CM ADVOCATES LLP

DATA PROTECTION IN THE WORKPLACE: EMPLOYEE ACCESS TO CUSTOMER DATA

The Data Protection Act, 2019 imposes obligations on data controllers not only in relation to external threats, but also with respect to internal handling of personal data by their own employees.

Where an employee accesses customer data without authorisation and shares it with an unauthorised third party, the employer is exposed to both reputational and regulatory risk.

The recent judgment in **Wenani v Safaricom Limited & another, Cause E243 of 2024 [2025] KEELRC 3628 (KLR)** delivered by the Employment and Labour Relations Court on 11 December 2025, illustrates the intersection of data protection obligations and employment law and confirms that an employer acts lawfully in summarily dismissing an employee who breaches its data protection policy.

Background

The Claimant, Dennis Wenani, was employed by Safaricom Limited as a Customer Experience Executive.

On 10 January 2024, he accessed a customer's M-Pesa account without authorisation at the request of a third party, Gordon, who claimed to be verifying a money transfer.

The Claimant failed to record the interaction as required by Safaricom's internal procedures and subsequently shared the customer's M-Pesa statement with Gordon — an individual with no job-related need to access that information.

Following an investigation, the Claimant was suspended and issued with a show-cause letter.
He was then invited to a disciplinary hearing, after which he was summarily dismissed on 9 February 2024 for gross misconduct, including breach of Safaricom's Data Protection Policy and Information Security Acceptable Usage Policy.

The Claimant challenged his dismissal at the Employment and Labour Relations Court, seeking a declaration of unfair termination and damages of Kshs. 1,326,000.

Determination

On the substantive question, the Court grounded its analysis firmly in data protection principles. The Claimant, had been entrusted with privileged access to customer data held by Safaricom access that carried with it a corresponding duty of care under both Safaricom's internal policies and the broader data protection framework. That duty was breached on two distinct counts.

First, the Claimant accessed a customer's M-Pesa account without authorisation and without a legitimate work-related purpose, in violation of Safaricom's Information Security Acceptable Usage Policy a policy he had personally signed and committed to upholding. Under clause 3.1 of that policy, all access to information was required to be authorised. The Claimant could not demonstrate any such authorisation.

Second, and more critically, the Claimant shared the customer's M-Pesa statement with Gordon, an unauthorised third party who had no job-related need to access that information. This directly contravened Safaricom's Data Protection Policy, which consistent with the principle of purpose limitation and the need-to-know standard permits the sharing of personal data only with persons who have a legitimate, job-related reason to receive it.

M-Pesa transaction records constitute personal data, and their disclosure to an unauthorised party amounted to an unlawful disclosure under that policy.

The Court rejected the Claimant's argument that his actions did not constitute gross misconduct. Even accepting that the initial access was inadvertent, the Court found that the Claimant made a deliberate choice to share the data with a third party a choice he made despite knowing, as he conceded under cross-examination, that he was not authorised to share data externally.

The Court was unequivocal: the fact that the two customers purportedly knew each other provided no lawful basis for disclosure. Convenience and familiarity are not recognised grounds for processing personal data.

Applying Sections 43 and 45 of the Employment Act, the Court was satisfied that Safaricom had established, on a balance of probabilities, a fair and valid reason for termination rooted in the Claimant's conduct. It further noted that the breach exposed Safaricom to both reputational harm and legal liability a consideration that underscores why organisations cannot afford to treat internal data protection violations as merely administrative infractions.

On procedural fairness, the Court found that Safaricom had fully complied with Section 41 of the Employment Act. The disciplinary process included: a 30-day suspension with full pay to allow for conclusive investigations; a show-cause letter setting out the specific charges, accompanied by the investigation report; a disciplinary hearing with adequate notice and the right to representation by a fellow employee; and formal notification of the right to appeal within 10 working days. The Court was satisfied that each requirement had been met. The claim was accordingly dismissed in its entirety, with no order as to costs.

Conclusion

This judgment affirms that a data protection breach by an employee can constitute valid grounds for summary dismissal, provided the employer follows fair procedure.

For organisations operating in data-intensive environments particularly those in the financial services and telecommunications sectors the decision underscores the need for robust data protection policies, clear access controls, and documented disciplinary procedures.

Employees with privileged access to customer data carry heightened obligations, and employers are entitled to enforce those obligations firmly.

The case also demonstrates that an employer need not secure a criminal conviction before taking disciplinary action; the applicable standard is whether there was a genuine and reasonable belief in the misconduct at the time of termination.

How Can We Help?

For Further Guidance

CM ADVOCATES LLP – Technology, Media & Telecommunications (TMT), Data Protection & Cybersecurity Practice

Email: law@cmadvocates.com

Head Office – Nairobi
I&M Bank House, 7th Floor, 2nd Ngong Avenue

Visit us: www.cmadvocates.com

CONTRIBUTOR

Joyce Mwaura,
Associate Advocate - Data Protection
Email : jmwaura@cmadvocates.com
CM Advocates LLP