UGANDA'S DRAFT DATA PROTECTION AND PRIVACY REGULATIONS AND GUIDELINES

DPO PRIVACY CENTRE (EAST AFRICA)'S SUBMISSION TO THE PERSONAL DATA PROTECTION OFFICE (PDPO)

May 2026

The Personal Data Protection Office (PDPO) has developed draft regulations and guidelines to strengthen Uganda's data protection framework. These include the **Data Protection and Privacy (Retention of Personal Data) Regulations, 2026**, **the Data Protection and Privacy (Data Security and Breach Management and Notification Obligations) Regulations, 2026**, **the Guidelines on Lawful Processing, the Guidelines on Data Protection Impact Assessment**, and **the Guidelines on Collaboration** (collectively referred to as "the instruments"). The instruments are expected to be gazetted and published later this year.

DPO Privacy Centre (East Africa) is pleased to contribute to the development of the instruments through submitting comments which identify specific concerns within the draft instruments and proposals of ways in which these concerns may be resolved. Throughout, reference is made to the Data Protection and Privacy Act Cap. 97 ("the Act") and the Data Protection and Privacy Regulations, 2021 ("the Regulations")

These comments are submitted in the public interest with the objective of strengthening the instruments in line with the Act, the Regulations, and applicable or persuading international standards, including the General Data Protection Regulation (GDPR), the Protection of Personal Information Act (POPIA) of South Africa, Kenya's Data Protection (General)Regulations, 2021, as well as the guidelines issued by the European Data Protection Board (EDPB) and its predecessor, the Article 29 Working Party.

References to international instruments provide comparative guidance only. The substantive framework governing data protection in Uganda remains the Act and the Regulations.

THE DATA PROTECTION AND PRIVACY (RETENTION OF PERSONAL DATA) REGULATIONS, 2026

1. Failure to Integrate the Right to Erasure

Issues Identified

Regulation 6(1)(e) references *"the rights of the data subject including the right to erasure and objection under the Act"* as a factor in determining retention periods. However, the draft Regulations do not set out the procedure or timeframe within which a controller must respond to a data subject's exercise of the right to erasure, nor do they specify the circumstances under which the right may be refused.

This omission is material. The right to erasure (sometimes referred to as the "right to be forgotten"), as provided under Section 28 of the Act and Regulation 39(1) of the Regulations, is one of the most practically significant rights under the Act. Without procedural rules governing its exercise in the retention context, data subjects cannot meaningfully enforce the right, and controllers lack clear guidance on handling erasure requests where extended retention is claimed under Regulation 8 of the draft regulations.

Comparative Standards

a) Under Article 17 of the GDPR, erasure requests must be responded to without undue delay and specific grounds for refusal are listed.
b) Comparable provisions exist in section 47 and 48 of the UK Data Protection Act 2018.[1]

Recommendations

We recommend that the draft Regulations be revised to establish an equivalent framework, specifically to:

a) define a clear timeframe for controllers to respond to erasure requests;
b) enumerate grounds for refusal consistent with the Act; and
c) provide procedural guidance for controllers on handling erasure requests in cases of extended retention.

[1] See also the ICO's guidance on the right to erasure under the UK GDPR: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/

Recommended Addition/Redraft

Right to Erasure

A data subject may, at any time, request a data controller, data processor or data collector to delete or destroy personal data relating to the data subject where:

a. the personal data is no longer necessary for the purpose for which it was collected or processed;
b. the data subject withdraws consent on which the processing was based and there is no other lawful basis for continued retention;
c. the data subject objects to the processing under the Act and there are no overriding legitimate grounds for retention;
d. the personal data has been unlawfully processed; or
e. the personal data must be erased to comply with a legal obligation.

Procedural Requirements

Upon receipt of a request, the data controller, data processor or data collector shall:

a. acknowledge receipt within five (5) working days; and
b. respond to the request with a decision, and implement the decision, within thirty (30) days, which period may be extended by a further thirty (30) days in complex cases upon notification to the data subject with reasons for the extension.

Grounds for Refusal

A data controller, data processor or data collector may refuse a request for erasure where the continued retention of the personal data is necessary for:

a. compliance with a legal obligation under any written law;
b. the establishment, exercise, or defence of legal claims; or
c. any of the grounds for extended retention under Regulation 8 of these Regulations.

Notification of Refusal

Where a request for erasure is refused, the data controller, data processor or data collector shall inform the data subject in writing of the reasons for the refusal and of the data subject's right to lodge a complaint with the Authority.

2. Inconsistency between the Act and the Regulations on the Right to Erasure

Issue Identified

There is a material inconsistency between the Act and the Regulations regarding the right to erasure:

a) Section 28 of the Act appears to vest the power to order an erasure in the Authority.
b) Regulation 39(1) of the Regulations, however, frames erasure as a direct right of the data subject.

This divergence creates uncertainty even within the draft Regulations as to whether erasure is a right that data subjects can directly enforce, or one that requires intervention by the Authority, and may need to be resolved by legislative amendment.

Implications

a) Controllers may be unclear on whether they may act directly on erasure requests or must await a directive from the Authority.
b) Data subjects may face barriers in exercising their rights if the procedural pathway is ambiguous.
c) The inconsistency undermines the clarity and enforceability of one of the most significant rights under the data protection framework.

The recommended procedural framework set out under Issue 1 above is drafted subject to the resolution of this inconsistency. The PDPO is urged to provide legislative clarification at the earliest opportunity.

3. Lack of Clarity on Erasure Obligations Applying to Backup and Archived Data

Issue Identified

The draft Regulations do not address how erasure obligations apply to backup systems, disaster recovery archives, or immutable storage environments. Organisations may technically "delete" active records while retaining recoverable copies indefinitely in archived systems. Without clarity, organisations may rely on technical storage architecture to circumvent erasure obligations.

Recommendations

The Regulations should clarify:

a) whether backup data must also be erased;

b) the timeframe within which archived copies must be overwritten;
c) circumstances where restricted retention in backup systems is permissible; and
d) safeguards preventing restored backup data from re-entering active processing environments.

4. Pseudonymisation Erroneously Listed as a Disposal Method

Issues Identified

Regulations 4(2)(b) and 10(1)(b) provide that a controller may fulfil its disposal obligation by anonymising, pseudonymising, or de-identifying data such that it can no longer be linked to an identifiable individual. The inclusion of pseudonymisation as an equivalent to anonymisation in this context is a fundamental legal and technical error.

By definition, pseudonymised data is remains personal data. The Definitions section of the Regulations correctly defines pseudonymisation as a process after which data "can no longer be attributed to a specific data subject without the use of additional information", with that additional information held separately. However, where such additional information exists and can be used to re-identify the individual, the data has not ceased to be personal data, and the retention obligation continues to apply.[2]

In contrast, anonymisation, is defined in the draft Regulations as an irreversible process after which "data ceases to be personal data." Only anonymisation can satisfy a disposal obligation.

Comparative Standards

This distinction is fundamental and is well-established internationally:

Recital 26 of the GDPR, the ICO's Guidance on Anonymisation and Pseudonymisation[3], and the EDPB Guidelines 01/2025 on Pseudonymisation and Opinion 05/2014 on Anonymisation Techniques[4], all confirm that

[2] Recital 26 of the GDPR: pseudonymised data could be attributed to a natural person by the use of additional information should considered to be personal data. See also EDPB Guidelines 01/2025 on Pseudonymisation (Adopted in January 2025)
[3] ICO, 'Guidance on Anonymisation and Pseudonymisation'(2022): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/pseudonymisation/#whatispseudonymisation
[4] EDPB, Opinion 05/2014 on Anonymisation Techniques (WP216), adopted 10th April 2014

pseudonymised data remains within the scope of data protection law and not a disposal method.

Recommendation

We recommend that:

Pseudonymisation be removed from the list of disposal methods and retain only as a safeguard during periods of extended retention, which is the correct and appropriate use reflected in Regulation 9(2)(a).

5. Absence of a Defined Standard for "Without Undue Delay"

Issue Identified

Regulation 4(2) requires deletion, destruction, or anonymisation "without undue delay" once the purpose has been fulfilled. However, the phrase is undefined and may create uncertainty in practice. Different organisations may interpret "undue delay" inconsistently, potentially resulting in prolonged retention under the guise of operational or technical constraints.

Recommendations

The Regulations would benefit from:

a) a prescribed timeframe;
b) sector-specific retention guidance; or
c) clear factors for determining what constitutes reasonable delay.

6. Need for Safeguards against Re-identification

Issues Identified

Regulation 4(2)(b) allows anonymisation or de-identification but does not impose safeguards preventing future re-identification. Modern data analytics and artificial intelligence systems can sometimes re-identify supposedly anonymised datasets when combined with other information.

Recommendations

The Regulations should impose:

a) technical safeguards;
b) access restrictions; and
c) prohibitions against intentional re-identification.

7. Annual Audit Requirement Imposes Disproportionate Burden on Small Entities

Issue Identified

Regulation 7(2)(b) requires that the periodic review mechanism include "manual audits by the Data Protection Officer." This provision creates two distinct problems:

a. **Implied Universal Requirement**
The Act and the Regulations do not impose a universal obligation to appoint a Data Protection Officer (DPO). Small organisations, sole traders, community-based organisations, and many SMEs are not required to have a DPO. By mandating audits "by the DPO", THE DRAFT Regulations effectively impose a defacto DPO appointment requirement on all controllers, without clear statutory authority.

b. **Disproportionate Burden on Small, Low Risk Controllers**
This requirement for annual audits applies uniformly, regardless of scale or risk. This means a village health clinic retaining 50 patients' records is subject to the same burden as a telecommunications company retaining the data of 15 million subscribers. Such uniformity is disproportionate, risks generating client fatigue and may discourage smaller entities from engaging meaningfully with the data protection framework.

Comparative Standards

International practice generally adopts a risk-based approach:

a) Under the GDPR, obligations are proportionate to the nature, scope, context, and risks of processing.

b) Supervisory authorities such as the ICO (UK) and EDPB (EU) emphasize scalability of compliance obligations, ensuring small entities are not overburdened relative to their risk profile.

Recommendation

These Regulations should introduce a risk-tiered audit obligation, with higher frequency and more rigorous mechanisms for large-scale or high-risk processors, and lighter-touch requirements for smaller, lower-risk entities.

This approach would align Uganda's framework with international best practice, preserve proportionality, and ensure compliance obligations remain effective, fair, and sustainable across different types of controllers.

Recommended Addition/Redraft

A data controller, data processor or data collector shall conduct periodic reviews of retained personal data at intervals appropriate to the nature, scale, and risk profile of its processing activities, and in any event:

a. at least once every twelve (12) months, for data controllers, data processors or data collectors that process sensitive personal data on a large scale, engage in systematic monitoring, or are classified as high-risk data processors by the Office; and
b. at least once every twenty-four (24) months, for data controllers, data processors or data collectors whose processing activities are limited in scope, involve no sensitive personal data, and present a low risk to the rights and freedoms of data subjects.

Where the data controller, data processor or data collector has a designated Data Protection Officer, manual audits by the Data Protection Officer; or where no Data Protection Officer has been designated, a review conducted by the senior officer responsible for data protection or compliance within the organisation.

THE DATA PROTECTION AND PRIVACY (DATA SECURITY BREACH MANAGEMENT AND NOTIFICATION OBLIGATIONS) REGULATIONS, 2026

8. Absence of Transition Periods (Both Regulations)

Issues identified

Neither the Retention Regulations nor the Breach Management Regulations contain transitional provisions to address the position of data controllers and processors that, at the time the Regulations come into force, are already:

a) retaining personal data or;
b) operating breach management plans that may not comply with the new requirements.

Without transitional provisions, every data controller and processor in Uganda would technically be in breach of both sets of Regulations from the day they come into force, unless they had already implemented fully compliant data retention schedules and breach management plans. This expectation is unrealistic, particularly for small and medium-sized entities.

Comparative Standards

International practice uniformly provides transitional periods to allow organisations time to adapt:

a) The GDPR provided a two-year implementation period (2016–2018) before enforcement commenced.
b) South Africa's POPIA provided a one-year implementation period after the substantive provisions came into force (2020–2021).
c) Kenya's Data Protection Act provided an eighteen-month grace period for registration and compliance.

Recommended Addition

Retention Regulations: A data controller, data processor or data collector that, at the date of commencement of these Regulations, is retaining personal data that was collected before that date shall, within three (3) months of commencement, review all such retained data and bring its retention practices into compliance with these Regulations.

A data controller, data processor or data collector shall establish and implement a data retention schedule compliant with Regulation … within six (6) months of the commencement of these Regulations.

Breach Management Regulations:

A data controller, data processor or data collector shall establish a data breach management plan compliant with Regulation 5 within six (6) months of the commencement of these Regulations.

The Office shall, within three (3) months of the commencement of these Regulations, publish a model data breach management plan template and notification form to assist data controllers, processors and collectors in meeting their obligations under these Regulations.

GUIDELINES ON LEGAL BASES FOR PROCESSING PERSONAL DATA

9. No Prohibition on Basis Swapping

The Preamble to the Guidelines correctly states that there is no hierarchy among the lawful bases recognized under the Act. This accurately reflects the position under Section 7 of the Act which provides a list of co-equal lawful bases without assigning precedence.

However, the Guidelines are silent on the internationally recognized prohibition against "basis swapping", the practice whereby a data controller, having initially sought consent which was refused or subsequently withdrawn by a data subject, then purports to rely on an alternative basis such as legitimate interests to continue processing for the same purpose.

This omission creates a significant gap in the protection afforded to data subjects. Without an explicit prohibition, controllers may exploit the silence to circumvent refusals of consent, undermining the integrity of consent as a rights-based mechanism and weakening the protections under Section 7(1) of the Act.

Comparative Standards

a) The UK Information Commissioner's Office (ICO) has explicitly held that where a controller has attempted to obtain consent and the data subject has refused or withdrawn it, the controller should not then switch to legitimate interest to justify the same processing, as this undermines the data subject's decision.[5]
b) The European Data Protection Board (EDPB) Guidelines 05/2020 on consent reinforce this position.[6]

Recommended Addition (Either as a new paragraph in the Preamble or in the Consent Section)

Prohibition on Basis Swapping Where a data controller, data collector or data processor has sought consent from a data subject and such consent has been refused or withdrawn, the controller, collector or processor shall not rely on an alternative lawful basis under Section 7 of the Act, including but not limited to legitimate interest, to continue processing of personal data for the same purpose in respect of which consent was sought and refused or withdrawn. Such a practice constitutes deceptive processing and is inconsistent with the principles of fairness, transparency, and data subject autonomy recognized under the Act.

10. Child Consent and the "Sufficient Age and Maturity" Provision

Issue Identified

Clause 3(2)(c) of the Guidelines provides that a child who is of "sufficient age and maturity" may provide consent to the processing of their personal data. This provision, while sound in principle and consistent with the international best practice, including Article 8 of the GDPR which sets 16 as the default age of consent and permits Member States to lower this to 13, directly conflicts with Section 8(a) of the Data Protection and Privacy Act, Cap 97.

[5] A guide to lawful basis: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/#Change
[6] Paragraph 122 and 123 of Guidelines 05/2020 on consent under Regulation 2016/679

Section 8(a) of the Act unambiguously provides that consent to the collection or processing of a child's personal data may only be given by a parent, guardian, or a person with parental responsibility over the child. The provision makes no exception for older or more mature minors. Accordingly, Clause 3(2)(c), as presently drafted, operates *ultra vires* the Act.

Implications

a) Controllers may be misled into believing that children can independently consent, exposing them to non-compliance with the Act.
b) Data subjects (children) may be given rights that are not legally enforceable under the current statutory framework.
c) The Guidelines risk undermining the authority of the Act and creating regulatory uncertainty.

Comparative Standards

a) Many jurisdictions adopt an age-differentiated approach: adolescents aged 16 and above may exercise independent autonomy, while parental consent remains required for younger children.
b) The GDPR sets 16 as the default threshold, with flexibility for Member States to lower it to 13.

Recommendation

We recommend that the PDPO initiates or advocates for a legislative amendment of the Act to introduce an age-differentiated approach to children's consent. Internationally, many jurisdictions provide a "carve out" permitting adolescents of 16 years and above to exercise independent autonomy, while retaining parental consent requirements for younger children. We recommend that 17 years be adopted as the threshold for independent consent by a child in Uganda, consistent with the dominant international standard. Until such amendment is effected, remove Clause 3(2)(c) from the Guidelines to avoid inconsistency with Section 8(a) of the Act.

11. **Additional Lawful Bases for Children's Data**

Issue Identified

The Guidelines focus primarily on consent as the lawful basis for processing children's data. However, **Section 8(c) of the Act** provides additional bases upon which children's personal data may be processed, including **research and statistical purposes**, subject to appropriate safeguards.

The omission of Section 8(c) from the Guidelines creates two risks:

a) Controllers engaged in legitimate research, public health monitoring, or educational assessment will either (a) process children's data without a properly identified lawful basis or;
b) rely on consent where the research basis would be more appropriate and less onerous.

The Guidelines should address all lawful bases under Section 8 comprehensively, unless the PDPO intends to release separate guidelines on processing children's personal data in the near term.

Recommendation

The Guidelines should:

a) Explicitly reference all lawful bases under Section 8 of the Act, not only consent.
b) Clarify the conditions under which children's data may be processed for research and statistical purposes, including safeguards such as anonymisation, minimisation, and ethical oversight.
c) Provide practical examples (e.g., public health surveillance, educational assessments, child welfare studies) to guide controllers in applying Section 8(c).
d) If the PDPO intends to issue separate guidelines on processing children's personal data, this should be clearly stated to avoid regulatory uncertainty.

Recommended Addition

Processing of Children's Data for Research and Statistical Purposes Personal data of a child may be collected or processed for purposes of research, historical, or statistical purposes under Section 8(c) of the Act, provided that:

a. The processing is in the public interest and cannot reasonably be achieved using anonymized or non-personal data;
b. Appropriate technical and organizational safeguards are in place, including restriction of access, pseudonymisation and data minimization;
c. Results are not published in a form that enables the identification of individual children; and
d. Where practicable, the consent of a parent, guardian, or person with parental responsibility is obtained.

The processing must be with consent of the parent, guardian or other person with the parental responsibility over the child except where there exists another lawful basis as provided under Section 8 of the Act.

12. National Security as a Lawful Basis

Issues Identified

Clause 8 of the Guidelines provides a lawful basis for processing personal data for national security and law enforcement purposes, grounded on Section 7(2)(b) (ii) and (iii) of the Act. The explanatory example in Clause 8 references "security agencies monitoring communications to prevent terrorist activity under lawful authority". While the example is not incorrect in law, it is presented without sufficient safeguards and risks being read as a broad or open-ended authorisation for surveillance.

The following concerns are raised:

a. **Absence of cross-reference to warrant requirement:** The interception of communications is already subject to prior judicial authorisation under the Regulation of Interception of Communications Act Cap 101, which requires that a warrant be sought before a lawful interception of communications is conducted. Clause 8 does not cross-reference this existing statutory safeguard, creating a risk that controllers threat the Guidelines as a standalone authorisation for surveillance without warrant.

b. **Failure to reference constitutional protections:** Article 27 of the Constitution of Uganda guarantees the right to privacy and Article 43 requires that any limitation of that right be demonstration justifiable in "a free and democratic society". The Guidelines should explicitly cross-reference both provisions to anchor the national security basis within Uganda's constitutional framework.

c. **Risk of blanket justification:** Without clear guardrails, Clause 8 could be used to justify routine mass surveillance of citizens under the guise of national security, contrary to the object and purpose of the Act.

Recommended Additions to the Clause

Constitutional Safeguards

Processing of personal data under this basis shall be subject to the right to privacy guaranteed under Article 27 of the Constitution of Uganda. Any limitation of this right shall only be to the extent that is permissible under Article 43 of the Constitution, being such as is acceptable and demonstrably justifiable in a free and democratic society.

Judicial Authorisation Requirement

Interception of, or access to, private communications for national security purposes shall be permitted only in accordance with the Regulation of Interception of Communications Act, Cap 101, including the requirement for a warrant issued by a competent judicial officer on the basis of sworn information. Generalised or speculative risk shall not suffice as a basis for interception.

13. Invalidity of Consent in Imbalanced Power Relationships

Issue Identified

Clause 3(c)of the Guidelines provides that; "consent shall be deemed invalid where there is a clear imbalance of power between the data subject and data controller." This is a welcome and important protection.

However, the clause as currently drafted places the burden on the data subject to establish that the power imbalance affected the consent given, which may be an evidential burden that is extremely difficult to discharge in practice.

Comparative Standards

a) Article 7(4) of the GDPR and Recital 43 provide that consent should not constitute a valid legal ground where there is a clear imbalance between the controller and the data subject, particularly where the controller is a public authority.
b) The EDPB Guidelines 05/2020 recommend that in such circumstances consent should be presumed invalid unless the controller can demonstrate otherwise[7]. We recommend that the Guidelines introduce a rebuttable presumption of invalidity of consent in contexts of power imbalance, transferring the evidential burden to the controller.

Implications

Without a rebuttable presumption, data subjects may be left without effective protection, and controllers may exploit the imbalance to secure consent that is neither voluntary nor genuine.

Recommended Redraft

"Where a clear imbalance of power exists between the data subject and the data controller, data collector or data processor, including but not limited to relationships of employer and employee, public authority and citizen, or provider and dependent recipient of an essential service, consent to the processing of personal data shall be presumed invalid unless the data controller, data collector or data processor demonstrates, with verifiable evidence, that the data subject had a genuine, voluntary choice and could have refused or withdrawn consent without any detriment whatsoever."

[7] EDPB, Guidelines 05/2020 on Consent, para 22

14. **Bundled Consent and Granularity**

Issues Identified

Clause 3(d) of the Guidelines states that consent should not be "bundled with" the performance of a contract or provision of a service. While directionally correct, the clause does sufficiently address the not the requirement for granularity in consent requests.

Comparative Standards

a) Article 7(2) of the GDPR provides that where consent is given in the context of a written declaration also concerning other matters, the request for consent must be clearly distinguishable from those other matters, in an intelligible and easily accessible form.
b) The EDPB has further clarified that data subjects must be able to give or withhold consent separately for each distinct processing purpose. [8] A single omnibus consent box covering multiple purposes does not satisfy this standard.

Implications

a) Controllers may continue to use omnibus or bundled consent mechanisms, undermining the meaningfulness of consent.
b) Data subjects may be forced into "all-or-nothing" choices, limiting their ability to exercise rights selectively.
c) The integrity of consent as a rights-based mechanism is weakened.

Recommended Redraft

"A request for consent shall be presented separately from, and shall not be bundled with, any other contractual terms, administrative provisions, or requests for consent to different processing purposes. Where a data controller, data collector or data processor seeks consent for more than one purpose, a separate consent request shall be made for each purpose, and the data subject shall be free to give or withhold consent independently for each. The use of pre-ticked boxes, omnibus consent clauses, or consent embedded within general terms and conditions shall not constitute valid consent. Data subjects shall be able to consent to,

[8] EDPB, Guidelines 05/2020 on Consent under Regulation 2016/679, adopted May 2020, paras. 22, 26-44 and 122 -123

for example: the performance of a contract while independently opting out of marketing communications."

15. **Withdrawal of Consent:**

Issues Identified

Clause 5 of the Guidelines does not presently impose any obligation on the data controller, data collector or data processor to notify or confirm to the data subject that, following withdrawal of consent, processing has ceased. Without such a confirmation obligation, data subjects have no practical assurance that their withdrawal has been acted upon.

Additionally, the clause does not distinguish between:

a) the right to order the right to withdraw consent, which applies only where the lawful basis is consent, and;
b) the right to object under Section 25 of the Act, which applies to processing on other bases such as legitimate interest.

Comparative Standards

a) Under the GDPR (Article 7(3)), controllers must ensure that withdrawal of consent is as easy as giving it, and must act upon withdrawal without undue delay.
b) The EDPB Guidelines on Consent emphasize that controllers should provide clear confirmation of withdrawal and cease processing immediately unless another lawful basis applies.

Recommendation

The Guidelines should be amended to:

a) Require controllers to acknowledge and confirm to the data subject that processing based on consent has ceased following withdrawal.
b) Clarify the distinction between withdrawal of consent (limited to consent-based processing) and the right to object (applicable to other lawful bases such as legitimate interest).

c) Provide practical guidance to controllers on how to implement withdrawal mechanisms (e.g., online opt-out tools, written confirmation notices).

Recommended Redraft

Clause 5(1):
Where processing of personal data is based on the consent of the data subject, the data subject shall have the right to withdraw that consent at any time. Such withdrawal shall not affect the lawfulness of processing carried out on the basis of consent before its withdrawal. The right to withdraw consent applies exclusively to processing whose lawful basis is consent; where processing is based on another lawful basis under section 7(2) of the Act, the applicable right of the data subject is the right to object under section 25 of the Act.

Clause 5(2):
Upon receipt of a notice of withdrawal of consent, the data controller, data collector or data processor shall:

a. Immediately cease all processing activities relying solely on the withdrawal consent;
b. Within seven (7) working days of receipt of the notice of withdrawal, communicate in writing to the data subject confirming that the processing has ceased, identifying specific processing activities discontinued; and
c. Where applicable, advise the data subject of any processing that continues under an alternative lawful basis under Section 7 of the Act, identifying that basis.

16. Performance of a Contract

Issues Identified

Clause 9 of the Guidelines addresses contractual necessity as a lawful basis under Section 7(2)(c) of the Act. The clause rightly provides that processing must be objectively necessary for the performance of a contract to which the data subject is a party, and includes useful illustrative examples on the distinction between necessary and excessive processing.

However, two further elements should be added to strengthen the clause:

a. **Purpose disclosure at inception of contract:** Data subjects should be clearly informed, at the commencement of the contractual relationship, of the specific categories of personal data to be processed and the particular purposes for which processing is necessary to perform the contract. This is consistent with the transparency obligations under Section 13 of the Act.

b. **Post-contractual retention:** The Guidelines are silent on how long personal data processed under this basis may be retained after termination or conclusion of the contract. Unlimited post-contractual retention under the guise of contractual necessity is inconsistent with the data minimization and storage limitation principles under Section 3(1)(c) and (d) of the Act. Controllers should be required to specify and communicate a defined retention period.

Recommended Addition

Before or at the time of entering into a contract, the data controller, data collector or data processor shall clearly and specifically inform the data subject of:

a. the personal data that will be processed;
b. the particular contractual obligations for which such processing is necessary; and
c. any third parties or processors to whom personal data will be disclosed in connection with the performance of the contract.

Upon the termination, expiry, or conclusion of a contract, the data controller, data collector or data processor shall not continue to process personal data under this lawful basis beyond the period reasonably necessary for the resolution of disputes, compliance with a legal obligation, or other identified legitimate purpose. The controller, collector or processor shall communicate the applicable retention period to the data subject and shall securely delete or anonymise personal data upon expiry of that period.

17. Explicit Consent for Special Personal Data

Issue Identified

Clause 2(1)(d) of the Guidelines provides that consent for sensitive personal data including health, biometric, and genetic data shall be explicit. This correctly reflects Section 9(3)(b) of the Act, which permits processing of sensitive personal data only where the data subject has given explicit consent. However, the Guidelines do not define what "explicitly consent" means or what form it must take. This omission risks controllers treating ordinary consent as sufficient for sensitive data.

Comparative Standards

The EDPB Guidelines 05/2020 confirm that implicit or inferred consent cannot constitute explicit consent for special categories.[9]

Recommendation

Explicit consent does not override the specific prohibitions and conditions in Section 9(1) and 9(3) of the Act. Therefore, the Guidelines should:

a) Define explicit consent as requiring a clear, affirmative statement by the data subject, separate from other consents, and recorded in a verifiable form (e.g., written, electronic, or audio).
b) Clarify that implicit or inferred consent (e.g., silence, pre-ticked boxes, or inactivity) does not constitute explicit consent.
c) State explicitly that explicit consent does not override the prohibitions and conditions in Section 9(1) and 9(3) of the Act.

Recommended Addition

Explicit consent for the processing of sensitive personal data as listed in Section 9(3)(b) of the Act shall satisfy the following requirements: a. it shall constitute a clear and specific statement by the data subject, expressly naming the category of sensitive data to be processed and the purpose of such processing; b. it shall be recorded in written or equivalent digital form, signed or authenticated by the data subject, or where oral, corroborated by a contemporaneous written record; c. it shall not be inferred from silence, inactivity, or general agreement to terms and conditions; and

[9] EDPB, Guidelines 05/2020 on Consent, Clause 4

d.	it shall not override or substitute compliance with the specific conditions and prohibitions applicable to sensitive personal data under Sections 9(1) and 9(3) of the Act.

18. Emergency Processing Without Consent

Issue Identified

Clause 10(9) of the Guidelines introduces an exception that permits the processing of sensitive personal data without consent in emergency situations, without mandating any written justification at the time of processing. This exception, as drafted, is dangerously overbroad.

While Section 9(3) of the Act contemplates certain exceptions to the prohibition on processing sensitive data, the absence of a contemporaneous documentation requirement creates a significant accountability gap. Post-hoc justifications in emergency contexts are susceptible to fabrication or overuse.

Comparable Standards

a) Under the GDPR (Article 9(2)(c)) processing of special categories of data is permitted for vital interests, but controllers must document the emergency basis and circumstances.
b) The UK Data Protection Act 2018 (Schedule 1) on health emergency exemptions, still require controllers to document the emergency basis and the specific circumstances at the earliest practicable opportunity.
c) International best practice emphasizes that emergency exceptions must be narrowly construed, documented, and subject to oversight.

Recommendation

The Guidelines should be amended to:

a) Require controllers to document the emergency circumstances and justification contemporaneously, or at the earliest practicable opportunity.

b) Clarify that emergency processing is limited to situations where the data subject is physically or legally incapable of giving consent, and the processing is strictly necessary to protect vital interests.
c) Provide for post-event review by the Office to ensure accountability and prevent misuse.

Recommended Redraft

Where processing of sensitive personal data is undertaken in an emergency without the consent of the data subject, the data controller, data collector or data processor shall: a. document, at the time of processing or as soon as reasonably practicable thereafter, the nature of the emergency, the specific personal data processed, the purpose of the processing, and the reason why consent could not be obtained; b. retain such documentation for a minimum period of five (5) years and make it available to the Personal Data Protection Office upon request; and c. where the emergency has passed, review whether continued processing is necessary or whether the data should be deleted or anonymised.

19. Legitimate Interest

Issue Identified

Clause 11 of the Guidelines addresses legitimate interest as a lawful basis under Regulation 10(2)(b) and (3) of the Data Protection and Privacy Regulations, 2021. The clause correctly identifies that a balancing test must be conducted. It also sets out useful conditions including lawful interest, defined interest, present and real interest, necessity, and balancing of rights.

However, the balancing test as described in Clause 11 does not follow the structured three-part framework that has become the international standard for legitimate interest assessments. The Article 29 Working Group

Opinion 06/2014 on legitimate interest[10] prescribe a three-stage sequential test commonly referred to as the Legitimate Interest Assessment (LIA):

(a) **Stage 1-Purpose Test**: Is there a legitimate interest that is lawful, clearly articulated, and real and present at the time of processing?
(b) **Stage 2-Necessity Test**: Is the processing actually necessary to achieve that interest? Could the same objective be achieved through means less restrictive of the data subject's rights?
(c) **Stage 3-Balancing Test:** Do the interests or fundamental rights and freedoms of the data subject override the identified legitimate interest? This includes considering the nature and sensitivity of the data, the reasonable expectations of data subjects and the impact of the processing.

The Guidelines' current formulation collapses these distinct stages and presents them non-sequentially, which may lead to controllers conducting a superficial or incomplete assessment. A formal LIA framework should be mandated and a template provided by the PDPO.

Recommended Redraft/Addition:

Before relying on legitimate interest as a lawful basis, a data controller, data collector or data processor shall conduct a structured LIA comprising the following sequential stages —

a. Stage 1 – Purpose Test: identify and clearly articulate the legitimate interest pursued, which must be lawful, specific, and real and present at the time of processing;

b. Stage 2 – Necessity Test: assess whether the proposed processing is strictly necessary to achieve the identified interest; and

c. Stage 3 – Balancing Test: evaluate whether the legitimate interest is overridden by the interests, rights, or freedoms of the data subject, having regard to the nature and sensitivity of the

[10] WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), adopted 9 April 2014. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

data, the reasonable expectations of the data subject, and the likely impact of the processing.

A data controller, data collector or data processor shall document the LIA in writing, retain it for so long as the processing continues and for a minimum of five (5) years thereafter, and make it available to the Office upon request.

The PDPO shall develop and publish a standard LIA template to assist controllers, collectors, and processors in conducting and documenting compliant assessments.

GUIDELINES ON DATA PROTECTION IMPACT ASSESSMENT (DPIA)

20. Absence of a Clear Statutory Grounding for the DPIA Obligation

Issue Identified

The Preamble and Clause 4 of the Guidelines state that a DPIA shall be conducted where processing is likely to result in a high risk to the rights and freedoms of natural persons, citing Regulation 12(3) of the Data Protection and Privacy Regulations, 2021. While this is correct, the Guidelines do not clearly identify the primary enabling provision within the Act itself that grounds the DPIA requirement, nor do they cross-reference the constitutional basis for it.

Since Regulation 12 of the Regulations is a delegated legislative instrument made under the Act, the Guidelines should, at the onset, anchor the DPIA obligation in the Act's foundational principles, particularly:

a. **Sect. 3(1)(c) of the Act** – the principle of data minimization which underpins the DPIA's necessity and proportionality assessment;
b. **Sect. 3(1)(e) of the Act** – the accuracy principle, relevant to assessing data quality risks;
c. **Sect. 3(1)(g) of the Act** – the security/integrity principle, which forms the backbone of the risk assessment in a DPIA; and
d. **Article 27 of the Constitution of Uganda** – the right to privacy, which is the ultimate value the DPIA mechanism seeks to protect.

We recommend that the Guidelines anchor these provisions to give the obligation proper constitutional weight.

Recommended Addition

These Guidelines are issued pursuant to Regulation 12 of the Data Protection and Privacy Regulations, 2021, and are grounded in the data protection principles established under Section 3 of the Data Protection and Privacy Act, Cap. 97, including the principles of data minimisation, accuracy, storage limitation, and integrity. The DPIA obligation derives its ultimate authority from the right to privacy guaranteed under Article 27 of the Constitution of Uganda, and must be interpreted in a manner consistent with that right and with the general limitations clause under Article 43 of the Constitution.

21. Inadequate Definitions

Issue Identified

The Definitions section of the Guidelines relies primarily on cross-references to the Act for key terms. However, several terms central to DPIA practice are used throughout the Guidelines but are **not defined,** creating interpretive uncertainty for practitioners.

Terms that requires definition include:

a. **"High risk":** The Guidelines identify ten (10) categories of high-risk processing but do not define "high risk" as a legal or evaluative standard. Without a definition, controllers may assess risk inconsistently. "High risk" must be assessed with reference to likelihood and severity of harm, and the Guidelines should adopt this two-dimensional definition.[11]
b. **"Residual Harm":** This term is used in Step 5 and Step 7 of the DPIA process without definition. Controllers need to understand what level of residual risk is acceptable before proceeding, or when PDPO consultation is triggered.

[11] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

c. **"Processing operation":** The Guidelines use both "processing activity" and "processing operation" interchangeably without defining either. Consistently with the Act's language is required.
d. **"Prior consultation":** Step 7 refers to consultation with the PDPO but does not define what constitutes prior consultation or what threshold of residual risk triggers the obligation.

Recommended Additions

"High risk" means a significant probability that a processing operation will result in harm to the rights and freedoms of data subjects, assessed by reference to the likelihood that the harm will occur and the severity of the harm if it does, including physical, material, or non-material harm such as discrimination, financial loss, reputational damage, identity theft, or denial of rights. **"Residual risk"** means the level of risk that remains after technical, organisational, and legal mitigation measures identified in the DPIA have been applied. A residual risk that is still assessed as high shall trigger the obligation to consult the PDPO under Regulation 12(4) of the Regulations before processing commences. **"Prior consultation"** means the formal process of submitting a completed DPIA to the PDPO before commencing a high-risk processing operation, as required under Regulation 12(4) of the Regulations, in circumstances where identified risks cannot be sufficiently mitigated.

22. Potential Ambiguity in the Threshold for Mandatory DPIA

Issue Identified

Clause 4 of the Guidelines correctly sets out ten (10) categories of high risk processing. However, point at which a DPIA becomes mandatory is internally inconsistent and insufficiently precise;

a. Singular vs cumulative criteria

The Guidelines state that a DPIA is required when processing "is likely to result in a high risk" (singular criterion), but also state that the "cumulative effect" of multiple criteria increases the likelihood. The relationship between a singular sufficient criterion and the cumulative approach is not clearly resolved. A controller meeting only one criterion, but not the high-risk categories that clearly trigger an obligation on their own (such as systematic monitoring of public spaces, or processing of sensitive data on a large scale), may incorrectly conclude no DPIA is needed.

b. Documentation of non-DPIA Decision

The condition for documentation where no DPIA is conducted despite meeting two or more criterial is correct in principle, but the Guidelines do not specify who within the organisation must sign off on that decision, or whether the PDPO should be notified.

Comparative Standard

The EDPB Guidelines on DPIA (WP248 rev. 01), state that a DPIA is always required where two or more of the identified criteria are met.[12]

We recommend that the Guidelines adopt this clearer rule.

Recommended Additions

Mandatory DPIA Threshold

A DPIA shall be mandatory where a proposed processing operation meets two (2) or more of the high-risk criteria set out in these Guidelines, regardless of whether any single criterion would, on its own, be considered sufficient to require a DPIA. Where a processing operation meets only one criterion, the data controller, data collector or data processor shall conduct a preliminary risk screening to determine whether the nature, scope, context, or purpose of the processing warrants a full DPIA, and shall document the outcome of that screening.

Decision Not to Conduct a DPIA

[12] EDPB, Guidelines on DPIA (WP248 rev.01), adopted 4 April 2017 (endorsed by EDPB 25 May 2018), para. 12

Where a data controller, data collector or data processor concludes that no DPIA is required despite meeting two (2) or more high-risk criteria, that decision shall be:

a. documented in writing by a senior officer with authority over data protection decisions within the organisation, or by the appointed Data Protection Officer;
b. retained as part of the organisation's accountability records for a minimum period of five (5) years; and
c. made available to the PDPO upon request.

23. Insufficient Guidance on Processing Data of Children and Vulnerable Persons

Issue Identified

Clause 4(g) of the Guidelines identifies processing data concerning vulnerable persons including children, patients, employees, asylum seekers, the elderly, and persons with mental illness, as a high-risk category requiring a DPIA. However, the Guidelines provide no specific guidance on how DPIAs should be conducted in respect of these categories, and in particular offer no guidance specific to children.

This is a significant gap as processing of children's data raises distinct risks that differ materially from those arising in respect of adult data subjects, including:

a. Children are less able to understand or evaluate the risks of data processing;
b. Children may be more susceptible to manipulation, profiling, and targeted adverting;
c. The developmental consequences of data misuse may be longer-lasting for children; and
d. Sect. 8 of the Act and the applicable children's consent framework impose specific obligations that the DPIA must reflect.

We hold the view and understanding that DPIAs for processing involving children should carry a heightened standard of assessment, including an explicit child-specific risk analysis and would recommend that the Ugandan Guidelines adopt such a requirement.

Recommended Addition

Where a proposed processing operation involves the personal data of children, the DPIA shall, in addition to the standard risk assessment, include:

a. an assessment of the developmental impact of the processing on the child, including risks of psychological harm, manipulation, or undue influence;
b. an assessment of whether the processing is consistent with the best interests of the child, as required under the Children Act, Cap. 59;
c. an evaluation of whether the consent mechanism adopted complies with Section 8 of the Act, including whether parental or guardian consent has been obtained for children below the applicable age of digital consent;
d. consideration of age-appropriate design measures to minimise data collection and protect children's privacy by default; and
e. consultation with a child safeguarding expert where the processing is large-scale or involves sensitive categories of children's data.

Where processing involves other categories of vulnerable persons, including patients, employees, asylum seekers, or persons with cognitive impairments, the DPIA shall include a specific assessment of the power imbalance between the data subject and the controller, and the adequacy of safeguards to protect the rights of those who may be unable to freely give, refuse, or withdraw consent.

24. Inadequate Treatment of Automated Decision Making

Issue Identified

Clause 4(b) of the Guidelines identifies automated decision-making with legal or significant effect as high-risk category referencing Section 27 of the Act. However, the guidance provided on this category is the least developed of all the ten categories. The Guidelines merely state that automated decisions producing legal effects or significantly affecting individuals fall into this category, and that "routine automated processes with little or no effect on individuals would not meet this threshold".

This is insufficient for the following reasons:

a. **"Significantly affects" is undefined**: The Guidelines do not explain what constitutes "significant effect" on an individual. The EDPB Guidelines automated decision making[13] and Guidelines on dark patterns[14] provide that significant effects include decisions that affect access to credit, employment, insurance, housing, education, and healthcare, as well as decisions that profile individuals in ways that affect their behavior.
b. **Section 27 of the Act is not adequately explained:** Section 27 of the Act confers rights on data subjects in relation to automate decision-making, including the right to be informed, to request human review, and to contest the decision. The DPIA Guidelines should explain that any DPIA covering automated decision-making must assess compliance with these rights, including whether appropriate safeguards for human oversight have been built in.
c. **Artificial Intelligence risks not addressed:** The reference to "innovative technology" in Clause 4(h) partially addresses AI, but the Guidelines do not address the distinct risks of machine learning models, including algorithmic bias, opacity, and discriminatory outputs, all of which are directly relevant to the DPIA process for automated decision making.

Recommended Redraft/Addition

Data processing that involves automated decisions, including those produced by artificial intelligence or machine learning systems, which produce legal effects or significantly affect individuals as provided under Section 27 of the Act, shall require a DPIA.
For purposes of these Guidelines, a decision "significantly affects" an individual where it:

a. determines or materially influences eligibility for, or access to, credit, insurance, employment, education, housing, or public services;
b. results in profiling that affects the individual's behaviour, opportunities, or treatment; or
c. produces outcomes that the individual could not reasonably have anticipated and cannot easily contest.

[13] EDPB, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251 rev.01), adopted 3 October 2017.
[14] EDPB, Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces (Version 2.0, adopted 8 September 2022).

The DPIA for automated decision-making shall, in addition to the standard risk assessment, include:

a. an assessment of the logic and criteria applied in the automated system and the potential for discriminatory or biased outputs;
b. an assessment of whether the system complies with Section 27 of the Act, including the right to be informed of the automated processing, the right to human review, and the right to contest decisions; and
c. a description of the technical and organisational safeguards implemented to ensure meaningful human oversight of automated decisions.

25. Unclear Prior Consultation Obligation

Issue Identified

Step 7 of the Guidelines provides that where a DPIA identifies risks that "remain high even after mitigation," the controller must consult the PDPO before processing begins. This correctly reflects the intention of Regulation 12(4) of the Regulations. However, the Guidelines fail to define what "**high" residual risk means, specify the consultation procedure or required** documents, specify the PDPO's powers on receipt of a DPIA, or set response timeframe for the PDPO. This absence of procedural clarity may deter controllers from engaging in prior consultation.

Recommended Redraft

Where a DPIA concludes that identified risks to the rights and freedoms of data subjects remain at a high level after all proportionate mitigation measures have been applied, the data controller, data collector or data processor shall, before commencing processing, submit the DPIA to the PDPO for prior consultation in accordance with Regulation 12(4) of the Regulations. For purposes of this provision, a residual risk shall be considered to remain at a high level where it is assessed as having a likelihood of "possible" or above and an impact of "major" or above on the risk assessment scale set out in Annex IV of these Guidelines.
A prior consultation submission to the PDPO shall include:

a. the completed DPIA report, including the risk register and action plan;
b. a summary of the mitigation measures applied and the residual risks that persist;
c. the legal basis relied upon for the processing; and
d. contact details of the Data Protection Officer or responsible person within the organisation.

The PDPO shall respond to a prior consultation submission within thirty (30) working days of receipt of a complete submission. Where additional information is required, the PDPO shall notify the controller within fifteen (15) working days, and the thirty (30) working day period shall be suspended until the additional information is received. Processing shall not commence before a response is received from the PDPO.

Upon reviewing a DPIA submitted for prior consultation, the PDPO may:
a. approve the processing with or without conditions;
b. require the implementation of additional technical or organisational safeguards before processing commences; or
c. prohibit the processing where the risks to data subjects' rights and freedoms cannot be adequately mitigated, and such prohibition shall be communicated in writing with reasons. A data controller, data collector or data processor aggrieved by a prohibition decision may appeal the PDPO's decision in accordance with the applicable procedure under the Act.

26. Absence of Data Breach Notification Interface

Issue Identified

The DPIA Guidelines are entirely silent on the relationship between the DPIA process and data breach notification obligations under the Act and the Regulations. A DPIA is a forward-looking risk assessment tool; however, where a processing operation that was subject to a DPIA subsequently suffers a data breach, it is essential that:

a. the controller is required to review and update the DPIA in light of the breach;
b. the breach notification obligations under the Act (and any forthcoming breach notification regulations) are cross-referenced so controllers understand the interplay; and
c. the DPIA record is available to the PDPO as part of any investigation into the breach, to assess whether the risk was foreseeable and adequately mitigated.

We therefore recommend that this review obligation be incorporated into the Guidelines.

Recommended Addition

Where a data controller, data collector or data processor suffers a personal data breach in connection with a processing operation that was the subject of a DPIA, the controller, collector or processor shall:

a. review the DPIA within thirty (30) days of becoming aware of the breach to assess whether the risk that materialised was identified in the original DPIA and whether the mitigation measures adopted were adequate;
b. update the DPIA to record the nature of the breach, its likely causes, and the revised mitigation measures adopted in response;
c. make the updated DPIA available to the PDPO as part of any investigation into the breach; and

where the breach reveals a systemic gap in the DPIA methodology, conduct a revised DPIA and submit it to the PDPO in accordance with Step 7 of these Guidelines if residual high risks are identified.

27. Insufficient Treatment of Joint Controllers and Processor Obligations

Issues Identified

Clause 5 of the Guidelines briefly addresses joint DPIAs and Clause 7 provides that processors must "assist the data controller by providing all relevant information." Both provisions are underdeveloped and fail to address several important practical scenarios.

a. Joint Controllers

Where two or more organisations are joint data controllers, the Guidelines do not specify:

i. which controller is responsible for initiating and leading the DPIA;
ii. how liability is apportioned between joint controllers where the DPIA is inadequate or where the obligation is not discharged; or
iii. whether a joint DPIA covers all parties' obligations or whether each controller must independently assess their role.

Under Recital 79 of the GDPR and EDPB Guidelines on controllers[15], each controller in a joint arrangement retains independent accountability. We recommend that the Guidelines reflect this principle.

b. Processor Obligations

The Guidelines are silent on whether a data processor who independently introduces a high-risk processing operation for example, a sub-processor using a new AI tool to process data on behalf of the controller has any obligation to notify the controller and trigger a DPIA review. Under Regulation 17 of the Regulations, processors must not engage sub-processors without the controller's authorisation, but the DPIA Guidelines do not connect this obligation to the DPIA framework.

Recommended Addition

Where processing is carried out by joint data controllers, each controller shall be independently responsible for ensuring that a DPIA is conducted in relation to their respective processing activities. Where a joint DPIA is agreed upon, the controllers shall designate in writing which controller has primary responsibility for conducting, managing, and submitting the DPIA, without prejudice to the independent accountability of each controller. The written arrangement between joint controllers shall specify the respective roles and responsibilities in the DPIA process and shall be made available to the PDPO upon request. A data processor who proposes to engage a sub-processor or to introduce a new technology, tool, or processing method that may significantly alter the nature or risk profile of the processing shall notify the data controller in writing before implementing such change. Upon receipt of such notification,

[15] EDPB, Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, adopted 7 July 2021

the data controller shall assess whether the proposed change constitutes a material change to the processing operation requiring a review or update of the existing DPIA, and shall conduct such a review where necessary.

DATA PROTECTION AND PRIVACY COLLABORATION GUIDELINES

28. Material Definition Gaps

Issue Identified

The Definitions section of the Guidelines defines eight terms, most by cross-reference to the Act. However, several terms that are central to the operation of the Guidelines are used throughout the document but are left undefined. This creates interpretive uncertainty and risks inconsistent application across sectors. The following terms require definition:

a. **"Collaboration instrument":** The Guidelines refer to multiple instruments including Memoranda of Understanding, Terms of Reference, joint advisories, and working group reports, but do not define what constitutes a collaboration instrument or the legal standing of each type.
b. **"High-risk data processor":** This term is used in Clause 13 but is defined only by sector example, without reference to the risk criteria in Regulation 12 of the Regulations or the DPIA Guidelines issued by the PDPO. The definition should align with the threshold in the DPIA Guidelines.
c. **"Mass data processor":** Similarly, Clause 14 defines this term by example only. A principled, criteria-based definition is needed to provide legal certainty and avoid arbitrary categorisation.
d. **"Adequacy":** Clause 41 addresses adequacy assessments for cross-border transfers but does not define what "adequacy" means for purposes of Ugandan law, beyond a general reference to "equivalent" protection. A definition aligned with the Act and international standards is required.

e. **"Standard Contractual Clauses (SCCs)"** and **"Binding Corporate Rules (BCRs)":** These instruments are referenced in Clause 41(5) but are not defined. Controllers relying on these mechanisms need to understand their legal character, the approval process, and where model SCCs can be found.

Recommended Addition

"Collaboration instrument" means any written instrument through which collaboration under these Guidelines is formalised, including Memoranda of Understanding, Terms of Reference, joint advisories, inter-agency records of decisions, and working group reports, each of which shall be of the standing specified in these Guidelines.

"High-risk data processor" means a data processor whose processing operations are likely to pose a high risk to the rights and freedoms of data subjects by reference to the criteria set out in Regulation 12(3) of the Regulations and the PDPO's Guidelines on Data Protection Impact Assessments, including processors engaged in large-scale processing of sensitive personal data, systematic monitoring, or automated decision-making with legal or significant effect.

"**Mass data processor"** means a data controller, data collector, or data processor that processes personal data of a very large number of data subjects on a systematic or continuous basis, including telecommunications operators, internet service providers, and national government agencies. The PDPO shall, from time to time, publish guidance on the numerical or proportional thresholds that constitute mass processing.

"Adequacy" means a determination made by the PDPO, following assessment, that a foreign jurisdiction provides a level of protection for personal data that is at least equivalent to the protection afforded under the Act and the Regulations, having regard to the rule of law, human rights standards, the independence of the supervisory authority, and the availability of effective redress mechanisms for data subjects.

"Standard Contractual Clauses (SCCs)" means model contractual provisions approved by the PDPO for use by data controllers and processors when transferring personal data to countries that have not been determined to provide an adequate level of data protection, which contractual provisions impose binding obligations on the importer to protect the personal data in accordance with the Act.

29. PDPO as Sole Gatekeeper for All Foreign Data Requests

Issue Identified

Clause 42(3) of the Guidelines provides that Ugandan data controllers and processors *"shall not respond directly to foreign requests without approval of the PDPO."* While the principle of channeling foreign requests through a central authority is sound, this provision as drafted is overbroad and raises the following concerns:

a. **No distinction between categories of request:** The Guidelines do not distinguish between requests made through formal legal channels such as Mutual Legal Assistance Treaties (MLATs) which involve foreign courts or prosecutorial authorities and carry legal obligations on the receiving party and informal requests from foreign regulators or businesses. The implications and urgency of these different categories differ materially.
b. **Potential conflict with court orders:** Where a foreign court issues an order requiring disclosure of data held by a Ugandan controller, and that order is recognisable and enforceable under Ugandan law, requiring PDPO approval before compliance may place the controller in an impossible legal position.
c. **No timeframe for PDPO approval:** The Guidelines do not specify how quickly the PDPO must respond to an approval request. This creates uncertainty for controllers and may result in unlawful delay where foreign requests are time-sensitive.
d. **No protection for controllers who act in good faith:** If a controller complies with a foreign request in good faith through a legally recognised channel, the Guidelines as drafted suggest the controller may still be in breach for not obtaining prior PDPO approval. A safe harbour provision is needed.

Recommended Redraft:

A Ugandan data controller or data processor that receives a request from a foreign government, regulator, or court for access to personal data located in Uganda shall:

a. notify the PDPO of the request within five (5) working days of receipt, providing a copy of the request and any supporting documentation; and
b. not disclose personal data in response to the request until PDPO clearance is obtained, except as provided in Clause ……

A data controller or processor may respond to a foreign request without prior PDPO approval where:

a. the request is made through a Mutual Legal Assistance Treaty or other formal legal mechanism under which Uganda has a binding obligation to respond, and the controller is acting in compliance with a court order or prosecutorial direction recognised under Ugandan law; or
b. delay in responding would result in imminent harm to the rights or safety of individuals and the controller has been unable to obtain PDPO clearance within forty-eight (48) hours of notification;

provided that in either case, the controller shall notify the PDPO of the disclosure as soon as practicable and in any event within twenty-four (24) hours of making the disclosure.

The PDPO shall respond to a notification of a foreign request within ten (10) working days of receipt. Where a matter is urgent, the controller shall flag this expressly, and the PDPO shall respond within forty-eight (48) hours. Failure by the PDPO to respond within the prescribed period shall not constitute deemed approval; the controller shall follow up and document the absence of a response.

30. Adequacy Assessment Process

Issue Identified

Clause 41(3) of the Guidelines provides that the PDPO shall publish a gazette notice listing countries with adequate data protection frameworks. Clause 41(4) provides that transfers to gazetted countries shall be deemed compliant with no further conditions. While this is a useful mechanism, the Guidelines are silent on several procedural elements that are essential for the adequacy process to operate with legal certainty:

a. **No timeframe for adequacy assessments:** The Guidelines provide no indication of how frequently the PDPO will conduct adequacy assessments, how long an assessment will take, or how often the gazette list will be updated. Without this, controllers cannot plan cross-border transfers with confidence.
b. **No process for suspension or revocation of adequacy:** If a gazetted country subsequently weakens its data protection framework, or if a significant systemic breach occurs in that country affecting Ugandan data subjects, the Guidelines provide no mechanism for the PDPO to suspend or revoke adequacy status. Under Article 45(5) of the GDPR, the European Commission may repeal an adequacy decision where the third country no longer ensures an adequate level of protection. A comparable mechanism is essential for Uganda.
c. **No transitional arrangements:** Where adequacy status is suspended or revoked, controllers with ongoing transfer arrangements to the affected country need guidance on what safeguards must be put in place and within what timeframe.
d. **No public consultation requirement:** Adequacy determinations can have significant implications for trade, diplomacy, and the rights of Ugandan data subjects. The Guidelines should require the PDPO to conduct stakeholder consultation before making or revoking an adequacy determination.

Recommended Addition

The PDPO shall, at least once every three (3) years, review the adequacy status of countries to which personal data is commonly transferred by Ugandan data

controllers. Prior to making or revoking an adequacy determination, the PDPO shall:

a. conduct a structured assessment against the criteria set out in Clause ….;
b. consult with the Ministry of ICT, the Ministry of Foreign Affairs, sector regulators, and civil society organisations with relevant expertise; and
c. publish the proposed determination for public comment for a period of not less than thirty (30) days before it takes effect.

The PDPO may, at any time, suspend or revoke an adequacy determination in respect of a country where:

a. the country has materially weakened its data protection framework;
b. a systemic breach or widespread misuse of Ugandan personal data has occurred in that country; or
c. the country's supervisory authority is no longer independent or effective.

A suspension or revocation shall be notified by gazette and shall take effect thirty (30) days after publication, during which period data controllers with existing transfer arrangements shall implement alternative safeguards under Clause…..

For any further information:

1. Namugera Joel Peter, Convenor & Team Lead, namugerajoelpeter@gmail.com , privacycentreea@gmail.com
2. Mugambe Andrew, Associate – SM & Co Advocates, amugambe@smco.ug
3. Hellen J. Ndagire, Associate – MMAKS Advocates, ndagire@ug.aln.africa