entering into written contracts with its data processors.

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

45. 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.

46. The Complainant sought for the immediate deletion of his personal data by the Respondent. The Respondent in its response claimed to have deleted the data but the screenshot provided were not sufficient to indicate that the Complainant's data was deleted. The Office sought to ascertain that the Complainant's data was deleted by conducting a site visit at the Respondent's premises but the same did not materialize as the Respondent willfully and conveniently closed its doors on the material day of the site visit.

47. The Respondent is hereby directed to **delete the Complainant's details from its records/database and provide proof of the same within seven (7) days** from the date of receipt of this Determination.

48. The Office notes with concern that the Respondent is a repeat offender having been found liable for similar violations of provisions of the Act in several other complaints lodged with the Office. The Office also notes that the Respondent obstructed the Data Commissioner in the exercise of her powers by refusing to

allow the Data Commissioner to enter its premises despite having been notified of a scheduled site visit.

49. Having found that that the Complainant's rights were violated and that the Respondent did not fulfil its obligations under the Act, an Enforcement Notice shall issue against the Respondent pursuant to Section 58 of the Act and Regulation 16 of the Enforcement Regulations.

H. FINAL DETERMINATION

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

i. The Respondent is hereby found liable.

ii. The Respondent is hereby directed to **delete the Complainant's details from its records/database and provide proof of the same within seven (7) days** from the date of receipt of this Determination.

iii. An Enforcement Notice to hereby be issued to the Respondent.

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

DATED at **NAIROBI** this 9th day of April 2024.

IMMACULATE KASSAIT, MBS
DATA COMMISSIONER