The Limits of Institutional Discretion in Data Processing: A Critical Analysis of the ODPC Determination in Merceline Akoth Odeyo v St. Luke Orthopaedic & Trauma Hospital Eldoret

Article by Benjamin Neto

The processing of personal data is an essential aspect of modern commerce and service delivery, particularly in the healthcare sector where institutions routinely handle sensitive patient information. However, the autonomy of organizations to process personal data is not absolute. Article 31 of the Constitution of Kenya, 2010 guarantees every person the right to privacy, including the right not to have information relating to their family or private affairs unnecessarily revealed.

To give effect to this constitutional right, Parliament enacted the Data Protection Act Cap. 411C. Section 5 of the Act establishes the Office of the Data Protection Commissioner (ODPC), which is mandated to regulate the processing of personal data, enforce compliance with data protection principles, and safeguard the rights of data subjects. Consequently, any processing of personal data that undermines the right to privacy must yield to constitutional and statutory safeguards.

The ODPC in *Complaint No. 2125 of 2025; Merceline Akoth Odeyo v St. Luke Orthopaedic & Trauma Hospital Eldoret* (16th March 2026) illustrates the boundaries of data processing autonomy among organizations in our country. In this case, the Complainant sought medical services at the Hospital on several occasions. On two separate visits, she was issued medical results belonging to an unrelated third party who only shared a similar first name but had a different surname. Further, the Hospital

transferred the Complainant's sensitive health samples and medical data to a third-party laboratory for testing without informing her and obtaining her explicit consent. The Hospital attributed the incident to human error during data reconciliation and only sought clarification from the laboratory after the mix-up had been discovered.

Upon considering the complaint, the ODPC found that the Hospital had violated several provisions of the Data Protection Act and ordered it to compensate the Complainant with Kenya Shillings Five Hundred and Twenty-Five Thousand (KES 525,000) affirming that organizations may process personal data in the course of service delivery, such processing must remain within the confines of constitutional and statutory safeguards.

Lawful, Fair, and Transparent Processing of Data

Section 25 of the Data Protection Act, 2019 establishes the principles governing the processing of personal data in Kenya. The provision requires every data controller or processor to ensure that personal data is processed in accordance with the right to privacy of the data subject; lawfully, fairly, and transparently; and only for explicit, specified, and legitimate purposes. The Act further requires that personal data be adequate, relevant, limited to what is necessary, accurate, and retained only for as long as necessary. Additionally, personal data must not be transferred outside Kenya without adequate safeguards or the consent of the data subject.

These principles emphasize transparency, accountability, accuracy, necessity, and the protection of data subject rights throughout the processing cycle. In the present case, the Hospital's failure to adequately inform the Complainant before transferring her sensitive health data to a third-party laboratory constituted a clear breach of the principles of lawful, fair, and transparent processing. The ODPC correctly held that the existence of a Data Sharing Agreement between the Hospital and the laboratory did not absolve the Hospital of its obligation to notify the data subject and obtain her consent.

Informed Consent and Sensitive Health Data

The Data Protection Act requires personal data to be processed only where the data subject has given freely informed consent or where another lawful basis exists under Section 30(1)(b). Importantly, the Act sets the conditions of consent under section 32 granting the data subject the right to withdraw the consent at any particular point. However, the data subject's withdrawal shall not affect lawfulness use of processing based on prior consent. Accordingly, the burden lies with the data controller or processor to demonstrate that the data subject was informed of and understood the purpose for which the data was being processed.

Importantly, health data is sensitive in nature, it receives enhanced protection under the law. Health data includes information relating to the physical and/or mental health of a data subject, including healthcare records and sourced information. Section 44 restricts the processing of sensitive personal data unless strict legal requirements are met, while Section 46 specifically regulates the processing of personal health information.

In this case, the Hospital transferred the Complainant's medical information to a third-party laboratory without obtaining proper informed consent. This constituted a direct violation of the statutory requirements governing the processing of sensitive health data. The determination therefore reinforces the principle that administrative convenience or assumptions cannot replace the requirement for explicit and informed consent.

Accuracy and Security of Personal Data

The Act further obligates data controllers and processors to ensure that personal data is accurate, up to date, and protected through appropriate technical and organizational measures. The repeated issuance of another person's medical results to the Complainant exposed significant deficiencies in the Hospital's data accuracy and reconciliation systems.

The ODPC found that these repeated administrative errors demonstrated inadequate technical and organizational safeguards, amounting to a breach of Section 41 of the Act. The determination highlights the legal obligation placed on organizations to establish robust internal systems capable of preventing unauthorized disclosure and ensuring the integrity and accuracy of personal data.

Conclusion

The determination in *Merceline Akoth Odeyo v St. Luke Orthopaedic & Trauma Hospital Eldoret* illustrates the limits of data processing autonomy in Kenya by institutions. While organizations may process personal data in the course of their operations, that autonomy is qualified by constitutional protections, statutory obligations, and regulatory oversight.

Healthcare institutions and other data controllers cannot justify breaches of data protection principles on the basis of administrative convenience or human error. The law requires proactive compliance through transparent processing practices, accurate data management systems, explicit consent mechanisms, and robust security safeguards.

Ultimately, the rights of data subjects take precedence over organizational convenience. The ODPC remains central in enforcing these standards and ensuring accountability where personal data is mishandled. It is proper for organizations to note that compliance with data protection obligations is not optional, but a legal imperative backed by meaningful sanctions.

DISCLAIMER:

This Legal Alert is provided strictly for informational and educational purposes and does not constitute legal advice or create an advocate-client relationship. Readers should not rely on its contents as a substitute for professional legal guidance, as succession matters and legal disputes depend on the specific facts and applicable law in each case. No legal action or decision should be taken solely on the basis of this publication without first seeking advice from a qualified advocate. For tailored legal guidance on wills, succession, estate planning, or probate disputes, kindly consult a licensed legal practitioner or contact our office for professional assistance.