

Ad Legal International Ltd v WhatsApp LLC & Meta Platforms, Inc.: A Commentary

An Analysis of the Personal Data Protection Office's Landmark Decision of 20th February 2026

February, 2026

On 20th February 2026, Uganda's Personal Data Protection Office (PDPO) delivered a watershed ruling in **Adlegal International Ltd v WhatsApp LLC & Meta Platforms, Inc. (Complaint No. PDPO 086/2025)**, finding that WhatsApp's practices as laid out in its January 2021 Privacy Policy update violated multiple provisions of the Data Protection and Privacy Act, Cap. 97. The PDPO issued comprehensive remedial orders requiring WhatsApp to overhaul its Uganda-facing privacy documentation, demonstrate compliance with cross-border transfer safeguards, and conduct a Data Protection Impact Assessment on intra-group data sharing. This commentary examines the decision, its reasoning, and its implications for data protection in Uganda.

A. Background

The Complainant, Adlegal International Limited, filed a complaint in the public

interest on behalf of Ugandan WhatsApp users. The complaint alleged that WhatsApp's 2021 Privacy Policy update and related practices contravened Ugandan data protection law in several respects: failing to obtain freely given, informed, and explicit consent for sharing user data with Meta; collecting personal data beyond what is strictly necessary for providing the messaging service; affording Ugandan users materially weaker transparency than users in other jurisdictions; and transferring personal data outside Uganda without demonstrating compliance with **Section 19 of the Act**.

The PDPO required the Respondents to file responses and both WhatsApp LLC and Meta Platforms, Inc. filed substantive responses, with Meta separately challenging its inclusion as a respondent.

B. Issues for Determination

PDPO framed seven issues for determination:

1. Whether Meta Platforms, Inc. was properly joined as a respondent.
2. Whether the January 2021 Privacy Policy afforded users a meaningful opportunity to consent and obtained valid consent where required.
3. Whether the Policy permitted excessive data collection and unlawfully bundled non-essential processing.
4. Whether WhatsApp's conduct constituted harm by undermining users' ability to exercise meaningful control over their data.
5. Whether the Respondents complied with Section 19 of the Act and Regulation 30 on cross-border data transfers.
6. Whether WhatsApp subjected Ugandan users to disparate treatment compared to users in other jurisdictions.
7. Whether the Complainant was entitled to the orders and remedies sought.

C. The Decision

The decision of the PDPO is highlighted with the following key findings:

- i. Public Interest Litigation is applicable to Data Protection violation matters:** The Act allows parties to file complaints with the PDPO in the public's interest under Section 31(1) of the Act read together with Regulation 41(1)(a) of the Regulations where they have reason to believe that a contravention of the Act has occurred.
- ii. Meta's Joinder to the Complaint:** Applying a functional test, PDPO found that while WhatsApp LLC is the primary

data controller for WhatsApp Messenger, Meta receives and processes Ugandan user data as part of intra-group sharing and infrastructure arrangements. Meta was therefore retained as a respondent for the limited purpose of ensuring effective implementation of remedial directions concerning intra-group disclosures and cross-border safeguards, though no adverse findings were made against Meta as a primary data controller.

iii. Lack of Transparency and Consent:

PDPO found that while intra-group sharing was disclosed, the policy failed to correlate specific data categories with specific purposes and lawful bases in a structured and intelligible manner. The update mechanism did not provide a differentiated opportunity for users to accept or decline ancillary intra-group sharing separately from acceptance of the Terms of Service. To the extent that ancillary processing ought to have relied on consent, valid consent was not demonstrated.

iv. Data Minimisation and Bundling of Personal Data:

PDPO distinguished between core messaging data which is indispensable to service operation and broader ecosystem-level processing for analytics, integration across Meta products, personalization, etc. While core messaging and security-related data collection were found proportionate, ongoing usage analytics and ecosystem-level integration processing presented without clear structural differentiation constituted non-compliance with the data minimisation and purpose limitation requirements of Sections 3(1)(c) and 14 of the Act.

v. Harm and User Control: While no demonstrable material injury was established, the structural deficiencies identified, blending essential and ancillary processing, unclear lawful basis correlation, materially impaired the statutory conditions necessary for informed and differentiated user control. PDPO held that this constituted an infringement of the Act, though limited to impairment of statutory conditions and interference with user autonomy rather than extending to demonstrable material injury.

vi. Cross-Border Data Transfers: PDPO adopted a functional interpretation of "transfer," holding that it includes any situation where personal data collected from Ugandan data subjects is processed or stored in a foreign jurisdiction whether through direct upload to overseas servers, remote hosting, or shared infrastructure operations. While applying the extra-territorial application established in ***Ssekamwa Frank & 3 Ors v Google LLC***, PDPO found that WhatsApp LLC falls within the scope of Section 19 which requires them to abide by the crossborder requirements set in the Act. Critically, the Respondents failed to demonstrate adequacy or appropriate safeguards for cross-border processing, with no documented adequacy assessment or structured demonstration of enforceable rights for Ugandan data subjects provided.

vii. Disparate Treatment: PDPO clarified that it was not making a finding of constitutional discrimination on prohibited grounds. However, it found that Ugandan users received materially weaker structured transparency than

users in other jurisdictions, pointing to concrete structural features present in documentation for other regions such as the European region which has a tabular correlation of processing activities, explicit identification of the right to object, layered disclosures, among others that were absent in substantively equivalent form in the Uganda-facing documentation. This disparity was held to be evidence of unfair and insufficiently transparent processing.

viii. Remedies: PDPO declined to grant the Complainant's most disruptive prayers such as immediate cessation of all intra-group sharing, holding that these exceeded the scope of established contraventions. Instead, it issued targeted remedial orders requiring WhatsApp to:

- Revise the Uganda-facing Privacy Policy to clearly correlate data categories, specific purposes, lawful bases, and recipients within 90 days.
- Implement clear structural differentiation between essential and ancillary processing, with granular opt-in mechanisms for ancillary processing relying on consent.
- Submit a documented adequacy and safeguard assessment under Regulation 30 within 90 days.
- Conduct and submit a Data Protection Impact Assessment addressing intra-group sharing.
- Prepare Legitimate Interests' Assessments for any processing relying on that lawful basis.

D. Implications of the Decision

This decision carries profound implications for data controllers operating in Uganda, particularly multinational companies:

- i. **Sound warning to Big Tech and Multinationals:** Big tech firms operating in growing economies like Uganda often apply weaker compliance mechanisms than in upscale jurisdictions such as in Europe, assuming lower scrutiny. This decision confirms that African regulators will not overlook such disparities in transparency, accountability and equitable practices. PDPO's decision aligns with similar enforcement against tech giants in Nigeria, Ethiopia, Kenya and Ghana, which is collective pressures continent-wide or risk facing fragmented sanctions.
- ii. **Registration is Foundational but Insufficient on its own to Prove Compliance:** Registration is only the first step in compliance. However, it is not conclusive. The Act provides for ongoing and continuing obligations that entities must observe to protect users' personal data. Both Respondents, Whatsapp LLC and Meta Inc. are registered with the PDPO under certificate numbers; PDPO-202512-9548 and PDPO-202512-9547, having duly registered in December 2025. Yet, this did not shield them from findings of substantive non-compliance. This applies universally: many controllers proceed to draft boilerplate policies merely to complete registration and tick the compliance requirement of such policies, hence ignoring the internal data flows. Data controllers ought to understand that registration only marks the start of accountability, and they are

expected to set up internal systems that ensure ongoing compliance with the data protection laws.

The PDPO also clarified that the Act does not require a complainant that collects or processes personal data to be registered with the PDPO before filing a complaint. To that extent, the PDPO noted that Adlegal International was not registered while WhatsApp and Meta were, implying that the complainant had not formally anchored itself within the accountability structure it was invoking against the respondents. The PDPO noted this but did not treat it as a violation in its findings, even though non-registration is a breach of section 29 of the Act and regulation 15.

In **Frank Sekamwa & 3 Others v Google LLC**, the PDPO expressly pronounced non registration to be a violation of the Act. Although Google was a respondent and not the complainant in that case, the statutory obligation remains the same. For the sake of consistency, once the PDPO identified Adlegal's non registration, it could similarly have made a clear finding of non compliance and made orders to that effect, even if that did not bar the complaint itself. Perhaps, had Meta or WhatsApp raised the issue more directly, the PDPO might have been prompted to address Adlegal's non compliance in the same manner as it did in the Google decision.

- iii. **Privacy Policies Must Be Structured, Not Mere Disclosures:** The PDPO has set a new benchmark for transparency which aligns within privacy policies requiring that they correlate data categories, purpose, and lawful bases intelligibly. The provision of broad, composite

purpose statements will no longer suffice. It's also noteworthy that most data subjects do not read these privacy policies but this shouldn't stop data controllers from having fully compliant policies in place.

iv. Differentiation of Essential and Ancillary Processing is Mandatory:

Controllers must clearly distinguish between processing strictly necessary for core service functionality and ancillary processing rather than merely bundling these together to the detriment of data subjects. Ancillary processing requires consent and as such granular, purpose-specific opt-in mechanisms are required, separate from core services terms, preventing coerced acceptance and restoring user autonomy.

v. Cross-Border Transfers Require Demonstrable Safeguards:

The functional definition of "transfer" closes any loophole for controllers who might argue that direct user uploads or global infrastructure operations fall outside Section 19. Controllers must maintain documented adequacy assessments or safeguard analyses specifically addressing Ugandan law, not merely rely on mechanisms recognised in other jurisdictions. Even the referral to other jurisdictions ought to point out the rights conferred to Ugandan citizens whose data is transferred under those laws, among others. It's also notable that the PDPO is yet to release a white list with countries considered to have measures safe for the transfer of the personal data of Ugandans.

vi. "Structural Harm" is Cognizable: The PDPO's recognition that impairment of statutory conditions for user control

constitutes an infringement and the absence of material injury doesn't guarantee that absence of procedural deficiencies with the ability to attract regulatory sanction. Controllers cannot defend opaque practices by arguing that no user has yet suffered quantifiable harm.

vii. Disparate Treatment Invites Scrutiny:

Where controllers provide richer transparency or stronger safeguards in other jurisdictions, the absence of substantively equivalent protections for Ugandan users will be treated as evidence of unfair processing. The "different legal regimes" defence has limits where operational capacity for better transparency exists. Multinationals tend to set their compliance standards based on the stringiness of the host nations where they're operating which in aspects of data protection turns out to be unfair to the data subjects.

viii. Parent Companies' Responsibility in Subsidiary Companies' Data Privacy Violation Proceedings:

Another key implication emerging from the PDPO's decision is that parent companies may be procedurally implicated in data protection proceedings arising from a subsidiary company's data collection and processing activities, even where they are not found to be data controllers. In that regard, the PDPO found that Meta Inc., though legally separate from Whatsapp LLC, was a necessary party to the proceedings for the limited purpose of enabling remedial effectiveness rather than as an entity bearing substantive liability for the alleged violations

An alternative basis for Meta's involvement lies in its possible qualification as a data processor in relation to the personal data collected by WhatsApp.

Section 1 of the Act defines a data processor as *"a person other than an employee of the data controller who processes the data on behalf of the data controller."* Based on this definition, Meta fits the statutory elements of a processor when it provides infrastructure, data storage and other processing services for WhatsApp.

Meta is not an employee of WhatsApp, it processes personal data such as IP addresses, usage logs, media and device information, and it does so entirely under WhatsApp's instructions as the data controller. WhatsApp's January 2021 Privacy Policy expressly confirms that "WhatsApp uses Meta's global infrastructure and data centers..." This intra-group sharing gives rise to Meta's processing role, as it receives personal data from WhatsApp for purposes such as cross-platform integration, service improvement and infrastructure maintenance.

Thus, in addition to the remedial effectiveness justification made by the PDPO for Meta's joinder to the proceedings, its involvement in the WhatsApp ecosystem as a data processor further supports the argument for its inclusion as a party to the proceedings.

In addition to data controllers, the determination also has the following implications for complainants.

ix. Persons Entitled to make Complaints

under the Act: The PDPO found that the right to lodge complaints under the Act is not limited to affected individuals. Any person who reasonably believes that a data controller, collector or processor is violating provisions of the Act may make a complaint in the interest of the affected persons such as the general public.

This aligns with the previous trends in the complaints filed under the Act. For instance, the Safe boda complaint which saw civil society organisation Unwanted Witness bring a claim against Guinness Transporters (trading as Safe Boda) for sharing users' personal data to third parties without their consent. Unwanted Witness, as an entity, was not, in its own capacity, affected by the violations of Safeboda, but made the complaint in the interest of Ugandans who used Safeboda's services.

E. Relationship with the Google Decision

This decision builds upon and significantly extends the principles established in *Ssekamwa Frank & 3 Ors v Google LLC* decided by the PDPO on 18th July 2025, and the first sounding check onto Big Tech by the Ugandan regulator. While the Google decision focused on establishing foundational accountability hence ordering registration and requiring demonstration of a compliance framework for cross-border transfers, this WhatsApp ruling delves into substantive continuing compliance focusing on the quality of transparency, the validity of consent, the proportionality of data collection, and the adequacy of cross-border safeguards. Together, these decisions demonstrate the PDPO's evolution from ensuring controllers are identifiable to scrutinizing how they process data. The

Google case established that multinationals operating in Uganda cannot avoid registration obligations which this WhatsApp decision confirms that registration alone is insufficient and that the substance of privacy practices will be rigorously examined.

F. Conclusion

This decision represents a sophisticated and technically informed exercise of regulatory authority, one that is an addition to other decisions taken by data protection regulators in other African countries including Nigeria, Kenya, Ghana and Ethiopia against Big Tech. The remedial orders issued are proportionate to the contraventions found and establish clear, actionable

compliance benchmarks. The key question now is enforcement: Big Tech's historical reluctance in smaller jurisdictions raises doubt about compliance.

The decision has sent a clear message to controllers both local and international that compliance requires structured transparency, principled differentiation between essential and ancillary processing, demonstrable safeguards for cross-border transfers, and genuine respect for the informational autonomy of Ugandan data subjects. The PDPO has signalled that it will not hesitate to scrutinise global platforms' practices and issue binding remedial orders where deficiencies are found.

Authors



Namugera Joel Peter

✉ namugerajoelpeter@gmail.com



Kityo Martin

✉ kityomartins@gmail.com

DISCLAIMER

This article is developed as an information resource summarizing the decision issued by the Personal Data Protection Office of Uganda. It is provided for general informational and educational purposes only and does not constitute legal advice. The application of its contents to specific situations will depend on the particular circumstances involved. While every care has been taken in its preparation, DPO Privacy Centre East Africa and its personnel accept no responsibility for any errors this document might contain, whether caused by negligence or otherwise, or for any loss, howsoever caused, incurred by any person as a result of utilizing or otherwise placing any reliance upon it. Readers are strongly advised to seek qualified legal counsel for advice tailored to their specific situation.

Connect with us

privacycentreeastafrica@gmail.com ✉

[@privacycentreea](https://twitter.com/privacycentreea) ✕

DPO Privacy Centre East Africa [in](#)

substack.com/@privacycentreea 📄