REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 00187 OF 2024

ROSE EMMA MUTHONI.....COMPLAINANT

-VERSUS-

SAMASOURCE KENYA EPZ LTD.....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 lodged a complaint against the Respondent alleging that whilst undertaking investigations against her, the Respondent processed her personal data without her consent which led an adverse investigation report against her. The alleged adverse investigation report led to her termination from the Respondent's employment.

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 29th 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 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 4th March 2024 referenced ODPC/CONF/1/5 VOL 1 (838). In the notification of the complaint, the Respondent was informed that if the allegations by the Complainant were true, they were in violation of various sections of the Act. Further, the Respondent was asked to provide this Office with the following:
    a. A response to the allegation made against them by the Complainant;
    b. Any relevant materials or evidence in support of the response;
    c. The lawful basis relied upon to process the complainant's personal data;
    d. Evidence to weather the complainant consented to the processing of their personal data; and

e. 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 do not take again.

8. The Respondent responded to the allegations *vide* letter dated 27th March 2024.

D. NATURE OF THE COMPLAINT

i. THE COMPLAINANTS' CASE

9. In her case, the Complainant stated that she had been employed by the Respondent for about 8 years until around 24th July 2023 when the Complainant received a termination notice of employment.

10. Preceding this termination, the Complainant was subjected to a disciplinary hearing with the Respondent regarding allegations of conflict of interest and receiving kickbacks from the Respondent's suppliers. The Respondent initiated an investigation into these allegations, which involved obtaining the Complainant's laptop for investigation purposes.

11. That, during this inquiry, the Complainant received a report from the Respondent Labeled 'Project Sync-Final Report dated 15th June 2023. This report contained financial data extracted from her Mpesa account statement, her Standard Chartered Bank Kenya Limited bank account.

12. It was the Respondent's case that the respondent being a data processor which handles personal data is obligated to comply with the principles of personal data protection outlined in Section 25 of the Data Protection Act.

13. The Respondent has failed to comply by the principles of personal data protection; processing personal data in accordance with the right to privacy; lawful, fair and transparent processing; purpose limitation and Data minimization as provided under the law.

14. The Respondent violated the Complainant's right to privacy by allowing the forensic company to access the Complainant's personal Gmail accounts, personal bank account, and Mpesa statements without obtaining explicit consent from the Complainant and that this action directly infringed upon the Complainant's privacy rights regarding her personal data.

15. The unauthorized access by the forensic company to the Complainant's personal data, without explicit consent of the Complaint or legal basis, violated the requirement for fair and transparent processing of data. There was no lawful basis for the forensic company accessing the Complainant's personal Gmail accounts and Bank statements during the investigations.

16. The personal data obtained was meant for investigation into work -related allegations. However, accessing the Complainant's personal Gmail accounts and financial statements went beyond the specified and legitimate purposes of the investigation, thus breaching the principle of purpose limitation.

17. That the forensic Company accessed extensive personal information from the Complainant's accounts using her laptop, exceeding what was necessary for the investigation and that this breached the principle of collecting data limited to what is necessary for the specified purpose.

18. The Complainant averred that her right to information was violated as she was not informed about how her personal data would be accessed and processed during the investigation, breaching her entitlement to be informed.

19. The Complainant's right to control access to her personal data was infringed upon as the data was accessed without her proper consent, thereby denying her the opportunity to manage access to her own information.

20. The Complainant's right to object to the processing of her personal data was disregarded as she raised objections to the unauthorized attempts to access her personal Gmail accounts. Yet these objections were not respected. Additionally, the Complainant was unaware of the fact that unauthorized access was also made to her bank accounts. Consequently, the Complainant had no opportunity to object to or challenge the access to her bank accounts by a third party, as she was unaware of this access, thereby further violating her rights to object to such data processing.

21. The Complainant averred that she was deprived of the opportunity to rectify or delete any false or misleading data collected or inferred from the unauthorised

access to her personal accounts, thus violating her rights to correction and deletion of inaccurate information.

ii. THE RESPONDENT'S RESPONSE

22. The Respondent stated its relationship with the complainant is that of an employer-employee and it is a duly registered Data Processor.

23. The Respondent observed that due to the Complainant's own admission that she was under investigation internally, and was subsequently subjected to a disciplinary hearing arising from allegations of conflict of interest and receipt of kick backs from its suppliers.

24. As part of its investigations and inquiry carried out in relation to the said allegations of conflict of interest and receipt of kickbacks, our clients intended to review the contents of the Complainant's work issued laptop.

25. That the said laptop being its property, it was subject to the terms and conditions of its Corporate Information Security Policy which provides as follows:-

    i. Clause 4 at page 5 on Scope of the Policy

This policy applies to all computer and network systems that Samasource owns, controls, or administers, including all operating systems, computers, and application systems. This policy is also applicable to all information, paper and electronic in the possession or control of Samasource Confidential information entrusted to Samasource by customers, business partners, suppliers, and other third parties are subject to this policy.

26. The despite the said policy, which was well within the knowledge of the Complainant, granting our client the right to monitor all company devices, including the Complainant's work issued laptop, the Respondent of obtaining the express written consent of the Complainant authorizing the Respondent to access and process any personal data contained in the Complainant's work issued laptop that may have been relevant to the ongoing investigation.

27. That the said written consent was duly signed by the Complainant on the 8th May 2023 and she confirmed that she granted the said consent freely and without coercion.

28. Upon obtaining the Complainant's express consent to access and process her personal data that may be relevant to the ongoing internal investigation, the Complainant contracted a duly registered Data Processor and Forensic Auditor, Stealth Africa Consulting LLP ('Stealth') to:-

- Access the information contained in the Complainant's work laptop;
- Process all documents and information contained therein that are relevant for purposes of the investigation;
- Conduct a forensic audit of the relevant documents and information; and
- Prepare an investigation report outlining the findings of the Forensic Auditor.

29. That a review of the contents of the said laptop computer by Stealth unearthed various documents, and information relevant to the ongoing investigations, including copies of personal bank and M-pesa statements that had been stored in the laptop, and none of the said documents were collected from any other source.

30. That from a reading of the said Digital Forensic Report, it is evident that all the documents relied on as part of the Forensic Audit and investigations:-

a) Were obtained solely from the Complainant's work issued laptop;

b) Were collected and processed solely for the purpose of investigating the allegations of solicitation and receipt of kickbacks and conflict of interest.

31. Upon processing the data contained in the laptop as described in the Digital Forensic Report, the Forensic Auditor proceeded to produce an investigation report dated 15th June 2023, setting out the findings of the Forensic Audit and a copy of the said report was duly provided to the Complainant as part of the internal proceedings.

32. That neither the Investigation Report nor any document obtained from the Complainant's laptop as part of the investigation was disclosed to any unnecessary third parties.

33. Further, the Investigation report dated 15th June 2023 was only shared with the Respondent's officials who were involved in the investigation and disciplinary process and no one else. And even then, the officials were only shown through the investigation report, portions of the personal information and documents deemed relevant to the investigation, and Not the entirety of personal information collected from the laptop.

34. That based on the said Investigation Report, a disciplinary meeting was conducted during which the Complainant was granted an opportunity to defend herself, and her employment was subsequently terminated.

35. The personal data contained in the laptop was collected and processed in a lawful manner compatible with the legitimate purpose for which it was collected and was never disclosed to any unnecessary third parties other the Respondent's officials involved in the investigation and disciplinary process. And even then, the officials involved in the disciplinary process were only shown, through the investigation Report, portions/excerpts of the personal information deemed relevant to the investigation and not the entirety of personal information collected from the laptop.

36. That the collection and use of the data was necessary for purposes of processing the legitimate interests of the Respondent and was necessary in aiding the investigation and detection of a potential offence and in pursuit of the establishment of a legal claim against the complainant.

37. As to the allegation that the Respondent failed to obtain her consent before sharing her information with a "third party" forensic auditor, the Respondent stated that the same lacks basis as forensic auditor is a duly registered Data Processor and at all material times it was processing data on behalf of it in accordance with the role of a data processor as defined in section 2 of the Act.

38. That the Forensic Auditor being a data processor, and a party acting under its authority it cannot be deemed to be a third party as alleged by the complainant.

39. That the allegation that the Complainant's Mpesa and Bank account statements were obtained from the custodian institutions is false and has been extensively rebutted in the detailed digital forensic report.

40. The Respondent stated that the allegation that the data was misrepresented is false for the reasons that nowhere in her complaint does the Complainant challenge the accuracy of the data.

E. INVESTIGATIONS UNDERTAKEN

41. Owing to the Respondent's response, it was necessary to conduct further investigations to this complaint prompting an on-site visit to the Respondent.

42. During the visit, our forensic investigators conducted a detailed analysis of the Complainant's work laptop, the images obtained and the procedure used by the Respondent's forensic investigators.

F. SUMMARY OF EVIDENCE ADDUCED

I. THE COMPLAINANT'S EVIDENCE

43. To support her complaint, the Complainant produced the investigation report relied upon by the Respondent to terminate her.

II. THE RESPONDENT'S EVIDENCE

44. To support its position, the Respondent adduced the following as its evidence:-

a) Written consent duly signed by the Complainant on the 8th of May 2024;
b) The detailed Digital Forensic Report, dated 22nd March 2024;
c) Investigation Report dated 15th June 2023; and
d) Samasource Corporate Information Security Policy.

G. ISSUES FOR DETERMINATION

45. In light of the above, the complaint, the Respondent's responses, and evidence adduced together with the investigations conducted, the following issues fall for determination by this Office:

i. Whether the Complainant's personal data was processed in accordance with the law;

ii. Whether the Complainant is entitled to any remedies under the Act and the attendant Regulations.

I. WHETHER THE COMPLAINANT'S PERSONAL DATA WAS PROCESSED IN ACCORDANCE WITH THE LAW

46. Before delving further, the Office notes that the complaint at hand is intertwined with an employment grievance and as such we would like to delink ourselves from any employment grievance fronted against the Respondent. The scope will be limited strictly to our mandate as stated above in paragraphs 4 to 6.

47. As earlier stated complaint relates to the processing of personal data wherein the Complainant alleges that her personal data was processed without her consent while the Respondent counters the allegations by submitting that it processed the Complainant's data with her consent.

48. Section 30 of the Data Protection Act provides the lawful bases for the processing of personal data. It provides:-

30. Lawful processing of personal data

(1) A data controller or data processor shall not process personal data, unless –

(a) the data subject consents to the processing for one or more specified purposes; or

(b) the processing is necessary-

(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

(ii) For compliance with any legal obligation to which the controller is subject;

(iii) In order to protect the vital interests of the data subject or another natural person;

(iv) For the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(v) The performance of any task carried out by a public authority;

(vi) For the exercise, by any person in the public interest, of any other functions of a public nature;

(vii) For the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interest of the data subject; or

(viii) For the purpose of historical, statistical, journalistic, literature, and art or scientific research.

(2) Further processing of personal data shall be in accordance with the purpose of collection.

(3) A data controller who contravenes the provisions of sub-section (1) commits an offence. (emphasis ours)

49. The Black's Law Dictionary, 10th Edition, defines consent as "agreement, approval, or permission as to some act or purpose, especially given voluntarily by a competent person.

50. Section 2 of the Act on the other hand defines consent as any manifestation of express, unequivocal, free, specific, and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data.

51. The definition of the Act details the minimum criteria of or for consent to be that it must be certain that the individual has consented, and what they have consented to. This certainty requires more than just a confirmation that they have read and understood the terms and conditions also there must be a clear signal that they agree or have agreed to what is there. The unambiguity of the consent also links in with the requirement that consent must be verifiable to the extent that one must be able to demonstrate that someone has consented to the consent.

52. From a combined reading of the above definitions, it is apparent that valid consent is a product of conscious decision-making and requires affirmative action. Therefore, knowledge of the subject of consent is required to make a decision for processing or not. Furthermore, valid consent is not a product of inactivity, as consent requires free will and communication by the person giving consent. Given that consent is a data subject determinant, it must be obtained before any processing and it must comply with the relevant data protection laws.

53. The Act goes further to state the conditions of consent. It states as follows with regard to the conditions of consent:-

32. Conditions of consent

(1) A data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose.

(2) Unless otherwise provided under this Act, a data subject shall have the right to withdraw consent at any time.

(3) the withdrawal of consent under sub-section(2) shall not affect the lawfulness of processing based on prior consent before its withdrawal.

(4) In determining whether consent was freely given, account shall be taken of whether, among others, the performance of a contract, including the provision of a service, is conditional on the consent of the processing of personal data that is not necessary for the performance of that contract. (emphasis ours)

54. From the evidence adduced to this office it is evident that at all material times in the processing of the Complainant's Personal data, there was consent. The Respondent has adduced a duly executed consent form by the Complainant. As such the Respondent has dispensed away with the burden of proof that there was consent.

55. The contents of the duly executed and witnessed consent form were as follows;-

"I Rose Emma of ID XXXXXXXX hereby give consent to my employer, Samasource Ltd, to use and process my personal data contained in my work computer XXXXXX

that may be relevant to the ongoing investigation relating to allegations of solicitation and receipt of kickbacks from suppliers.

I understand that I can ask to see this data for purposes of checking its accuracy at any time.

I have not been coerced to give this consent and I confirm that I have given my consent herein freely."

56. From the above it is evident that the scope of the consent related to investigations being done on the personal data contained in the Complainant's work computer.

57. From our investigations which we conducted upon the Respondent we found that the Respondent acted per the consent obtained from the complainant. The Respondent carried out its investigations strictly on the complainant's work laptop. The information contained in the Respondent's investigation report was found on the Complainant's work laptop and no other source as alleged by the Complainant.

58. We also found that the Respondent and the Forensic audit company that conducted the forensic audit had a data controller- data processor relationship. As such the forensic audit company acted on the instructions of the Respondent, who was the Data controller in this case.

59. Further, upon interrogating the Respondent company's policies we established that laptop being its property, was subject to the terms and conditions of its Corporate Information Security Policy which provides that all information contained in all the Respondent's property shall be deemed to be the company's property.

60. From the foregoing, it is evident that there existed a duly executed consent form and the processing of the Complainant's personal information was well in the in accordance with the Respondent Company's internal policies.

61. It is therefore our finding that the Respondent had a lawful basis for the processing of personal data.

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

62. According to Regulation 14 (2) of the Enforcement Regulations, a determination shall state the remedies entitled to the parties. Further, the remedies are provided for in Regulation 14 (3) of the Enforcement Regulations.

63. Having established that the Respondent acted within the law it therefore follows that the Complainant is not entitled to any remedy under the Act.

H. FINAL DETERMINATION

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

i. The Complaint lacks merit and it is hereby dismissed.

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

DATED at **NAIROBI** this 27th day of April 2024.

IMMACULATE KASSAIT, MBS
DATA COMMISSIONER