



Personal
DATA
Protection
OFFICE

THE REPUBLIC OF UGANDA

IN THE MATTER OF THE DATA PROTECTION AND PRIVACY ACT, CAP 97

COMPLAINT NO. PDPO 086/2025

BETWEEN

ADLEGAL INTERNATIONAL LIMITED.....COMPLAINANT

VERSUS

WHATSAPP LLC.....1ST RESPONDENT

META PLATFORMS, INC2ND RESPONDENT

DECISION OF THE PERSONAL DATA PROTECTION OFFICE

Having reviewed the complaint lodged with the Personal Data Protection Office on 31st March 2025 alleging that WhatsApp LLC shares Ugandan users' personal data with Meta Platforms, Inc. without freely given, informed and explicit consent, collects personal data beyond what is strictly necessary for the provision of WhatsApp Messenger, affords Ugandan users materially weaker structured transparency than users in certain other jurisdictions and transfers personal data outside Uganda without demonstrating compliance with Section 19 of the Data Protection and Privacy Act, Cap. 97 (hereinafter referred to as the "Act, Cap. 97"), the decision of the Personal Data Protection Office is as follows:

A. INTRODUCTION

1. The Personal Data Protection Office (hereinafter referred to as the "Office" or "PDPO") received a complaint dated 31st March 2025 from Adlegal International Limited (hereinafter referred to as "Adlegal" or the "Complainant") titled "Complaint Concerning Violation of the Data Protection and Privacy Act, Cap 97 by WhatsApp LLC and Meta Platforms, Inc".



2. The Complainant alleged that the WhatsApp Privacy Policy update communicated to users in or around January 2021 (hereinafter referred to as the "2021 Privacy Policy" and/or the "2021 Privacy Policy Update") and the related practices of WhatsApp LLC (hereinafter referred to as "WhatsApp"/"1st Respondent") and Meta Platforms, Inc. (hereinafter referred to as "Meta"/"2nd Respondent") (collectively hereinafter referred to as the "Respondents") contravened the Data Protection and Privacy Act, Cap 97 and the Data Protection and Privacy Regulations, 2021 (hereinafter referred to as the "Regulations").
3. By notices communicated to the Respondents by email on 22nd April 2025, and with attachments provided on 30th April 2025, PDPO required the Respondents to file responses and supporting material. The deadline to respond was extended to 22nd May 2025.
4. On 22nd May 2025, WhatsApp filed a cover letter addressed to the National Personal Data Protection Director, and a substantive response to the PDPO's Notice to Respond, together with an annex bundle of materials referenced in its response.
5. On the same day, Meta likewise filed a cover letter and a substantive response to the PDPO's Notice to Respond.
6. PDPO has considered the complaint, the parties' written submissions, the annexed materials to their respective responses, and versions of the WhatsApp privacy policies referenced by the parties. This decision is rendered under Regulation 45(2) of the Regulations.

B. THE PARTIES/REPRESENTATION

7. The Complainant is Adlegal International Limited. The Complainant stated it brings this matter in the public interest and on behalf of Ugandan users of WhatsApp Messenger.



8. The 1st Respondent is WhatsApp LLC. According to the January 2021 WhatsApp Privacy Policy applicable to users outside the European region, WhatsApp LLC is described as a limited liability company incorporated in the United States of America and responsible for operating the WhatsApp messaging, voice, and video communication service for such users.
9. The 2nd Respondent is Meta Platforms, Inc. The WhatsApp Privacy Policy effective January 2021 and the related WhatsApp Help Centre materials describe WhatsApp as part of the Meta group of companies (“Meta Companies”) and indicate that Meta Companies work together to provide infrastructure, systems, and other support services across products. The Help Centre FAQ referenced in the complaint further explains that certain information may be shared between WhatsApp and other Meta Companies in accordance with the Privacy Policy, and describes Meta Platforms, Inc. as the parent company within the Meta group structure.
10. Meta challenged its inclusion as a respondent, contending that WhatsApp LLC is a separate legal entity and that Meta is not the data controller for WhatsApp Messenger user data. This objection is addressed as a preliminary issue in this decision.
11. The parties appeared in their own right and filed written submissions and supporting materials. The Complainant filed the complaint and attachments. The 1st Respondent, WhatsApp LLC, filed a formal written response dated 22nd May 2025 with annexures. The 2nd Respondent, Meta Platforms, Inc., filed a formal written response dated 22nd May 2025 with annexures. All such materials form part of the record before PDPO.

C. EVIDENCE

12. The Complainant submitted the following materials in support of its allegations:
 - (i) Copies/extracts of WhatsApp privacy policy materials applicable to the European region (relied upon to argue that Ugandan users receive materially weaker disclosures and safeguards);



- (ii) Selected regulatory/enforcement materials from other jurisdictions referenced under the complaint's section 3.8, including enforcement or investigative actions relating to WhatsApp and/or Meta; and
- (iii) User interface screenshots and/or written descriptions relating to how the 2021 update was presented in-app to users (relied upon to support the allegation of "take-it-or-leave-it" acceptance).

13. The 1st Respondent relied on the following materials in support of its response: —

- (i) The WhatsApp Privacy Policy effective 4th January 2021, including (among other provisions) the sections titled “How We Work With Other Meta Companies” and “Our Global Operations”, relied upon to evidence WhatsApp’s disclosures regarding data sharing within the Meta group, its approach to advertising disclosures (including the statement that WhatsApp does not run third-party banner adverts), and cross-border processing and storage (including processing in the United States of America); and
- (ii) WhatsApp Help Centre materials describing user settings and controls, relied upon to demonstrate that users have meaningful controls over certain data and account choices, including the ability to edit profile information and delete their accounts.

14. The 2nd Respondent relied on the following materials in support of its response: —

- a) A letter dated 22nd May 2025 addressed to PDPO, seeking exclusion from the complaint on the basis of corporate separateness and the contention that Meta is not the data controller for WhatsApp Messenger; and
- b) Meta’s response dated 22nd May 2025, which (among other matters) sets out Meta’s grounds for dismissal/exclusion, responds to allegations identified as relevant to Meta, and addresses the specific prayers directed at Meta.



D. PRELIMINARY MATTERS

15. This decision summarizes the parties' positions and refers to submitted materials only to the extent necessary for the findings and orders made herein. PDPO does not publish any technical details, internal operational documentation, or any personal data that is not necessary for this determination.
16. In determining the issues before it, PDPO assesses the facts on the balance of probabilities and draws reasonable inferences from the documentary record. Where an allegation is pleaded without supporting evidence beyond assertion, PDPO may decline to make an adverse factual finding.
17. As a preliminary matter, PDPO emphasises that regulatory compliance under the Data Protection and Privacy Act, Cap. 97 is anchored in accountability, and accountability begins with registration. Registration under Section 29 of the Act and Regulation 15 of the Data Protection and Privacy Regulations, is not a procedural formality; it is the foundational act by which a data collector, controller, or processor establishes an accountable point of contact and affirms its processing within Uganda's legal framework.
18. In that context, PDPO notes that the Complainant, Adlegal International Limited, is not registered with the Personal Data Protection Office as a data collector, data controller, or data processor. PDPO further recognises that the 1st Respondent (WhatsApp LLC) and the 2nd Respondent (Meta Platforms, Inc.) are registered with PDPO.
19. This clarification is recorded to reflect the regulatory posture of the parties before the Office and the accountability architecture contemplated by the Act, Cap 97. It does not, of itself, determine the Complainant's standing to lodge a complaint in the public interest under Section 31(1) of the Act, Cap 97 and Regulation 41(1)(a). Neither does it, by itself, confirm compliance by any party with other substantive obligations under the Act, Cap 97 and the Regulations.



20. The Complainant brings this matter in the public interest and on behalf of Ugandan users of WhatsApp Messenger. Section 31(1) of the Act, Cap 97, read together with Regulation 41(1)(a), permits any person to lodge a complaint with PDPO where they have reason to believe that a contravention of the Act has occurred. The Act does not restrict complaints to individual data subjects personally affected; it contemplates complaints in the public interest. PDPO is satisfied that the Complainant has standing to bring this complaint in the public interest, and no jurisdictional bar arises from the Complainant's corporate status.
21. Both Respondents are incorporated outside Uganda. The question arises whether PDPO has authority to adjudicate a complaint concerning their processing of Ugandan users' personal data. Section 1(b) of the Act, Cap 97 provides that the Act applies to data collectors, controllers and processors who, though not established in Uganda, process personal data of data subjects who are Ugandan citizens.

In *Ssekamwa Frank & 3 Others v Google LLC (18th July 2025)*, PDPO adopted a purposive interpretation, holding that an entity offering services to persons in Uganda and determining the purposes and means of processing of their personal data falls within the Act's scope irrespective of its place of incorporation. PDPO applies that reasoning and confirms that it has jurisdiction over this complaint. WhatsApp LLC offers WhatsApp Messenger to Ugandan users and determines the purposes and means of processing their personal data. Meta Platforms, Inc., as the parent company and recipient of intra-group data sharing, participates in the processing ecosystem. Both are therefore within the territorial scope of the Act, Cap 97.

22. In matters concerning proportionality, adequacy, and cross-border safeguards, once an arguable contravention is raised, the statutory burden rests on the data controller, processor or collector to demonstrate compliance under Sections 3(1)(c), 14 and of the Act, Cap 97 and Regulation 30 of the Regulations.



E. ISSUES FOR DETERMINATION

23. PDPO considers that the following **seven (7)** issues arise for determination:

Issue 1: Whether Meta Platforms, Inc. is properly joined as a respondent in this complaint and, if so, the scope of any findings applicable to Meta.

Issue 2: Whether the January 2021 WhatsApp Privacy Policy update afforded users a meaningful DATA opportunity to consent, and obtained valid consent where required.

Issue 3: Whether WhatsApp's January 2021 Privacy Policy permitted excessive data collection and unlawfully bundled non-essential processing without a valid lawful basis.

Issue 4: Whether the conduct by WhatsApp constitutes harm to Ugandan users by undermining data subjects' ability to exercise meaningful control over the use of their data.

Issue 5: Whether the Respondents complied with Section 19 of the Act, Cap 97 and Regulation 30 in relation to processing or storage of personal data outside Uganda.

Issue 6: Whether WhatsApp LLC subjected Ugandan users to disparate treatment by providing materially weaker privacy disclosures and safeguards than those provided to users in other jurisdictions.

Issue 7: Whether the Complainant is entitled to the orders sought and other remedies arising from the Respondents' alleged violations of the Act, Cap 97 and its Regulations.

F. RESOLUTION OF ISSUES

Issue 1: Whether Meta Platforms, Inc. is properly joined as a respondent in this complaint and, if so, the scope of any findings applicable to Meta.

Submissions of the Complainant

24. The Complainant joined Meta Platforms, Inc. as a respondent on the basis that the WhatsApp Privacy Policy effective January 2021 expressly provides for the sharing of

Handwritten signature



personal data between WhatsApp and other Meta companies. The Complainant contends that WhatsApp operates within the Meta corporate group and that personal data of Ugandan users is accessed, used, and further processed across that group. On that basis, the Complainant argues that Meta is implicated in the processing activities complained of and is properly joined to these proceedings.

Submissions of the 2nd Respondent

25. Meta Platforms, Inc. submitted that it is improperly joined to the Complaint and should be removed as a respondent. Meta's position is that WhatsApp is a separate and distinct legal entity and that WhatsApp, and not Meta Platforms, Inc., determines the purposes and means of processing personal data for WhatsApp Messenger.

26. Meta further submitted that the relief sought against it relates to the design and operation of WhatsApp Messenger, which Meta states it does not operate or control. Meta argued that the allegations in the complaint are directed at WhatsApp's privacy policy and WhatsApp's own processing activities, and that it would be improper to attribute alleged contraventions by WhatsApp to Meta in the absence of evidence establishing Meta's own role as a data controller in respect of the specific processing complained of.

27. Notwithstanding the foregoing, Meta's response dated 22nd May 2025 expressly acknowledges that WhatsApp forms part of the Meta corporate group and that Meta ultimately owns WhatsApp.

Determination

28. In determining whether Meta Platforms, Inc. is properly joined to this complaint, PDPO is guided primarily by Section 2 of Act, Cap. 97, which defines a "data controller" as:



“A person who alone, jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed”.

29. The statutory test is therefore a functional one, focused on whether an entity determines, alone or jointly, the “purposes and manner” of processing personal data. Formal corporate status or legal personality, while relevant, is not dispositive.
30. On the record before PDPO, it is established that WhatsApp LLC and Meta Platforms, Inc. are distinct legal persons, and that the January 2021 Privacy Policy identifies WhatsApp LLC as the entity responsible for providing WhatsApp services to users outside the European region. It is also established that the January 2021 Privacy Policy and WhatsApp’s annexures describe WhatsApp as one of the “Meta Companies”, and expressly state that WhatsApp “receives information from, and shares information with, the other Meta Companies”, including for infrastructure and delivery systems, safety and integrity, service improvement and personalisation, and integrations across Meta company products.
31. PDPO further takes note that WhatsApp itself asserts that Meta ultimately owns WhatsApp, but that WhatsApp (and not Meta) controls WhatsApp Messenger, sets the policies governing Ugandan users’ data, determines the purposes and manner of processing, and controls decisions on whether data is shared with Meta or other third parties. WhatsApp also states that it uses Meta’s infrastructure and that WhatsApp’s infrastructure is hosted on Meta infrastructure.
32. In considering the implications of group ownership and control for regulatory responsibility, PDPO has had regard, for limited analytical guidance, to the principle in ***Akzo Nobel NV v Commission (Case C-97/08 P)*** that full ownership may give rise to a rebuttable presumption of decisive influence.



33. PDPO emphasises that Akzo Nobel arises in a different legal context and is not binding in Uganda; it is considered only for the limited proposition that formal corporate separateness does not invariably preclude attribution where decisive influence is established on the facts. The presumption of decisive influence recognized in Akzo Nobel is evidential rather than automatic; it requires factual grounding demonstrating determination of purposes and means in the specific processing at issue. The applicable test under Act, Cap. 97 remains whether an entity determines the purposes and manner of the processing, alone or jointly.

Applying the statutory test to the evidentiary record, PDPO makes the following findings.

34. The record establishes group ownership and intra-group sharing as described in the 2021 policy and WhatsApp's submissions. However, the complaint and materials before PDPO do not sufficiently particularise how Meta Platforms, Inc. itself determines (alone or jointly) the specific purposes and manner of processing of Ugandan users' WhatsApp Messenger data that are complained of, beyond being the ultimate parent company and a recipient/service provider within the Meta group. The policy and WhatsApp's response identify WhatsApp as the entity responsible for WhatsApp Messenger and as the decision-maker for the processing and sharing decisions for that service.

35. PDPO therefore determines that it would be procedurally unfair and evidentially unsound, on this record, to make adverse findings of contravention against Meta Platforms, Inc. as a primary data controller for WhatsApp Messenger. At the same time, PDPO finds it appropriate that Meta remains joined for the limited purpose of ensuring that any remedial directions concerning intra-group disclosures, infrastructure-related processing, and cross-border safeguards are capable of effective implementation where Meta acts as a recipient and/or service provider in relation to WhatsApp's processing, as described in the policy and responses.



Issue 2: Whether the January 2021 WhatsApp Privacy Policy update afforded users a meaningful opportunity to consent, and obtained valid consent where required.

Consolidation of issues

36. PDPO notes that core allegations “A” and “C” raise closely related and overlapping questions concerning: —

- (i) Consent and other lawful bases for sharing data with other Meta companies, and
- (ii) The breadth and clarity of purpose statements.

37. These allegations arise from the same factual matrix, namely, the WhatsApp Privacy Policy effective January 2021 and the associated in-app update experience. In the interests of coherence and to avoid repetition, PDPO consolidates and determines these allegations together.

Submissions of the Complainant

38. The Complainant submitted that the January 2021 update expanded and formalized the sharing of personal data with other Meta companies without affording Ugandan users a meaningful opportunity to understand or control such sharing.

39. It was contended that continued use of WhatsApp Messenger was effectively conditioned on acceptance of updated Terms of Service and policy; that the purposes of sharing were framed in broad and composite terms; and that users were not enabled to distinguish between data strictly necessary for the core messaging service and data used for ancillary or ecosystem-level purposes. The Complainant further contended that any consent to such sharing was neither freely given nor sufficiently informed.

Submissions of the 1st Respondent

40. WhatsApp submitted that the Privacy Policy is a transparency document rather than a consent instrument. It emphasized that consent is not the sole lawful basis under



Section 7(2) of the Act, Cap 97 and Regulation 10(2)(b), and that it relies primarily on contractual necessity and legitimate interests for most processing.

41. WhatsApp further submitted that the January 2021 Privacy Policy expressly informs users that certain categories of personal data are shared with other Meta companies and describes the purposes of such sharing. It maintained that consent is relied upon only in limited circumstances for optional features (such as precise location sharing and media access), which are governed by device-level permission prompts capable of withdrawal.

Determination

42. As a preliminary observation, PDPO addresses WhatsApp's submission that the Privacy Policy is a "transparency document rather than a consent instrument". PDPO accepts that a privacy policy may serve primarily as a transparency instrument, and that consent is not the sole lawful basis for processing under the Act, Cap 97.

43. However, the statutory framework does not relieve a controller of the obligation to demonstrate a valid lawful basis for each processing purpose, or to ensure that the transparency it provides is structured, coherent, legible, and sufficient to support informed user understanding and meaningful control. Whether characterized as a "transparency document" or otherwise, the policy must enable clear purpose specification, lawful basis identification, and the exercise of informed user control as required by Sections 3(1)(a), 12 and 13 of the Act, Cap 97. The characterization does not alter the analytical framework or the statutory obligations applicable to the controller.

44. Section 2 of the Act, Cap. 97, defines "consent" as:

"Any freely given, specific, informed and unambiguous indication of the data subject's wish, which he or she, by a statement or a clear affirmative action, signifies agreement to the collection or processing of personal data relating to him or her".



45. Section 7 of the Act, Cap 97 provides that processing shall not occur without consent unless one of the lawful bases under Section 7(2) applies. This is augmented by Regulation 10(2)(b) that provides for “legitimate interests” as a lawful ground for collecting and processing data.
46. Sections 12 and 13 of the Act, Cap 97 require that personal data be collected for specific and explicitly stated purposes and that data subjects be provided, prior to collection, with clear and intelligible information regarding the purposes of processing and any disclosures.
47. The Ugandan High Court in ***Nalubega Shadia v Stabex International Ltd (Civil Suit No. 665 of 2021)*** affirmed that, where consent is relied upon, it must be clear, informed, and demonstrable, and that a data subject must be placed in a position to understand what they are agreeing to before consent can be regarded as valid.
48. Having reviewed the January 2021 Privacy Policy, PDPO finds, first, that intra-group sharing with other Meta companies was expressly disclosed. The policy contains a dedicated section titled “How We Work With Other Meta Companies”, which explains that WhatsApp receives information from, and shares information with, other Meta companies for purposes including operating and improving services, promoting safety and integrity, improving user experiences, showing relevant offers across Meta company products, and enabling integrations. PDPO therefore does not accept that intra-group sharing was undisclosed.
49. However, PDPO further finds that the policy presents purposes for processing and sharing in broad and composite terms across several sections, including “How We Use Information”, “Information You and We Share”, and “How We Work With Other Meta Companies”. While categories of personal data are described, the policy does not correlate, in a structured and intelligible manner, specific categories of data with specific purposes and the particular lawful basis relied upon for each purpose. This absence of structured correlation is not merely a drafting deficiency; it materially impairs the data



subject's ability to assess necessity, challenge processing, and exercise rights under Part V of the Act, Cap 97.

50. In the Uganda-facing policy, there is no clear mapping of which processing relies on contractual necessity, which relies on legitimate interests, and which, if any, relies on consent. PDPO finds that this absence of correlation weakens intelligibility and undermines compliance with Sections 3(1)(a), 12 and 13 of the Act, Cap 97.

51. PDPO considers it necessary to distinguish between processing strictly necessary for performance of the messaging contract and processing that extends beyond core functionality. Processing indispensable to the WhatsApp Messenger service includes account registration data, message routing metadata, and limited device and connection data necessary for security and integrity. Such processing may properly rely on contractual necessity or other lawful bases under Section 7(2) of the Act, Cap 97.

52. The policy, however, also describes processing and sharing for broader ecosystem-level purposes, including integration across Meta company products, product improvement across the group, personalization, and related optimization functions. While such purposes may be "commercially legitimate", they are not, on their face, strictly necessary for the transmission of messages between users. Where processing extends beyond what is indispensable to core service provision, the lawful basis must be clearly identified, and where consent is relied upon, it must satisfy the statutory standard.

53. PDPO accepts that WhatsApp demonstrated device-level consent prompts for limited optional features such as precise location and media access. However, those prompts are feature-specific and do not address the broader and continuing intra-group sharing described in the policy. The January 2021 update mechanism did not provide a differentiated, purpose-specific opportunity for Ugandan users to accept or decline ancillary intra-group sharing separate from acceptance of the Terms of Service. Users



were therefore not placed, at the point of acceptance, in a position to give consent that was specific to such ancillary processing.

54. Accordingly, PDPO determines that, while intra-group sharing was disclosed and consent is not required for all processing, the January 2021 Privacy Policy and update mechanism did not adequately correlate purposes, lawful bases, and categories of data in a manner sufficiently specific and intelligible to satisfy Sections 3(1)(a), 12 and 13 of the Act, Cap 97. Further, to the extent that ancillary intra-group processing was not strictly necessary for the provision of the core messaging service and required reliance on consent, the 1st Respondent did not demonstrate that valid consent meeting the statutory definition was obtained in the circumstances of the January 2021 update.

55. Issue 2 is therefore partly upheld to the limited extent of deficiencies in transparency, purpose specification, and demonstration of valid consent where required.

Issue 3: Whether WhatsApp’s January 2021 Privacy Policy permitted excessive data collection and unlawfully bundled non-essential processing without a valid lawful basis.

56. PDPO notes that core allegations “B” and “D” arise from the same factual and legal matrix and are therefore consolidated for purposes of determination.

57. Core allegation “B” concerns whether WhatsApp collected and processed personal data in excess of what was necessary for the provision of a messaging service.

58. Core allegation “D” concerns whether WhatsApp bundled processing necessary for the operation and delivery of WhatsApp services with ancillary processing that was not strictly necessary, without lawful differentiation or freely obtained consent.

59. Both allegations require application of the data minimisation and proportionality principles under Sections 3(1)(c) and 14 of the Data Protection and Privacy Act, Cap 97. In the interests of coherence and to avoid duplication, PDPO determines them together.



60. PDPO emphasizes that this issue is distinct from Issue 2. Issue 2 concerned the lawfulness of processing, the validity of consent where relied upon, and the adequacy of transparency. The present issue concerns whether the categories and scope of personal data collected and processed under the January 2021 Privacy Policy were proportionate to the specific purpose of providing WhatsApp Messenger, and whether essential and non-essential processing were impermissibly bundled in a manner inconsistent with the data minimization principle.

Submissions of the Complainant

61. The Complainant submitted that the January 2021 Privacy Policy reflects collection and processing of personal data beyond what is strictly necessary for the provision of a messaging service. It was contended that WhatsApp collects not only core account identifiers and routing metadata, but also device identifiers, IP addresses and derived location data, behavioural and usage analytics, identifiers associated with other Meta company products, and data enabling integration across the Meta ecosystem.

62. The Complainant argued that while certain data are indispensable to sending and receiving messages, the broader analytics and cross-product integration described in the policy exceed what is required for the specific purpose of operating a messaging service.

63. The Complainant further alleged that the policy bundled such ancillary processing together with core processing, without providing users with differentiated choice or freely obtained consent in respect of data not strictly necessary for the operation and delivery of WhatsApp services.

Submissions of the 1st Respondent

64. WhatsApp submitted that it does not collect excessive personal data and that the categories described in the January 2021 Privacy Policy are necessary to provide, secure,



and maintain the WhatsApp Messenger service; detect spam, fraud, and abuse; ensure network optimization and reliability; and improve service performance.

65. WhatsApp emphasized that messages are end-to-end encrypted; precise location data is collected only when users voluntarily activate location-sharing features; cookies are used for service functionality such as WhatsApp Web; and that the Act, Cap 97 does not prohibit processing required for legitimate operational and business purposes. WhatsApp denied bundling ancillary processing with core processing and maintained that optional features are activated by users voluntarily.

Determination

66. Section 3(1)(c) of the Data Protection and Privacy Act, Cap 97 requires that personal data be adequate, relevant, and not excessive or unnecessary in relation to the purposes for which it is collected or processed.

67. Section 14(2) further provides that personal data shall not be processed in excess of what is authorized by law or required for a specific purpose.

68. The statutory test is one of proportionality and objective necessity. Where processing extends beyond core service functionality, the controller bears the burden of demonstrating objective necessity for each category of data collected.

69. Having reviewed the January 2021 Privacy Policy, PDPO finds that WhatsApp collects and processes core messaging data, including mobile numbers, contact discovery information where permission is granted, and routing metadata necessary for message transmission.

70. PDPO also finds that WhatsApp collects device and connection data such as device model, operating system, IP address, identifiers, and diagnostic logs, and usage data reflecting interaction frequency, timestamps, and feature engagement.



71. PDPO accepts that core account and routing data are indispensable to the operation of a messaging service and that certain device and connection data are necessary to ensure service integrity, prevent abuse, and maintain network reliability. To that extent, such processing is proportionate and compliant with Sections 3(1)(c) and 14 of the Act, Cap 97.
72. However, the January 2021 Privacy Policy also describes broader processing and intra-group sharing for purposes including product improvement, personalization, integration across Meta company products, and ecosystem-level optimization. While such purposes may be “commercially legitimate”, the Respondent did not demonstrate, on the record before PDPO, that all categories of behavioural analytics, cross-product identifiers, and integration-related data are strictly necessary for the transmission and security of messages.
73. The Act, Cap 97 does not prohibit corporate integration or product enhancement; it does, however, require that personal data not be excessive in relation to the specific purpose for which it is collected. Where the purpose is framed as the provision of WhatsApp Messenger, the controller bears the burden of demonstrating that each category of data collected is proportionate to that purpose.
74. PDPO further finds that the January 2021 Privacy Policy presents essential service processing and broader ecosystem-level processing within the same structural framework, without clearly segregating indispensable data from ancillary data. The aggregation of indispensable service data with broader ecosystem-level analytics without structural segregation reinforces the bundling concern and obscures proportionality assessment.
75. Although WhatsApp asserts that certain optional features are activated voluntarily, the broader integration and analytics processing described in the policy are not clearly differentiated from core service processing in a manner that enables a transparent proportionality assessment. To the extent that ancillary processing is not strictly



necessary for the operation and delivery of WhatsApp Messenger, and where such processing relies on consent rather than another lawful basis, the absence of differentiated choice reinforces the bundling concern raised by the Complainant.

76. PDPO therefore determines that core messaging and security-related processing are proportionate and compliant with Sections 3(1)(c) and 14 of the Act, Cap 97.

77. However, to the extent that ongoing usage analytics and ecosystem-level integration processing extend beyond what has been demonstrated to be strictly necessary for the provision of a messaging service, and are presented without clear structural differentiation from essential processing, such processing constitutes non-compliance with the data minimisation and purpose limitation requirements of Sections 3(1)(c) and 14 of the Act, Cap 97. PDPO notes that WhatsApp did not advance a sufficiently documented legitimate interests balancing assessment to justify ancillary analytics processing under Regulation 10(2)(b). Even accepting that fraud prevention and service improvement may in principle constitute legitimate interests, the absence of any transparency to users about such processing and the structural bundling of ancillary data with essential service data precluded users from exercising an effective right to object in practice, thereby rendering reliance on a legitimate interests basis insufficiently demonstrated on the record before PDPO.

78. Issue 3 is accordingly partly upheld, confined to the non-essential processing categories identified above and the associated bundling of such processing with core service data without adequate differentiation.

Issue 4: Whether the conduct by WhatsApp constitutes harm to Ugandan users by undermining data subjects' ability to exercise meaningful control over the use of their data.

79. Core allegation "F" asserts that the January 2021 Privacy Policy update and related intra-group data sharing practices caused actual harm to Ugandan users by undermining their



ability to exercise meaningful control and informational self-determination over their personal data.

Submissions of the Complainant

80. The Complainant submitted that the 2021 update effectively placed users in an “all-or-nothing” position, conditioning continued use of WhatsApp Messenger on acceptance of revised Terms of Service that formalised expanded intra-group data sharing. It was contended that the breadth and structure of the policy prevented users from fully understanding the scope of data sharing and deprived them of meaningful choice.

81. The Complainant argued that such structural opacity constitutes actual harm because it undermines user autonomy and self-determination over personal information.

Submissions of 1st Respondent

82. WhatsApp denied that any harm occurred. It submitted that users retain significant control over their data, including the ability to:

- Manage privacy settings;
- Control profile information;
- Limit visibility of account data;
- Delete their account;
- Revoke device-level permissions for optional features.

83. WhatsApp maintained that no evidence of financial loss, misuse of content, or other tangible injury had been demonstrated, and that the complaint alleges speculative harm rather than demonstrable injury.



Determination

84. The Data Protection and Privacy Act, Cap 97 does not define “harm”. However, the statutory structure is premised on protecting informational autonomy. Sections 3, 7, 12, 13 and Part V of the Act, Cap 97 collectively recognise that data subjects must be placed in a position to exercise informed control over the processing of their personal data.
85. In considering whether the conduct complained of constitutes harm in the absence of demonstrated financial loss, PDPO has had regard to the scholarly treatment of privacy harms in comparative literature.
86. Citron and Solove observe that *“privacy harms are not limited to economic or physical injuries”* but extend to *“harms to autonomy, dignity, and self-determination”*. The authors further note that *“a lack of meaningful control over personal data can itself constitute a privacy harm, even when no immediate financial loss is shown”*. (See Danielle Keats Citron and Daniel J. Solove, “Privacy Harms”, *Boston University Law Review*, Vol. 102, 2022, at pp. 806–809.)
87. Part V of the Act, Cap 97 confers enforceable rights precisely to safeguard informational control; structural impairment of those rights is therefore legally cognizable under Ugandan law. This approach is consistent with the recognition in Article 27 of the Constitution of the Republic of Uganda that every person has a right to privacy, which encompasses informational self-determination. The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) similarly grounds data protection in the dignity and autonomy of the individual.
88. PDPO does not adopt foreign standing doctrine. However, this articulation is consistent with the structure of the Act, Cap 97, which protects not merely against financial loss but against opaque processing. The Act, Cap 97 does not treat transparency and informed control as mere procedural formalities. They constitute substantive protections through



which the data subject's autonomy interest is given legal effect. Their impairment is therefore not a technicality but an infringement of a legally protected interest.

89. Having reviewed the January 2021 Privacy Policy and related materials, PDPO makes the following findings;
90. First, WhatsApp provided certain mechanisms of control. Users could delete their account, adjust profile visibility, and revoke device-level permissions for specific optional features. PDPO therefore does not find that users were wholly deprived of control.
91. Secondly, as determined under Issue 2, the January 2021 update did not clearly correlate categories of data, purposes, and lawful bases in relation to intra-group sharing. Nor did it provide purpose-specific differentiation between essential processing and ancillary ecosystem-level processing.
92. Thirdly, as determined under Issue 3, the policy aggregated indispensable service data with broader analytics and integration processing without clearly demonstrating necessity for all such categories relative to the core messaging function.
93. The cumulative effect of these deficiencies is not merely procedural. Informational self-determination requires that users be placed in a position to understand and meaningfully determine how their data will be used. Where essential and ancillary processing are structurally blended, and lawful bases are not clearly articulated, users' practical ability to exercise informed control is materially constrained.
94. That said, the complaint does not establish quantifiable or specific material injury such as financial loss, identity theft, discriminatory profiling, or breach of encrypted message content. The harm alleged is primarily structural and autonomy-based.
95. PDPO therefore makes a calibrated finding.
96. It does not find that WhatsApp's conduct caused demonstrable material injury to Ugandan users on the record before it. However, PDPO finds that the structural



deficiencies identified in Issues 2 and 3 materially impaired the conditions necessary for informed and differentiated user control as contemplated by the Act, Cap 97. In that sense, limited to the impairment of the statutory conditions for informed user control, and not extending to demonstrable material injury, the conduct constitutes an infringement of the Act, Cap 97.

97. PDPO therefore determines that core allegation “F” is partly upheld to the extent that the deficiencies in transparency, lawful basis correlation, and proportional differentiation materially undermined the effective exercise of user control protected under the Data Protection and Privacy Act, Cap 97. It is not upheld to the extent it alleges demonstrable material injury beyond that structural impairment.

Issue 5: Whether the Respondents complied with Section 19 of the Act, Cap 97 and Regulation 30 in relation to processing or storage of personal data outside Uganda.

Submissions of the Complainant

98. The Complainant alleged that WhatsApp unlawfully transfers and processes personal data of Ugandan users outside Uganda, including to data centres in the United States of America. It was contended that the January 2021 Privacy Policy expressly discloses that personal data may be transferred to, stored in, or processed in countries outside Uganda, yet the Respondents did not demonstrate that those receiving jurisdictions afford protection equivalent to that required under Ugandan law.

99. The Complainant further submitted that no documented adequacy assessment, or enforceable protections were provided to PDPO, and that users were not meaningfully informed of the safeguards applicable to cross-border processing.

Submissions of the Respondents

100. WhatsApp and Meta submitted that Section 19 of Act, Cap 97 applies only to controllers or processors “based in Uganda”, and that neither entity is incorporated in



Uganda. They argued that there is no “transfer” in substance where users directly transmit data to foreign servers as part of using the service.

101. The Respondents further submitted that cross-border processing is inherent in global digital infrastructure, that adequate protections exist in receiving jurisdictions, and that safeguards recognised under other legal regimes demonstrate sufficient protection.

102. Meta additionally submitted that it is not the primary controller of WhatsApp Messenger data and that any cross-border compliance obligation rests with WhatsApp.

Determination

103. Section 19 of the Act, Cap 97 regulates processing or storage of personal data outside Uganda and requires that such processing ensure an adequate level of protection equivalent to that provided under the Act, or that other lawful conditions apply. Regulation 30 operationalises Section 19 and places the burden on the controller to demonstrate adequacy or appropriate safeguards where personal data is processed or stored outside Uganda.

104. The Act, Cap. 97 does not expressly define the term “transfer”.

Interpretation of “Transfer”

105. In the absence of a statutory definition, PDPO adopts a purposive interpretation consistent with the protective objective of Section 19, which is to ensure that personal data of Ugandan data subjects is not subjected to diminished protection when processed abroad.

106. While not bound by foreign regulatory interpretations, PDPO finds persuasive guidance in the functional approach articulated by the European Data Protection Board in Guidelines 05/2021 on international transfers. Those Guidelines identify three elements commonly present in a transfer:

(i) a controller or processor subject to the applicable legal regime;



Personal
DATA
Protection
OFFICE

- (ii) a disclosure or making available of personal data; and
- (iii) the recipient being located in another country.

107. Similarly, modern data protection frameworks describe transfers in functional terms, focusing on whether personal data collected under one legal regime becomes accessible or processed in another jurisdiction.

108. PDPO adopts this functional understanding as persuasive interpretive guidance. Accordingly, for purposes of Section 19 and Regulation 30, a transfer includes any situation where personal data collected from data subjects in Uganda is processed or stored in a foreign jurisdiction, whether through direct upload to overseas servers, remote hosting arrangements, onward disclosure, or shared infrastructure operations. This interpretation is grounded in the protective purpose of Section 19 and does not import foreign law into the Ugandan statutory framework.

109. The January 2021 Privacy Policy expressly states that WhatsApp operates a global infrastructure and that information may be transferred to and maintained on servers located outside the user's country of residence. PDPO therefore finds that personal data of Ugandan users is processed and stored outside Uganda within the meaning of Section 19 of the Act, Cap 97.

110. The Respondents' argument that no "transfer" occurs because data is directly uploaded by users is rejected. Section 19 of the Act, Cap 97 would be rendered ineffective if controllers could avoid its application by characterizing cross-border processing as mere "direct transmission" rather than transfer. The operative question is whether personal data of Ugandan data subjects leaves Uganda's territorial sphere of protection and is processed abroad. On the evidence before PDPO, it does.

Handwritten signature



Interpretation of “Based in Uganda”

111. Section 19 of the Act, Cap 97 refers to controllers or processors “based in Uganda”. In *Ssekamwa Frank & 3 Others v Google LLC (18th July 2025)*, PDPO adopted a purposive interpretation of territorial application, holding that an entity offering services to persons in Uganda and determining the purposes and means of processing of their personal data falls within the Act’s scope irrespective of corporate incorporation.
112. Applying that reasoning here, PDPO finds that WhatsApp LLC, which offers services to persons in Uganda and determines the purposes and means of processing of their personal data, falls within the scope of Section 19 of the Act, Cap 97. A narrow interpretation limited to domestic incorporation would materially weaken the protective purpose of Section 19 in the context of cross-border digital services and would be inconsistent with Section 1(b) of the Act, Cap 97.

Adequacy and safeguards

113. Regulation 30 requires that where personal data is processed or stored outside Uganda, the controller must demonstrate that the receiving jurisdiction ensures protection at least equivalent to that provided under the Act, or that appropriate safeguards exist. In the absence of an officially recognized adequacy determination under Regulation 30(4), the burden of proof lies squarely on the controller.
114. On the present record, the Respondents made general submissions regarding privacy protections in foreign jurisdictions and referenced safeguards recognised under other legal regimes. However, PDPO was not provided with:
- A documented adequacy assessment addressing the requirements of the Act, Cap 97;
 - A structured demonstration of enforceable rights available to Ugandan data subjects in the receiving jurisdiction;
 - Detailed safeguards governing onward transfers.

Handwritten signature



115. Regulation 30 places the burden of proof on the controller in the absence of an officially recognised adequacy determination. PDPO finds that this burden has not been discharged. PDPO notes that the Respondents referenced protections available under other legal regimes and general assertions about global privacy standards. To the extent that WhatsApp or Meta may rely on transfer mechanisms recognised in other jurisdictions, such as standard contractual clauses or binding corporate rules, the Respondents did not demonstrate that such mechanisms provide data subjects with enforceable rights equivalent to those under the Act, Cap 97, or that such mechanisms have been assessed for compatibility with Ugandan legal standards. General reliance on foreign transfer mechanisms does not discharge the burden under Regulation 30 in the absence of a Uganda-specific adequacy or safeguards analysis.

Role of Meta Platforms, Inc.

116. The January 2021 Privacy Policy indicates that data may be processed within Meta's global infrastructure. PDPO notes that both WhatsApp LLC and Meta Platforms, Inc. are now registered with PDPO. Registration confirms recognition of regulatory oversight but does not cure prior non-compliance.

117. Under Section 2 of the Act, Cap 97, a controller determines the purposes and means of processing, while a processor processes on behalf of a controller.

118. On the record before PDPO, WhatsApp LLC is the controller of WhatsApp Messenger data. To the extent that Meta hosts or processes such data outside Uganda, it acts at minimum as a processor; if it participates in determining purposes of cross-border integration or onward sharing, it may bear joint obligations. Corporate structuring does not relieve entities of responsibility where they functionally participate in cross-border processing.



119. PDPO determines that personal data of Ugandan users of WhatsApp Messenger is processed and stored outside Uganda within the meaning of Section 19 and Regulation 30, and that such cross-border processing constitutes a transfer in substance. WhatsApp LLC bears primary responsibility as controller for demonstrating adequacy and safeguards.
120. Meta Platforms, Inc., to the extent it participates in hosting or determining purposes of cross-border processing, bears obligations commensurate with its functional role.
121. The Respondents have not demonstrated compliance with the adequacy or safeguard requirements of Regulation 30. Accordingly, Issue 5 is upheld to the extent of non-demonstrated adequacy and safeguards and requires remedial action.

Issue 6: Whether WhatsApp LLC subjected Ugandan users to disparate treatment by providing materially weaker privacy disclosures and safeguards than those provided to users in other jurisdictions.

Submissions of the Complainant

122. The Complainant contended that Ugandan users received materially weaker privacy protections than users in certain other jurisdictions. The Complainant's case was not merely that the documents were drafted differently, but that Ugandan users were given less meaningful transparency and fewer structured safeguards around intra-group sharing, lawful basis articulation, and user understanding. It was argued that this disparity left Ugandan users less able to exercise control and self-determination over their personal data.

Submissions of the 1st Respondent

123. WhatsApp denied discrimination. It submitted that the Act, Cap 97 does not require identical privacy policies across jurisdictions and that differences reflect different legal and regulatory environments. WhatsApp maintained that the Ugandan facing policy



discloses key processing practices, including sharing with other Meta companies, and that the service applies strong security measures globally.

Determination

124. In determining this issue, PDPO first clarifies the legal question. Ugandan law recognizes “discrimination” most sharply in constitutional terms as differential treatment on prohibited grounds. The complaint before PDPO does not plead discrimination on enumerated protected characteristics (such as race, religion, ethnicity, sex, or disability).
125. On the evidentiary record before PDPO, there is also no basis to conclude that WhatsApp differentiated disclosures on such prohibited grounds. PDPO therefore does not make a finding of constitutional discrimination in the strict Article 21 sense.
126. However, where a controller demonstrably possesses the operational capacity to provide structured articulation of lawful bases and purpose differentiation, failure to provide equivalent structural transparency to Ugandan users is not a neutral drafting choice but a substantive compliance issue under Sections 12 and 13 of the Act, Cap 97.
127. That said, PDPO finds that the matter cannot be resolved on that basis alone. The Act, Cap 97 is not a “format comparison” statute; it is a substantive protection regime grounded in fairness, transparency, purpose specification, and informed user control. A controller may not defend materially reduced transparency for Ugandan users merely by saying “other jurisdictions have different rules”, if the reduced transparency results in Ugandan users falling below the minimum standards imposed by Act, Cap 97.
128. On the evidence before PDPO, it is established that WhatsApp is operationally capable of providing highly structured articulation of processing purposes, lawful bases, and user rights in other contexts. PDPO also finds, consistent with its determinations under Issues 2 and 3, that the Ugandan facing January 2021 documentation did not correlate purposes, data categories, and lawful bases in a structured and intelligible manner, and did not sufficiently differentiate essential from ancillary processing linked to broader ecosystem



integration. Those are not mere stylistic differences; they have substantive consequences for user understanding and control.

129. By way of concrete illustration, the WhatsApp privacy documentation applicable to users in the European region contains: a structured tabular correlation of processing activities, specific purposes, and the lawful basis relied upon for each; explicit identification of the right to object to processing for each relevant lawful basis; layered disclosures differentiating between processing necessary for the contracted messaging service and processing for advertising, analytics, or ecosystem-integration that is not required for delivery of that service; and clear information on how users may withdraw consent or exercise rights in respect of each category of ancillary processing. None of these structural features appear in the Ugandan-facing January 2021 documentation in substantively equivalent form. This concrete and verifiable structural deficit, rather than a mere stylistic or cosmetic difference, constitutes the evidentiary foundation for the finding of disparate treatment and demonstrates that Ugandan users received materially weaker structured transparency than required by the Act, Cap 97.

130. PDPO therefore finds that Ugandan users were subjected to disparate treatment in transparency and accountability, not proved as discrimination on prohibited grounds, but as a materially weaker disclosure and safeguards architecture that impaired the Act, Cap 97's core protections. This disparity is legally relevant because it results in reduced substantive compliance with Sections 12 and 13 (and, where applicable, the proportionality requirements addressed under Issue 3). In short: the disparity is evidence of unfair and insufficiently transparent processing, not necessarily unconstitutional discrimination.

131. PDPO further notes that, where a controller has already implemented structured purpose lawful basis correlation tables and layered disclosure frameworks for users in other jurisdictions, the revised Uganda facing policy required under this decision must achieve substantively equivalent transparency standards. WhatsApp may not satisfy the order herein by adopting a format that remains structurally inferior to the disclosures it

Handwritten signature



provides to users in jurisdictions whose data protection standards it regards as comparable to, or more demanding than, those of Uganda.

132. Accordingly, PDPO determines that the allegation of discrimination is partly upheld only in the sense of disparate treatment producing reduced substantive protection for Ugandan users, which constitutes non-compliance with the Act, Cap 97 transparency and accountability requirements as already found under Issues 2 and 3. PDPO does not uphold the allegation as constitutional discrimination on prohibited grounds.

Issue 7: Whether the Complainant is entitled to the orders sought and other remedies arising from the Respondents' alleged violations of the Act, Cap 97 and its Regulations.

133. Having considered the submissions, and evidence adduced by the parties, PDPO makes the following determination regarding the orders and remedies sought:

G. DECLARATIONS

134. That the January 2021 WhatsApp Privacy Policy applicable to Ugandan users disclosed intra-group data sharing with other Meta Companies but failed to adequately correlate categories of personal data, purposes of processing, and lawful bases in a structured and intelligible manner, contrary to Sections 3(1)(a), 12 and 13 of the Data Protection and Privacy Act, Cap 97.

135. That while core messaging and security-related data collection are proportionate and compliant with Sections 3(1)(c) and 14 of the Act, Cap 97, certain categories of ancillary usage analytics and ecosystem-level integration processing were not demonstrated to be strictly necessary for the provision of WhatsApp Messenger, and therefore constitute non-compliance with the data minimisation principle to that limited extent.

136. That the structural deficiencies identified materially impaired the statutory conditions necessary for fully informed user control and informational self-determination under the Act, Cap 97, though no demonstrable material injury was established.

Handwritten signature in blue ink.



137. That personal data of Ugandan users is processed and stored outside Uganda within the meaning of Section 19 and Regulation 30, and that the Respondents have not demonstrated compliance with the adequacy and safeguard requirements prescribed therein.

138. That the allegation of constitutional discrimination is not established; however, the differential transparency framework applicable to Ugandan users resulted in reduced substantive protection below the standards required by Cap 97, reinforcing the findings of non-compliance under Issues 2 and 3.

These declarations are made on the balance of probabilities and are confined strictly to the scope of the findings set out in this Decision.

H. ORDERS

In light of the foregoing declarations, and pursuant to the powers conferred under the Act, Cap 97 and Regulation 45(2), PDPO issues the following orders:

139. Transparency and lawful basis correlation

Within **ninety (90) days** of this Decision, WhatsApp LLC shall revise the Uganda-facing Privacy Policy to clearly and intelligibly correlate:

- Categories of personal data;
- Specific purposes of processing;
- The lawful basis relied upon for each purpose; and
- The categories of recipients, including intra-group recipients.

140. Differentiation of essential and ancillary processing

Within **ninety (90) days** of this Decision, WhatsApp LLC shall implement clear structural differentiation between:

- Processing strictly necessary for the provision and security of core messaging functionality; and

Handwritten signature



- Ancillary ecosystem-level processing not strictly necessary for that purpose.

Where such ancillary processing relies on consent, such consent must meet the definition under Section 2 of the Act, Cap 97. Additionally, where ancillary processing constitutes profiling for advertising or analytics purposes, WhatsApp LLC shall implement a granular, freely given opt-in mechanism enabling Ugandan users to consent to, or decline, each category of such ancillary processing separately from, and without prejudice to, their acceptance of the terms governing core messaging functionality.

141. **Cross-border compliance demonstration**

Within **ninety (90) days** of this Decision, WhatsApp LLC shall submit to PDPO a documented adequacy and safeguard assessment under Regulation 30 addressing:

- Legal protections applicable in receiving jurisdictions;
- Enforceable rights available to Ugandan data subjects;
- Safeguards governing onward transfers;

142. **Intra-group Data Protection Impact Assessment**

WhatsApp LLC shall conduct and submit a Data Protection Impact Assessment (DPIA) addressing intra-group sharing.

The DPIA shall address, at minimum:

- a) description of the categories of personal data shared within the Meta group and the purposes and lawful bases for such sharing;
- b) an assessment of the necessity and proportionality of intra-group data flows relative to the specific purposes of WhatsApp Messenger;
- c) an identification of risks to the rights and freedoms of Ugandan data subjects arising from intra-group sharing; and
- d) proposed mitigation measures, technical and organisational safeguards, and residual risk assessment.

This assessment shall be submitted to PDPO within **ninety (90) days** of this Decision.

Handwritten signature



143. In addition to the orders above, the following further orders are issued.

Where the 1st Respondent invokes legitimate interests under Regulation 10(2)(b) as a lawful basis for any category of processing of Ugandan users' personal data, WhatsApp LLC shall prepare a written legitimate interests assessment (LIA) documenting:

- a) the specific legitimate interest pursued;
- b) the necessity of the processing for that interest; and
- c) the balancing of that interest against the rights and freedoms of Ugandan data subjects, with particular regard to their reasonable expectations and the risk of harm. The LIA shall be submitted to PDPO as part of the revised policy documentation within the **ninety (90) day** compliance period prescribed herein.

144. The directives above are compliance measures intended to align processing practices with the requirements of Cap 97 and to enhance the protection of Ugandan data subjects.

145. **Failure to comply** with the above orders is an offence under Regulation 48 and may attract a fine for each day in default of this notice.

146. For the avoidance of doubt, non-compliance with orders relating to cross-border transfers under Section 19 of the Act, Cap 97 and Regulation 30, may, in addition to daily fines under Regulation 48, expose the Respondents to the further sanctions available under Regulation 30(6), including fines and, in the case of a natural person, imprisonment.

147. PDPO reserves the right to initiate further enforcement proceedings, if compliance with the orders herein is not demonstrated within the prescribed periods.

148. In accordance with Regulation 45(3) of the Data Protection and Privacy Regulations, 2021, this Decision is hereby served on the Respondents as an enforcement notice requiring each Respondent to:

- a) take the steps specified in this Decision within the timelines prescribed herein;

Bisikyo



- b) refrain from processing the personal data of Ugandan users except in accordance with the directions contained in this Decision; and
- c) take such remedial action as is specified in this notice.

149. Service of this Decision on the Respondents constitutes formal notice under Regulation 45(3).

150. PDPO has elected not to grant the Complainant's prayers in the form in which they were sought. The Complainant's principal prayers requested:

- a) an immediate cessation of all data sharing between WhatsApp and Meta companies pending user-by-user consent to each instance of processing and sharing;
- b) an immediate reversion to the data-sharing practices adopted under the 2016 policy and the establishment of an opt-in mechanism for additional data sharing with Meta and its affiliates; and
- c) an immediate cessation of the automatic transfer and integration of data from WhatsApp to Facebook, Instagram, and other Meta-affiliated services.

151. PDPO declines to grant these prayers in their immediate and absolute form for the following reasons.

152. First, the findings in this Decision are confined to structural deficiencies in transparency, purpose specification, lawful basis correlation, and cross-border compliance demonstration; they do not extend to a finding that all intra-group sharing is unlawful in its entirety. Ordering an immediate cessation of all such sharing would exceed the scope of the established contraventions.

153. Second, the complaint did not establish demonstrable material injury to individual users of the kind that would justify the most disruptive forms of interim relief.

Signature



Personal
DATA
Protection
OFFICE

I. Right of Appeal

154. Any party aggrieved by this Decision may appeal to the Minister of ICT and National Guidance within **thirty (30) days** from the date of receipt of this Decision, in accordance with Regulation 46 of the Data Protection and Privacy Regulations.

Dated this 20th day of February 2026

Baker Birikujja



CERTIFIED COPY

NATIONAL PERSONAL DATA PROTECTION DIRECTOR