



**OFFICE OF THE DATA PROTECTION COMMISSIONER
ODPC COMPLAINT NO. 1099 OF 2024**

JOHN THUO KAMAU.....COMPLAINANT

-VERSUS-

THE BOARD OF KENYA MOTOR

SPORTS FEDERATION LTD.....1ST RESPONDENT

MAINA MUTURI2ND 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 against the Respondents alleging that the 2nd Respondent in his capacity as the Chairperson of the 1st Respondent federation diverged the Complainant's personal data to other third parties without the Complainant's knowledge, authority, and or 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

JK

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 26th July 2024. The complaints were lodged pursuant to Section 56 of the Act and Regulation 4 of the Enforcement Regulations.
7. The complaint was lodged against the 2nd Respondent in his capacity as the Chairperson/President of the 1st Respondent.
8. Pursuant to Regulation 11 of the Enforcement Regulations, the Office, notified the Respondents of the complaint filed against them *vide* a letter dated 31st July 2024. The Office in the said complaint notification letter requested the Respondent to furnish the Office with –
 - a) A response to the allegations made against it by the Complainant;
 - b) A contact person who can provide further details as regards the complaint;
 - c) Any relevant materials or evidence in support of its response;
 - d) The lawful basis relied upon to process the Complainant's personal data.

NT

9. In the interest of fair justice, and pursuant to Regulation 11 of the Data Protection (Complaints Handling Procedures and Enforcement) Regulations, 2021, the Office further informed the Respondents of the options of -
- a. Reviewing the complaint and summarily resolving the same to the satisfaction of the Complainant, or
 - b. Resolving the complaint through mediation, negotiation, and/or conciliation, as the alternative dispute resolution (ADR) mechanisms provided for by the Act and the Regulations.
10. The Respondents responded to the notification letter on 30th August 2024.

D. NATURE OF THE COMPLAINT

11. The Complainant alleged that the 2nd Respondent being one of the members and directors of the 1st Respondent board, upon coming into possession of his personal data which he shared with the board, diverged the said personal data to other unknown third parties without the Complainant's knowledge, authority and or consent.

E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

i. THE COMPLAINANTS' CASE

12. The Complainant stated that he notified the 1st Respondent that he would like to apply for 2 passes to the Mexico Formula One races in October for himself and his wife. He stated that he provided the passport details of himself and his wife as required by the world governing body for Motor Sports to enable them to prepare the guest passes.
13. He stated that unknown to him, the 2nd Respondent had offered the same passes to persons unrelated to motorsport, and he became aware of this when an email copied to the secretariat & to the persons was forwarded to him and it contained a pdf copy of the email he had sent to the 1st Respondent.
14. He contended that his and his wife's unredacted personal data was sent to third parties without his knowledge, authority, or consent.

15. He stated that whilst he is the 1st Respondent's alternate director when he provided his personal details, he was a data subject who believed that his personal data would not be disclosed to third parties when provided to the 1st Respondent for legitimate reasons.
16. He further contended that the 2nd Respondent's actions of forwarding a copy of privileged information that came into his possession as the 1st Respondent's director to third parties is a clear breach of the data privacy that he is entitled to.
17. To him the actions of the 1st Respondent secretariat to bring to his attention the data breach by the 2nd Respondent does not absolve it its duty to educate all the directors on the need for confidentiality of communications as required by the 1st Respondent's internal rules and regulations.

THE RESPONDENT'S RESPONSE

18. The Respondents in their response to the Complaint dated 30th August 2024, stated that the secretariat received the Complainant's email sharing his personal details from the Complainant with the authority to share the personal information of the Complainant with the FIA for issuance of the requested passes. The Respondent further stated that the email from the Complainant was copied to all directors of the federation as required by internal transparency rules.
19. The Respondents stated that the Secretariat as a whole did not share these details with anyone else apart from the party the federation was authorized to share the information with FIA.
20. The secretariat contended that it became aware of the data breach on 19th July 2024 where the personal information of the Complainant was shared by one of the directors to a third party.
21. The Respondent stated that the data breach was advised to the Complainant immediately for his information as remedial action but it did not inform the ODPC in accordance with Section 43 of the Act due to an oversight in interpreting the law.

11/1

22. The Respondent stated that the KMSF secretariat, on receipt of a notice from the Complainant that a report had been made to the ODPC, notified directors of their responsibility not to share private director communications with third parties and their responsibilities on matters related to Data protection when handling personal information, they receive as directors of the federation.

G. ISSUES FOR DETERMINATION

23. The following issues therefore 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.

24. Contextually, as it relates to this issue, the following questions arise:

- a. Did the Respondents fulfill their obligation as stipulated under Section 43 of the Act?
- b. Did the Respondent process the Complainants' personal data lawfully?

Did the Respondents fulfill their obligation as stipulated under section 43 of the Act?

25. It was the Respondents' position that once they became aware of the data breach on 19th July 2024 they informed the Complainant immediately but did not inform this Office of the same. They stated that it was an oversight on their part.

26. Section 43 of the Act provides as follows: -

43. Notification and Communication of breach

(1) where personal data has been accessed or acquired by an unauthorized person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorized access, a data controller shall:-



- a) *notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach, and*
- b) *subject to subsection (3), communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established.*
- (2) *where the notification to the Data Commissioner is not made within seventy-two hours, the notification shall be accompanied by reasons for the delay.*
- (3) *where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller without delay and where reasonably practicable, within forty-eight hours of becoming aware of such breach.*
- (4) *The data controller may delay or restrict communication referred to under subsection (1)(b) as necessary and proportionate for purposes of prevention, detection, or investigation of an offence by the concerned relevant body.*
- (5) *The notification and communication referred to under subsection (1) shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including –*
- a) *description of the nature of the data breach;*
- b) *description of the measures that the data controller or data processor intends to take or has taken to address the data breach;*
- c) *recommendation on measures to be taken by the data subject to mitigate the adverse effects of the security compromise;*
- d) *where applicable, the identity of the unauthorized person who may have accessed or acquired the personal data; and*
- e) *the name and contact details of the data protection officer where applicable or other contact point from whom more information could be obtained.*
- (6) *The Communication of a breach to the data subject shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data.*

(7) where and to the extent that it is not possible to provide all the information mentioned in subsection (5) at the same time, the information may be provided in phases without undue delay.

(8) The data controller shall record the following information in relation to a personal data breach-

a) the facts relating to the breach;

b) its effects; and

c) the remedial action taken.

27. From the above section of the Act, it is evident that in the event of any breach, a data controller ought to report the said breach within 72 hours of becoming aware of such breach. The Respondents by their own admission stated that they did not inform this Office of the said breach within the prescribed timelines.

28. As such, it is our finding that the Respondents did not comply with Section 43 of the Act. They did not fulfil their obligation contained therein.

Did the Respondent process the Complainant's personal data lawfully?

29. The Complainant contended that his and his wife's unredacted personal data was sent to third parties by the 2nd Respondent without his knowledge, authority, or consent.

30. It was the Respondent's position that the KMSF secretariat became aware of the data breach on 19th July where they discovered that the Complainant's personal information was shared by one of the directors to a third party.

31. The above averments by the Respondent is tantamount to an admission on the part of the Respondent. It is therefore evident that the Respondents jointly and severally shared the complainant's data to an unknown third party. It therefore follows that the Respondents did not process the Complainant's personal data lawfully.

32. This Office therefore finds that as far as issue no **(I)** is concerned, the Respondent did not fulfill its obligations as required by the Act.

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

33. Under 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.

34. Having considered the merits of the Complaint, the evidence adduced by both the Complainants and the Respondent, and having found that the Respondent did not fulfil its obligations as required by the Act, it therefore, follows that there has been a violation of the Act by the Respondent to that extent.

35. Section 58 of the Act as read together with Regulations 14 and 16 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 further contemplates, as a remedy, the issuance of enforcement notices against an entity that has failed or is failing to comply with any provisions of the Act and the attendant regulations thereto.

36. This Office is guided accordingly and an Enforcement Notice hereby ensues as against the Respondents.

G. FINAL DETERMINATION

37. In the ultimate, the Data Commissioner therefore makes the following final determination;

- i. The Respondents are hereby found liable.
- ii. An Enforcement Notice is hereby issued to the Respondents.
- iii. Parties have the right to appeal this determination to the High Court of Kenya within thirty (30) days.

DATED at **NAIROBI** this 19th day of October 2024.



IMMACULATE KASSAIT, MBS
DATA COMMISSIONER