REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

IN THE SUO MOTO INVESTIGATION NO. 0003 OF 2024

ON

ELDORET HOSPITAL.....RESPONDENT

(DETERMINATION ON THE SUO MOTO INVESTIGATION BY THE OFFICE OF THE DATA PROTECTION COMMISSIONER ON PERSONAL DATA PROCESSING PRACTICES BY ELDORET HOSPITAL)

DETERMINATION

(Pursuant to Section 8(1)(f), 9(1) (a), 56 and 57 of the Data Protection Act, 2019 and Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021)

A. INTRODUCTION

1. On 3rd September, 2024, the Office instituted a *suo moto* investigation, being, ODPC *Suo Moto* Investigation NO. ODPC/SM/0003/2024, on its own initiative into Eldoret Hospital and taking cognizance of the public interest generated by the entity's personal data processing practices.

B. LEGAL BASIS

2. Article 31(c) and (d) of the Constitution of Kenya 2010 provides for the right to privacy. Consequently, as an effort to further guarantee the same, the Data Protection Act, 2019 (hereinafter as 'the Act') was enacted.

3. The Office of the Data Protection Commissioner (hereinafter 'this Office' 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 9(1)(a) of the Act provides that the Office shall has the power to conduct investigations on its own initiative, or on the basis of a complaint made by a data subject or a third party.

5. This determination is premised on the provisions of Regulation 14 of the Data Protection (Complaint 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 INVESTIGATION

6. Eldoret Hospital (hereinafter the 'Respondent') is a medical and health facility offering health services to members of the public. The facility primarily, and to a large extent, processes high volumes of personal data, including health data, from its patients and other parties seeking its services.

7. Concerns relating to the processing and use of the collected data have arisen. These concerns include inappropriate use of the personal data collected, violation of the data subjects' rights, unlawful data transfers, and inappropriate processing of the data collected.

8. Pursuant to Regulation 11 of the Enforcement Regulations, the Office notified the Respondent of the *suo moto* investigations *vide* a letter dated 3rd September, 2024 and referenced ODPC/CONF/1/5 VOL II(163). In the notification, the Respondent was asked to provide this Office with the following:

    a. A response to the alleged violations made against them and a contact person who can provide further details as regards this investigation;

b. Any relevant materials or evidence in support of the response;
c. The mitigation measures adopted or being adopted to address the alleged violations and to ensure that such occurrences mentioned do not take place again;
d. Documentation outlining the organization's data processing activities;
e. Details of the security measures implemented to safeguard personal data; and
f. Any relevant policies and procedures related to data protection.

9. Notably, the Respondent failed, refused or neglected to furnish the Office with a statement of response to the Notification.

10. On 4th December, 2024, the Office conducted a site visit at the Respondent's premises.

11. This determination is therefore as a result of an analysis of the investigations conducted by the Office.

D. NATURE OF THE INVESTIGATION

12. The Office conducted investigations into publicly available information regarding potential violations of the Act by the Respondent. The investigation focused on the Respondent's processing activities, particularly its indiscriminate classification and use of personal data for multiple purposes without notifying data subjects, obtaining their consent, or informing them of their rights. Additionally, the Respondent retained personal data for undefined periods and processed personal data, including photographs, for advertising purposes without implementing adequate safeguards.

E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

I. THE SUO MOTO INVESTIGATION

13. According to preliminary investigations by the Office, there was potential noncompliance in the Respondent's processing operations, particularly on how the Respondent used, handled and stored personal data in its custody as a data controller. The alleged violations against the Respondent were communicated to the Respondent *vide* the notification referenced hereinbefore and included:-

i) Lack of lawful basis for processing contrary to Section 25(b) and 30 of the Act to *wit* –

   a. the data being collected is not processed in accordance with the right to privacy of the data subjects;
   b. the data collected is used for illegitimate purposes which are incompatible with the purposes of collection.

ii) Failure to process personal data in a transparent manner and failure to fulfil the duty to notify contrary to Section 25(b) and 29 of the Act to *wit:-*

   a. The data subjects are not adequately informed of the use of the data that they collect; and
   b. the new purpose of the data collected is not compatible with the original purpose for which the data was collected.

iii) Inadequate security measures to protect personal data contrary to Sections 41, 42 of the Act as read with Regulation 32 of the Data Protection (General) Regulations 2021 to *wit-*

   a. a Data Protection Impact Assessment is yet to be undertaken by them;
   b. lack of appropriate technical and organizational measures to ensure the data collected is protected by design and default;
   c. lack of an operative means of managing policies and procedures for information security; and
   d. lack of adequate information security.

iv) Violation of the data minimization principle contrary to Section 25(d) of the Act as read with Regulation 33 of Data Protection (General) Regulations 2021 to *wit* –

   a. Procedural issues arising during collection of data. The Omnibus manner of collecting data violates or potentially violates the data minimization principle;
   b. they process personal data altogether even in circumstances where it's possible to only process the personal data for the relevant purpose; and
   c. Inefficient data flows which lead to unnecessary data collection and breaches.

v) Violation of the storage limitation principle (retention period if any) contrary to Section 25(g) of the Act as read with Regulation 35 of Data Protection (General) Regulations 2021 *to wit*–

a. The data collected is kept for longer periods beyond the required periods,
b. There is no regular review of whether the processing of the data collected is necessary for the purpose for which the data was collected.

II. THE RESPONDENT'S RESPONSE

14. The Respondent remained unresponsive, failing to address the concerns raised in the investigation. Consequently, the identified violations remained unchallenged and unrefuted.

F. INVESTIGATIONS UNDERTAKEN

15. The Office conducted a site visit at the Respondent's premises on 4th December, 2024.
16. During the site visit, the Office interrogated the Respondent's modes of operations and systems.
17. Among others, it was established that:

a. The Respondent does not have a functional data governance framework.
b. Whereas the Respondent collects and processes personal data from the public, it is not registered with this Office as a data controller or data processor.
c. While the Respondent collects and processes large volumes of personal data it had not conducted a data protection impact assessment of its activities.
d. The Respondent did not have a data protection policy for its processing activities.
e. The Respondent had not conducted a data protection training to its staff members.
f. It did not have a functional data breach incident response plan.
g. They had no data retention policy.
h. They had no mechanism for handling data subject's requests relating to access of personal data in their custody.

i. They had no mechanism for handling data subject's requests relating to rectification of personal data in their custody.
j. the Respondent was sharing its information with third parties with no data sharing agreements.
k. The Respondent had not implemented the aspects of data protection by design or default.
l. The Respondent did not apply the principle of minimization as it collected all manner of data from its patients without a justifiable purpose.
m. The data subjects are not adequately informed of the use of the data being collected.
n. The measures put in place by the Respondent are insufficient for handling the mass volumes of personal data and sensitive personal data being processed.

G. ISSUES FOR DETERMINATION

18. In light of the above, the following issues fall for determination by this Office:

i. Whether the Respondent has complied with the Act and its attendant regulations.
ii. Whether there are any remedies to issue with respect to the suo moto investigation.

I. WHETHER THE RESPONDENT HAD COMPLIED WITH THE ACT AND ITS ATTENDANT REGULATIONS.

19. Upon investigations, it follows that the Respondent has not complied with Sections 25, 26, 28, 29, 30, 32, 37 and Section 41 of the Act, as read together with Part V of the Data Protection (General) Regulations 2021 of the Act.

20. Section 25 of the Act provides for the principles of data protection as follows:-

a) Processed in accordance with the right to privacy of the data subject;
b) Processed lawfully, fairly, and in a transparent manner in relation to any data subject;

c) *Collected for explicit, specified, and legitimate purposes and not further processed in a manner incompatible with those purposes;*

d) *adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;*

e) *collected only where a valid explanation is provided whenever information relating to family or private affairs is required;*

f) *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;*

g) *kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and*

h) *not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.*

21. From this Office's investigations, it emerged that the Respondent has contravened the above principles of data protection to the extent that:

a) the patients' personal data was not being processed lawfully, fairly, and in a transparent manner;

b) the Respondent a wide range of personal data from the patients instead of collecting the personal data limited to what was necessary in relation to the purposes.

22. Section 29 of the Act provides for the Respondents duty to notify and provides that " *a data controller or data processor shall before collecting personal data, in so far as practicable, inform the data subject of:-*

a) *the rights of data subject specified under section 26;*

b) *the fact that personal data is being collected;*

c) *the purpose for which the personal data is being collected;*

d) *the third parties whose personal data has been or will be transferred to, including details of safeguards adopted;*

e) *the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data;*

f) *a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data;*

g) *the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and*

h) *the consequences if any, where the data subject fails to provide all or any part of the requested data."*

23. From this Office's investigations, the Respondent could not demonstrate how it notified its clients and patients of what they ought to be notified of before collection of their personal data as envisaged by Section 29 of the Act.

24. Section 30(1) of the Act provides for lawful processing of personal data and states that a data controller or data processor shall not process personal data unless the data subject consents to the processing for one or more specified purposes or the processing is necessary for one or more purposes specified in Section 30(1)(b).

25. During investigations, the Respondent could not demonstrate the lawful basis for collection and processing of the wide range of personal data that it was collecting.

26. As stated earlier, from our investigations, the Office found that the Respondent does not apply the principle of data minimization. It collects the patient's personal data in an omnibus manner.

27. Section 41 of the Act, as read together with Part V of the Data Protection (General) Regulations 2021, provides for data protection by design or by default and mandates the data controller to implement appropriate technical and organizational measures designed to implement the data protection principles effectively and to integrate necessary safeguards for that purpose into the processing. This is further elaborated upon in Part V of the General Regulations.

28. From our investigations, it emerged that the Respondent had not implemented appropriate and elaborate technical and organizational measures designed to

implement the data protection principles at your workplace. The system that the Respondent had installed at its premises did not meet the required elements to comply with Section 41 of the Act as read with Part V of the Data Protection (General) Regulations 2021.

29. To reiterate, the Respondent failed, refused, or neglected to provide the Office with an official statement addressing the concerns raised. Despite multiple opportunities to engage with the Office and clarify its data processing practices, the Respondent remained unresponsive, thereby obstructing efforts to assess its compliance with the Act. The Respondent's inaction not only demonstrated a lack of transparency but also raised serious concerns about its commitment to safeguarding personal data.

30. In light of the foregoing, the Respondent's continued failure to cooperate with the Office, its unwillingness to provide crucial information, and its disregard for statutory obligations under the Act, constitute clear non-compliance. The lack of transparency in its data processing activities, coupled with the failure to implement adequate safeguards, particularly concerning illegitimate use of personal data for other purposes other than the originally intended purpose and other undisclosed purposes, further underscores the severity of these violations.

31. Accordingly, the Respondent is found to be in breach of its legal obligations, warranting appropriate regulatory action. It is the finding and determination of this Office that the Respondent is non-compliant to the extent drawn above.

II. WHETHER THERE ARE ANY REMEDIES TO ISSUE WITH RESPECT TO THE SUO MOTO INVESTIGATION

32. Pursuant to Regulation 14 (2) of the Enforcement Regulations, a determination shall state the remedy directed by the Office. The remedies are provided for in Regulation 14 (3) of the Enforcement Regulations.

33. Having found that the Respondent failed to fulfil their obligations under the Act and attendant regulations, **an Enforcement Notice shall issue against the Respondents** pursuant to Section 58 of the Act and Regulation 16 of the Enforcement Regulations.

H. FINAL DETERMINATION

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

i. The Respondent is hereby found non-compliant in respect of this *suo moto* investigation.

ii. An Enforcement Notice be and is hereby issued to the Respondent.

iii. The Respondent has the right to appeal this determination to the High Court of Kenya within thirty (30) days.

DATED at **NAIROBI** this 16th day of December 2025

IMMACULATE KASSAIT,SC, MBS
DATA COMMISSIONER