

REPUBLIC OF KENYA

IN THE HIGH COURT OF KENYA AT NAIROBI

JUDICIAL REVIEW DIVISION

JUDICIAL REVIEW O.M APPLICATION NO. E366 OF 2025

KENYA UNION OF JOURNALISTS.....APPLICANT

VERSUS

KENYA BROADCASTING CORPORATION.....RESPONDENT

JUDGMENT

1. Before this Court for determination is the Originating Motion dated 20th November, 2025 brought under certificate of urgency, under the provisions of Articles 22, 23 and 47 of the Constitution, sections 2,4, 7 and 11 of the Fair Administrative Action Act and Rules 11,13 and 14 of the Fair Administrative Action Rules, 2024.

2. The Applicant seeks, inter alia:

4. *Under Article 23 of the Constitution, the court does grant the following or other appropriate judicial review reliefs:*

i. *A declaration that the introduction and rollout of the Biometric Attendance system without obtaining the consent of the data subjects; Mailing to provide any pertinent information to the data subjects on the processing of their data; ignoring the data*

subjects' objections and concerns on the processing of their data; and failing to carry out a Data Protection Impact Assessment prior to the rollout of the system violates Article 31 of the Constitution and Sections 25, 26, 29, 30,31, 32 and 36 of the Data Protection Act, 2019 and Regulations 4, 25(c) and (d), 30,and 36(a) (b) (d) of Data

Protection (General) Regulations.

- ii. A declaration that the refusal of the Respondent to engage the Data subjects in any consultation despite repeated requests for meaningful engagement prior to the rollout violates Article 10(2)(a) of the Constitution which requires public participation in crucial decision making.*
- iii. A declaration that the refusal of the Respondent to provide information relating to the use of the system and processing of data violates the data subjects' right to information under Article 35 (2) of the Constitution.*
- iv. A declaration that the Respondent's refusal to provide any pertinent information regarding the identity and procurement of the systems service provider, the manner in which the system supplier was contracted to provide the service, as well as a*

confirmation of whether they are licensed either as a Data Controller or Processor violates the principles of good governance, integrity, transparency and accountability required of public institutions under Article 10(2)(c) of the Constitution of Kenya, 2010.

- v. *An order of prohibition do issue restraining the Respondent from implementing the decision to rollout the Biometric Attendance System requiring all its staff to register their attendance by use of facial recognition, without obtaining the consent of the staff as data subjects; without providing pertinent information to the data subjects on the processing of their data; ignoring the data subjects' concerns and objections to the processing of their data; and without procuring a Data Protection Impact Assessment in violation of Sections 26,29,30,31, 32 and 36 of the Data Protection Act, 2019 and Regulations 4, 25(c) and (d), 30,and 36(a) (b) (d) of Data Protection (General) Regulations.*
- vi. *An order of certiorari do issue quashing the decision of the Respondent to rollout the Biometric Attendance System without obtaining the consent of the employees to the use and*

processing of their data; without providing any information to the employees on the processing of their data; ignoring the employees objections and concerns to the use of their data in the exercise, and without undertaking a Data Protection Impact Assessment in violation of Sections 26,29,30, 31 and 36 of the Data Protection Act, 2019 and Regulations 4, 25(c) and (d), 30, and 36(a) (b) (d) of Data Protection (General) Regulations.

vii. An order of mandamus do issue compelling the Respondent to erase and destroy the personal biometric data collected from the data subjects which are now in the hands of an unknown third party, having been unlawfully obtained.

viii. Costs of the application be borne by the Respondent.

3. The application is premised on the grounds on the face of the application and the affidavit in support sworn by Eric Oduor, the Secretary General of the Kenya Union of Journalists, the applicant herein, suing on behalf of the journalists employed and working for the Respondent Kenya Broadcasting Corporation-KBC, a state parastatal/ corporation established under section 3 of the Kenya Broadcasting Corporation Act, Cap 221 of the Laws of Kenya.
4. The Applicant's case is contained in the founding facts and constitutional and statutory grounding set out by the applicant in the Originating motion.

Summative, that the introduction and implementation of the facial biometric attendance system by the respondent, and enforced upon all its employees vide a memo Ref KBC/MD/2/5/C announcing its decision to introduce the mandatory biometric attendance system, coupled with the use of facial recognition to record the time and attendance, violated the employees' constitutional right to privacy and protection of personal data under Article 31 of the Constitution and Section 25 of the Data Protection Act.

5. It is asserted that none of the employees' consent was sought and obtained prior to the introduction of the impugned system and that neither were the employees informed of the safety of the said system and or possible violation of their rights and especially the rights of cancer patients within the Respondent institution.
6. That despite the applicant writing to the Respondent raising concerns of the roll out of the system in issue and calling for a consultative meeting with the respondent, in July 2025, the respondent ignored the concerns raised in the latter dated 3/7/2025 and on September 9th, 2025 vide a memo KBC/PERS/1/100 communicated to staff of the successful installation of the system ready for use from 15th September, 2025.
7. That the applicant wrote another letter protesting the use of the installed device and the respondent is alleged to have instead pretended to be

engaging the applicant only for it to fully demand compliance by all staff before engaging stakeholders on the concerns raised by the applicant.

8. That on 13th October 2025, the applicant again wrote to the respondent protesting and demanding the suspension of the use of the system to allow consultations and information to ensure necessary safeguards are in place in accordance with the Data Protection Act but that to date, the respondent has not supplied the requested information.
9. The applicant avers that no Data Protection Impact Assessment (DPIA) was undertaken; that no public participation or stakeholder consultation took place; and that the identity, capacity and security credentials of the procured system and its unknown third-party handlers were not disclosed.
10. The Applicant thus seeks the erasure of biometric data already collected and protection of its members from continued unlawful data processing thereby denying them autonomy over their personal sensitive data.
11. When the matter came up for inter partes mention this morning, on the question of whether a conservatory order staying the implementation of the directive that all the members of the applicant Union use the facial biometric system, learned counsel for the Respondent, Ms Kwang'a informed the Court that the Respondent does not oppose the application. Counsel unequivocally confirmed that the Respondent is in the process of

undertaking full compliance with the Data Protection Act, including conducting a DPIA, and was amenable to any orders or directions that the Court deemed just. The Respondent therefore conceded the application in its entirety.

Issues for Determination

12. In view of the concession by the Respondent, the issues that remain for determination are:

- a. Whether the impugned decision and implementation of the facial biometric system violated constitutional and statutory requirements; and*
- b. What orders are appropriate in the circumstances, including orders for costs, if any.*

Analysis and Determination

13. Article 31 of the Constitution guarantees every person the right to privacy, including the right not to have information relating to their family or private affairs unnecessarily revealed. Processing of facial biometric data constitutes processing of sensitive personal data, which under the Data Protection Act demands heightened safeguards, including a mandatory Data Protection Impact Assessment where such processing poses a high risk to data subjects.

14. The Applicant has demonstrated, and the Respondent has not disputed, that no DPIA preceded the roll-out of the system.
15. Section 31 of the Data Protection Act makes such an assessment mandatory in circumstances involving new technologies and sensitive data.
16. The Applicant's further averments that no consultation, disclosure, or transparency measures were undertaken in the procurement of the subject biometric system remain unchallenged.
17. In addition, Article 10 of the Constitution obliges public bodies to uphold public participation, transparency, accountability and the rule of law in decision-making. The alleged but uncontroverted unilateral and opaque adoption of a facial biometric surveillance tool on employees of the respondent who are data subjects and without obtaining their informed consent no doubt falls short of these standards.
18. Since the Respondent conceded the application and expressed willingness to comply with the law, meaning it has reflected on the impact of its decision, this Court is left with undisputed evidence of procedural and substantive irregularities. The remedy of judicial review is therefore merited, being a constitutional remedy under Article 23 of the Constitution, for violation of constitutionally guaranteed rights.

19. The Respondent's concession also aligns with its statutory obligations and the constitutional imperative to respect, protect and promote the right to privacy. This Court therefore expects strict and demonstrable compliance with the Data Protection Act going forward.

20. Before concluding on this matter, this Court finds it necessary to observe that it is deeply perturbed by the continuing disregard of constitutional and statutory safeguards governing the collection and processing of personal data. It is surprising and indeed troubling, that even after the clear pronouncements made in **Republic v Tools for Humanity Corporation (US) & 8 others; Katiba Institute & 4 others (Ex parte Applicants); Data Privacy & Governance Society of Kenya (Interested Party) (Judicial Review Application E119 of 2023) [2025] KEHC 5629 (KLR) (Judicial Review) (5 May 2025) (Judgment)** the *Worldcoin judgment*, institutions and public bodies like the respondent herein, would dare harvest subjects' sensitive biometric data without informed consent, without transparency and in patent breach of the Data Protection Act and Article 31 of the Constitution.

21. The right to privacy is not aspirational; it is a firm constitutional guarantee and therefore, entities that deploy intrusive technologies such as facial recognition or biometric capture must adhere strictly to the mandatory

requirements of conducting Data Protection Impact Assessments, ensuring informed consent, providing full disclosure and adopting robust safeguards. Anything less amounts to an unconstitutional intrusion and an unlawful violation of the very rights that the Constitution obliges all state and private actors to respect, protect and uphold.

22. The respondent is therefore guided to read the *Judgment in the World Coin* case on the limits to sensitive data collection and processing.

23. Consequently, and in view of the Respondent's express concession, this Court hereby makes the following orders:

a. A declaration is hereby issued declaring that the introduction and rollout of the Biometric Attendance system without obtaining the consent of the data subjects; Mailing to provide any pertinent information to the data subjects on the processing of their data; ignoring the data subjects' objections and concerns on the processing of their data; and failing to carry out a Data Protection Impact Assessment prior to the rollout of the system violates Article 31 of the Constitution and Sections 25, 26, 29, 30, 31, 32 and 36 of the Data Protection Act, 2019 and Regulations 4, 25(c) and (d), 30, and 36(a) (b) of Data Protection (General) Regulations.

- b. A declaration is hereby issued declaring that the refusal of the Respondent to engage the Data subjects in any consultation despite repeated requests for meaningful engagement prior to the rollout violates Article 10(2)(a) of the Constitution which requires public participation in crucial decision making.***
- c. A declaration is hereby issued declaring that the refusal of the Respondent to provide information relating to the use of the system and processing of data violates the data subjects' right to information under Article 35 (2) of the Constitution.***
- d. A declaration is hereby issued declaring that the Respondent's refusal to provide any pertinent information regarding the identity and procurement of the systems service provider, the manner in which the system supplier was contracted to provide the service, as well as a confirmation of whether they are licensed either as a Data Controller or Processor violates the principles of good governance, integrity, transparency and accountability required of public institutions under Article 10(2)(c) of the Constitution of Kenya, 2010.***
- e. An order of prohibition do is hereby issued restraining the Respondent from implementing the decision to rollout the Biometric***

Attendance System requiring all its staff to register their attendance by use of facial recognition, without obtaining the consent of the staff as data subjects; without providing pertinent information to the data subjects on the processing of their data; ignoring the data subjects' concerns and objections to the processing of their data; and without procuring a Data Protection Impact Assessment in violation of Sections 26,29,30,31, 32 and 36 of the Data Protection Act, 2019 and Regulations 4, 25(c) and (d), 30,and 36(a) (b) (d) of Data Protection (General) Regulations.

- f. An order of certiorari is hereby issued removing into this court for purposes of quashing and I hereby quash the decision of the Respondent to rollout the Biometric Attendance System without obtaining the consent of the employees to the use and processing of their data; without providing any information to the employees on the processing of their data; ignoring the employees objections and concerns to the use of their data in the exercise, and without undertaking a Data Protection Impact Assessment in violation of Sections 26,29,30, 31 and 36 of the Data Protection Act, 2019 and Regulations 4, 25(c) and (d), 30, and 36(a) (b) (d) of Data Protection (General) Regulations.*

- g. An order of mandamus is hereby issued compelling the Respondent to delete, erase and destroy the personal biometric data collected from the employees data subjects which are now in the hands of an unknown third party, having been unlawfully obtained.*
- h. An order of Mandamus is hereby issued compelling the Respondent to forthwith delete, erase and destroy all biometric data already collected from the Applicant's members through the said impugned system from the date of the roll out to date and to file in Court, within 30 days of this judgment, an affidavit confirming compliance, including details of the measures undertaken to ensure that no copies of such data remain with any third party.*
- i. In implementing Order No. h above, the Data protection Commissioner, who is responsible for regulation of data protection and privacy in the Country is hereby directed to supervise the deletion, erasure and destruction of all data collected from the data subjects and stored by the respondent using the facial biometric attendance system from the date of deployment of the said system and to report to this Court such erasure and the supervision thereof shall be in the presence of the applicant's representatives.*

j. On costs, as the respondent has conceded to these proceedings thereby saving on the time and costs, I order that each party shall bear their own costs of the originating Motion.

- a. This matter shall be mentioned on 21/1/2026 to confirm compliance with the above orders regarding deletion and erasure of the data collected from the respondent's employees in violation of the right to data privacy.

Dated, Signed and Delivered at Nairobi this 25th Day of November, 2025

**R.E. ABURILI
JUDGE**