REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC SUO MOTU INVESTIGATION NO. 020 OF 2025

ON

LAKE VICTORIA FIELD OF SEVENTH DAY ADVENTIST CHURCH.....RESPONDENT

(DETERMINATION ON THE SUO MOTU INVESTIGATION BY THE OFFICE OF THE DATA PROTECTION COMMISSIONER ON THE OPERATIONS OF LAKE VICTORIA FIELD OF SEVENTH DAY ADVENTIST CHURCH, HOMABAY)

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. The Office instituted a *suo motu* investigation, being ODPC Suo Motu Investigation NO. ODPC/SM/020/2025, on its own initiative and taking cognisance of the public interest generated by the Respondent'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 have 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. The Respondent is a faith-based organization that operates in Kenya and processes a considerable volume of personal data.

7. Concerns relating to the processing and use of the collected member personal data were brought to the attention of the Office by a whistleblower. The concerns included allegations that the Respondent had exported members personal data from Church Financial Management System (CFMS) to a new electronic system (e-Sadaka) developed by a third party without the consent of members. The whistleblower further alleges that the transfer violated the principle of lawfulness, fairness & transparency, and that the new system is owned and maintained by the third party.

8. Pursuant to Regulation 11 of the Enforcement Regulations, the Office notified the Respondent of the *suo moto* investigations *vide* a letter dated 26th August 2025 and referenced ODPC/CIE/CON/2/1 (583) and served upon the Respondent. In the notification, the Respondent was asked to provide this Office with the following:

    a) A response to the alleged violations made against the Respondent;
    b) The lawful basis relied upon to engage in data sharing with other/third party entities (Savannah);

KENYA VISION 2030

c) The organizations' compliance with Section 31 of the Act during the process of data migration from Church Financial Management System (CFMS) to E-sadaka developed by Savannah;

d) The organizations compliance with Section 25 of the Act as read together with Regulation 21 of the Data Protection (General) Regulations, 2021;

e) A contact person who can provide further details as regards the investigations;

f) Any relevant materials or evidence in support of the response above; and

g) The mitigation measures adopted or being adopted to address the alleged violations and to prevent such reoccurrence.

9. Despite acknowledging receipt of the notification of complaint letter on 1st September 2025, the Respondent failed, refused or neglected to provide a substantive response to the complaint as required by this Office per the notification letter sent to it.

10. This determination is therefore as a result of an analysis of the preliminary investigation by the Office and the investigations conducted by the Office.

D. NATURE OF THE INVESTIGATION

11. The Office conducted a preliminary investigation on the information and materials adduced to the Office by the whistleblower. From the adduced information and adduced materials, the allegations revolved around: -

a) Unlawful processing of member personal data contrary to Section 30 of the Act.

b) Processing of personal data contrary to the principle of lawfulness, fairness & transparency contrary to Section 25(b) of the Act.

c) Failure to notify church members of the processing activities prior to data collection contrary to Section 29 of the Act.

d) Engaging in unlawful data sharing of church members' personal data with third parties.

e) Exposing church members' personal data to advance commercial interests.

f) Engaging in high-risk processing operations, including automation, and data migration without conducting a DPIA contrary to Section 31 of the Act.

KENYA VISION 2030

g) Failure to implement appropriate technical and organizational measures contrary to Section 41 of the Act.

E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

I. THE SUO MOTO INVESTIGATION

12. According to preliminary investigations by the Office, there was potential non-compliance in the Respondent's personal data processing operations, particularly concerning the collection, use, handling, storage, and sharing of the Respondent's members' personal data within its custody as a data controller.

13. The alleged violations against the Respondent included unlawful processing of members' personal data contrary to Section 30 of the Data Protection Act, 2019; failure to uphold the principles of lawfulness, fairness, and transparency contrary to Section 25(b) of the Act; failure to inform church members of the intended processing activities prior to the collection of their personal data contrary to Section 29 of the Act; unlawful sharing of members' personal data with third parties; and the use of members' personal data to advance commercial interests.

14. Further, the Respondent was alleged to have engaged in high-risk processing operations, including automated processing and data migration, without conducting a Data Protection Impact Assessment (DPIA) as required under Section 31 of the Act, and to have failed to implement appropriate technical and organizational measures to safeguard personal data contrary to Section 41 of the Act. The alleged violations were communicated to the Respondent *vide* the notification letter dated 26th August 2025.

II. THE RESPONDENT'S RESPONSE

15. The Respondent did not submit a formal response to the Notification issued to them, despite having been granted more time to respond to the Notification as requested.

F. INVESTIGATIONS UNDERTAKEN

16. The Office conducted a site visit at the Respondent's premises on the 4th August 2026. During the site visit, the Office established the following: -

KENYA VISION 2030

a) The CFMS system was developed and owned by Isoft, a third-party private firm that offered it as Software as a Service model.

b) The Respondent was onboarded on the platform sometime in 2019 and continued to use the platform until 2025.

c) The service provider, Isoft, owned and hosted the CFMS system

d) The Respondent onboarded its members on the CFMS system for processing members' deposit receipts.

e) The Respondent did not demonstrate the lawful basis relied upon to process member details in the manner depicted.

f) There was no demonstrable contract or data sharing agreement between the Respondent and the service provider defining the obligations.

g) Upon termination of the contract in early 2025, the Respondent's access to CFMS system was revoked, and the vendor retained all member data that were domiciled in the system.

h) There was no framework guiding the retention period and secure deletion of member data processed after termination of contract with Isoft.

i) Upon termination of the engagement with Isoft, in April 2025 the Respondent engaged a different service provider, Savannah, who deployed the e-Sadaka system.

j) The Respondent subsequently migrated members' personal data to the new platform, e-Sadaka.

k) There was no demonstrable evidence of the Respondent's members having been informed of deployment and on-boarding on both systems.

l) There was no demonstrable evidence of the Respondent having conducted a DPIA for the deployment of both systems.

m) The Respondent did not demonstrate mechanisms put in place to afford members the opportunity to exercise their rights.

n) The Respondent engaged and continues to engage in unlawful data sharing with third parties.

KENYA VISION 2030

G. ISSUES FOR DETERMINATION

17. 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.

18. Upon investigations, and considering the findings as noted hereinbefore, the Office finds that the Respondent has not complied with Sections 25,29,30,31, and 41, as read together with the relevant regulations, as outlined hereunder.

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

"Every data controller or data processor shall ensure that personal data is:-

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.

20. From this Office's investigations, it emerged that upon termination of the contract with Isoft and the Respondent's access to CFMS system revoked, the Respondent did not retrieve all the members' personal data domiciled in the Isoft systems. There was no framework guiding the retention period and secure

KENYA VISION 2030

deletion of member data processed after termination of contract with Isoft. This goes against the principles of data protection as stated in Section 25 of the Act.

21. The failure to retrieve the members' personal data upon termination of the contractual relationship with Isoft, coupled with the absence of a clear framework governing the retention and secure deletion of such data, raises concerns regarding compliance with the principles of purpose limitation, data minimization and storage limitation under Section 25 of the Act. In particular, the continued retention of members' personal data within systems controlled by Isoft, without a defined retention period or documented justification for such retention, undermines the requirement that personal data be retained only for as long as is necessary for the purposes for which it was collected. Further, the absence of appropriate arrangements to ensure the secure retrieval, transfer or deletion of the data following termination of the contract exposes the personal data to the risk of unauthorised access, use or disclosure, contrary to the requirement for lawful, fair and transparent processing.

22. Accordingly, the Respondent, as the data controller, had an obligation to ensure that appropriate measures were in place to safeguard members' personal data throughout the data processing lifecycle, including upon termination of its engagement with Isoft. This obligation extended to ensuring that the contractual arrangements provided for the return, continued lawful retention and/or secure deletion of personal data held by Isoft, in accordance with the purposes for which the data had been collected and the requirements of the Act. The failure to establish such measures constitutes a shortcoming in the Respondent's

23. data governance and accountability obligations and demonstrates inadequate implementation of the data protection principles under Section 25 of the Act.

24. Section 30 of the Act of the act further provides for the lawful processing of personal data. It states as follows: -

"30. Lawful processing of personal data

KENYA VISION 2030

(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 interests 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 subsection (1) commits an offence."

25. The above section of the law places an obligation on every data controller and data processor to identify and establish a lawful basis for processing personal data. Such processing must be founded on the consent of the data subject for one or more specified purposes or any of the other lawful grounds expressly provided under Section 30(1) of the Act. Further, Section 30(2) requires that any subsequent or further processing of personal data remains consistent with the purpose for which the data was initially collected.

26. Accordingly, the processing of the Respondent's members' personal data through the CFMS system was required to be supported by a valid lawful basis, with the

KENYA VISION 2030

purposes of such processing clearly established and communicated to the affected members.

27. However, from this Office's investigations, the Respondent did not demonstrate the lawful basis upon which it relied to process members' personal data in the manner depicted, particularly following the termination of its contractual relationship with Isoft and the subsequent revocation of its access to the CFMS system. Neither did the Respondent demonstrate that the continued retention or processing of members' personal data within Isoft's systems was supported by the consent of the data subjects or any other lawful basis under Section 30(1) of the Act. In the absence of such justification, the Respondent failed to demonstrate compliance with the requirement for lawful processing under Section 30 of the Act, particularly the obligation to ensure that any further processing of personal data is consistent with the original purpose of collection.

28. Section 29 of the Act further provides for the duty to notify. It provides as follows:

"29. Duty to notify

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."

KENYA VISION 2030

29. The above provision of the Act imposes an obligation on data controllers and data processors to ensure that data subjects are adequately informed, prior to the collection of their personal data, of the circumstances and purposes surrounding such collection and processing. This includes informing data subjects of their rights under Section 26 of the Act, the purpose for which their personal data is collected, the entities to whom such data may be transferred, the applicable security measures, and the contacts of the data controller or data processor. The provision is intended to promote transparency and ensure that data subjects are sufficiently informed about how their personal data is collected, used, stored and shared, thereby enabling them to make informed decisions and exercise their rights under the Act.

30. From this Office's investigations, there was no demonstrable evidence that the Respondent informed its members of the deployment and onboarding of their personal data onto both systems (CFMS and E- Sadaka), including the purposes for which their personal data would be processed and the entities that would have access to such data. Further, the Respondent did not demonstrate that it had established mechanisms to ensure that members were adequately informed of, and afforded the opportunity to exercise, their rights as data subjects under the Act. Consequently, the Respondent failed to demonstrate compliance with its duty of notification under Section 29 of the Act, particularly the obligation to ensure transparency and accountability in its collection and processing of members' personal data.

31. Section 31 of the Act provides for the carrying out of Data Protection Impact Assessments. It provides as follows: -

"31. Data protection impact assessment

(1) Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, carry out a data protection impact assessment.

(2)A data protection impact assessment shall include the following—

KENYA VISION 2030

(a)a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor;

(b)an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects;

(d) the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights, and legitimate interests of data subjects and other persons concerned.

(3) The data controller or data processor shall consult the Data Commissioner prior to the processing if a data protection impact assessment prepared under this section indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject.

(4) For the purposes of this section, a "data protection impact assessment" means an assessment of the impact of the envisaged processing operations on the protection of personal data.

(5) The data impact assessment reports shall be submitted sixty days prior to the processing of data.

(6) The Data Commissioner shall set out guidelines for carrying out an impact assessment under this section."

32. The above provision of law places an obligation on data controllers and data processors to undertake a Data Protection Impact Assessment (DPIA) before commencing any processing operation that is likely to result in a high risk to the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing. The assessment is intended to identify and evaluate potential risks arising from the envisaged processing activities, assess the necessity and proportionality of the processing in relation to its intended purposes, and establish appropriate safeguards and security measures to mitigate the identified risks. This requirement is particularly important where the deployment of new systems involves the collection, storage, access to or sharing of substantial amounts of personal data, as it enables the data controller or processor to identify and address potential data protection risks before processing commences.

KENYA VISION 2030

33. As stated above under **F**, from this Office's investigations, there was no demonstrable evidence that the Respondent conducted a DPIA prior to the deployment and onboarding of members' personal data onto the two systems. Consequently, the Respondent failed to demonstrate that it had assessed the potential risks to members' rights and freedoms arising from the processing activities, evaluated the necessity and proportionality of the processing, or put in place appropriate safeguards to mitigate any identified risks.

34. Section 41 of the Act provides for data protection by design or by default. The section enjoins all data controllers like the Respondent herein to implement appropriate technical and organisational measures designed to implement the data protection principles in an effective manner and to integrate necessary safeguards for that purpose into the processing.

35. From this Office's investigations, it emerged that the Respondent had not implemented appropriate technical and organisational measures designed to implement the data protection principles effectively. In the present circumstances, such safeguards ought to have included measures to ensure the lawful and transparent processing of members' personal data, including clear procedures for notifying members of the purposes of processing, obtaining and documenting the appropriate lawful basis, regulating access to members' personal data, and ensuring that such data is only accessed and used for specified and legitimate purposes.

36. Further, the Respondent ought to have instituted appropriate data retention and secure deletion policies, contractual safeguards governing the handling of personal data by Isoft, as well as measures for the secure retrieval, transfer or deletion of members' personal data upon termination of the contractual relationship. These measures would give effect to the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, storage limitation, integrity and confidentiality under Section 25 of the Act.

37. The absence of these safeguards exposed members' personal data to risks of unauthorised access, inappropriate retention and processing beyond the specified purposes, thereby undermining the principles of transparency, lawfulness, purpose

KENYA VISION 2030

limitation, storage limitation, integrity and confidentiality. Accordingly, the Respondent failed to demonstrate compliance with its obligations under Section 41 of the Act.

38. From the foregoing, it is therefore our finding and determination that the Respondent is not compliant with the Act and its attendant regulations to the extent stated above.

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

39. 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.

40. Having found that the Respondent failed to fulfil their obligations under the Act and attendant regulations, 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

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

i. The Respondent is hereby found liable in respect of this *suo motu* 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 11th day of November 2026.

IMMACULATE KASSAIT, SC, MBS
DATA COMMISSIONER

KENYA VISION 2030