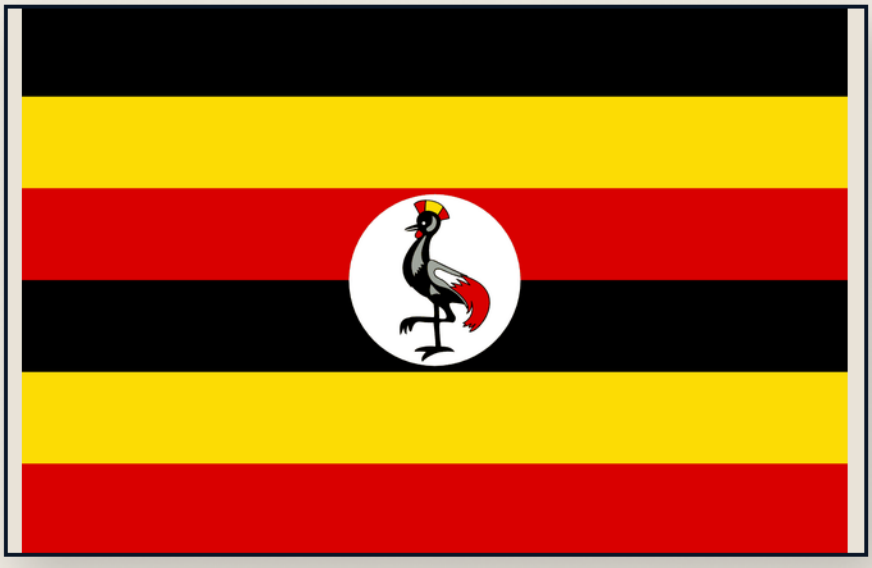
VOVE ID

VOVE COUNTRY CONTROL FILE

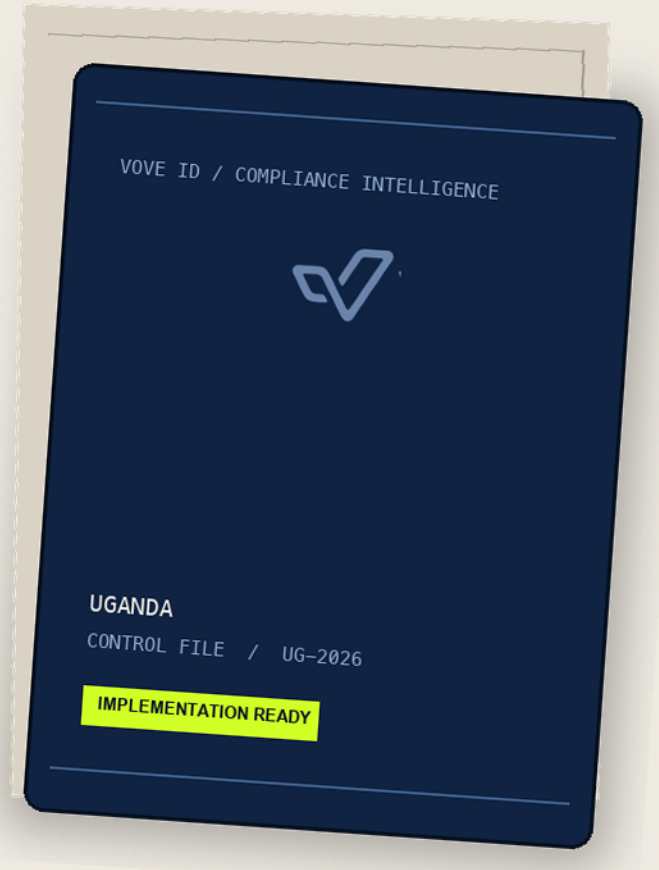
KYC / KYB / AML

2026 EDITION

UGANDA



UGANDA / UG



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Uganda KYC, KYB & AML Compliance Checklist

A practical implementation checklist for fintechs, payment providers, financial institutions and other accountable persons operating in Uganda.

Financial intelligence unit	**Financial Intelligence Authority (FIA)**
Large cash reporting	**Conservatively UGX 20,000,000 or more**
Record retention	**At least 10 years from the applicable identity, transaction/correspondence or relationship-closure date, whichever is later**
Annual compliance return	**Due by 31 January**
FATF public list	**Exited increased monitoring on 23 February 2024**

Scope and legal framework

Anti-Money Laundering Act, Cap. 118 as amended, including the Anti-Money Laundering (Amendment) Act, 2017, the Anti-Money Laundering (Amendment) Act, 2022 (Act 18), the Anti-Money Laundering (Amendment) (No. 2) Act, 2022 (Act 23), and the Anti-Money Laundering (Amendment of Schedule 2) Instrument, 2025; Anti-Money Laundering Regulations, 2015 as amended in 2022 and 2023; Anti-Terrorism Regulations, 2025 (S.I. 75/2025); Companies (Beneficial Owners) Regulations, 2023 and Companies (Beneficial Owner) (Amendment) Regulations, 2024 (S.I. 35/2024); National Payment Systems Act, Cap. 59 and National Payment Systems Regulations, 2021; Data Protection and Privacy Act, Cap. 97 and Regulations, 2021; Protection of Sovereignty Act, 2026 (Act 7 of 2026), commenced 22 May 2026, solely where its provisions apply to an institution licensed under an Act of Parliament to facilitate cross-border money transfers

FATF context

Uganda exited FATF increased monitoring in February 2024. Continue risk-based country screening against current FATF statements.

IMPORTANT	Operational guidance, not legal advice. Requirements vary by licence, activity and supervisor. Confirm the current consolidated laws, FIA directives, Bank of Uganda conditions and sector-specific rules before implementation.

HOW TO USE THIS GUIDE

Turn each requirement into owned evidence

For every row, assign an owner, confirm whether the control applies, link the evidence, record gaps, and set a remediation date. A checked box is not evidence by itself.

01 / SCOPE	02 / DESIGN	03 / EVIDENCE	04 / REVIEW
Confirm institution, supervisor, product, customer and risk scope.	Map each obligation to a policy, system control or human review.	Retain the document, decision, timestamp, owner and rationale.	Test the control and update it when rules or risks change.

Checklist legend

CONTROL tells you what outcome to cover. IMPLEMENTATION ACTION translates that outcome into operational work. EVIDENCE suggests what an auditor or reviewer should be able to inspect. SOURCE points back to the primary rule or regulator guidance.

1. REGULATORY PERIMETER AND GOVERNANCE

Regulatory perimeter and governance

Establish the licences, accountable-person status and governance structure before onboarding customers.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map the regulatory perimeter	Document each product, customer type, payment flow and delivery channel; identify the applicable accountable-person category and sector supervisor, including Bank of Uganda licensing where relevant.	Approved perimeter memo, product inventory and legal sign-off	AMLA Cap. 118, Second Schedule; FIA registration guidance; Bank of Uganda supervision framework
Register with FIA	Register the entity as an accountable person using the prescribed process and maintain the registration particulars.	FIA registration acknowledgement and entity profile	AMLA Cap. 118, s.21(pb); AML Regulations 2015, reg. 4
Report registration changes	Notify FIA using the prescribed form within 15 days after a change to registered particulars.	Change log, Form 2 and submission receipt	FIA Registration Guidelines for Accountable Persons
Appoint and empower the MLCO	Every accountable person must appoint or designate an MLCO in a senior managerial position with sufficient competence and experience and notify FIA on Form 3. The internal auditor is ineligible; the CEO is ineligible except for a sole proprietorship or single-member company. Notify cessation on Form 3 within 15 days. Give the MLCO unrestricted access to relevant information and responsibility for FIA liaison, the internal escalation system and external reporting.	Board appointment, competence assessment, eligibility check, Form 3 notices, access profile, escalation procedure and goAML role	AMLA Cap. 118, s.6(m); AML Regulations 2015, regs. 6-7, as amended by AML (Amendment) Regulations 2023, reg. 5 [01][02][20]
Approve an AML/CFT programme	Maintain board-approved policies, procedures and controls covering risk assessment, CDD, reporting, records, sanctions, training and independent audit.	Current policy suite, board minutes and control owners	AMLA Cap. 118; AML Regulations 2015; FIA Guidance Notes
Submit the annual compliance return	File the annual compliance report and current internal AML/CFT policy with FIA by 31 January following each calendar year.	Signed return, policy copy and FIA receipt	AML Regulations 2015, reg. 45

2. ENTERPRISE AND CUSTOMER RISK

Enterprise and customer risk

Use documented risk assessment to determine control intensity and review frequency.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Assess enterprise ML/TF/PF risk	Assess customers, products, services, channels, technologies and geographies; document inherent risk, control effectiveness and residual risk.	Approved methodology, risk register and remediation plan	AMLA Cap. 118; AML Regulations 2015; FIA Guidance Notes
Assess new products before launch	Complete ML/TF/PF, fraud and privacy assessments before launching a product, delivery mechanism or material technology change.	Product risk assessment and approval gate	FIA Guidance Notes; risk-based obligations under AMLA
Risk-rate every relationship	Assign and explain a customer risk rating using customer, ownership, PEP, sanctions, product, channel, transaction and geographic factors.	Scoring model, input data, overrides and review date	AMLA Cap. 118, s.6; AML Regulations 2015
Apply enhanced due diligence	For high-risk relationships obtain additional identity, ownership, purpose, source-of-funds or source-of-wealth information, senior approval and enhanced monitoring.	EDD file, approvals and monitoring plan	AMLA Cap. 118, s.6; FIA Guidance Notes
Use simplified measures only after low-risk finding	Document the low-risk basis and never use simplified measures where suspicion exists or higher-risk factors apply.	Low-risk assessment and approved control configuration	AML Regulations 2015; FIA CDD guidance

3. KYC AND CUSTOMER DUE DILIGENCE

KYC and customer due diligence

Identify and verify customers before or during establishment of the relationship, subject only to lawful risk-controlled exceptions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply the prescribed natural-person identification rules	For a Ugandan citizen or person lawfully resident in Uganda, obtain the applicable national identification card or alien identification document and any one of the particulars listed in regulation 19(1)(b). Residential address is one alternative among those particulars, not a separately mandatory requirement. The other alternatives include contact details; an employer or senior-government-official introduction; TIN where applicable; for a student, a school introduction and student ID copy; a summary of business activities; or a sample signature. Separately obtain the customer's fingerprints as required by regulation 19(6). Resolve doubtful citizen identity with NIRA and doubtful immigration status with the Uganda Citizenship and Immigration Control Board. For a foreign citizen not resident in Uganda, apply regulation 20's prescribed identification and independent-verification requirements.	Regulation 19 or 20 identity checklist, applicable national identification card or alien identification document, one regulation 19(1)(b) particular, separate fingerprint record, independent verification and doubt-resolution record	AMLA Cap. 118, s.6; AML Regulations 2015, regs. 19-20, as amended by the AML (Amendment) Regulations 2023, including regs. 19(1)(b) and 19(6) [01][02][20]
Identify representatives	Verify every person acting for a customer and confirm authority through a mandate, resolution, power of attorney or equivalent record.	Representative KYC and authority instrument	AMLA Cap. 118, s.6; AML Regulations 2015
Understand purpose and intended nature	Record why the relationship is opened, expected products, counterparties, volumes, value, geographies and source of funds.	Customer profile and expected-activity baseline	AMLA Cap. 118, s.6; AML Regulations 2015
Apply every CDD trigger to the correct customer type	Apply CDD to every one-off transaction, including every domestic or international wire transfer, without treating 5,000 currency points as a minimum threshold for regulation 18 CDD. Track and apply the 5,000-currency-point threshold separately only where another applicable provision expressly retains it. Also apply CDD whenever suspicion exists or previously obtained identification data is doubtful. For established customers, maintain ongoing CDD throughout every business relationship and ensure required originator and beneficiary information accompanies applicable wire transfers.	One-off transaction trigger matrix, separately configured threshold controls, ongoing CDD schedule, wire-information controls and completed CDD cases	AMLA Cap. 118, ss.6-7; AML Regulations 2015, reg. 18 as substituted by AML (Amendment) Regulations 2023, reg. 16, and regs. 34-35 [01][02][20]
Resolve failed CDD safely	Do not open, transact or continue where mandatory CDD cannot be completed; consider ending the relationship and filing an STR without tipping off.	Decline or exit record and STR decision	AMLA Cap. 118; AML Regulations 2015
Monitor and refresh CDD	Keep identification and risk data current, scrutinise transactions against the profile and refresh promptly after triggers or according to risk.	Review schedule, trigger events and refreshed files	AMLA Cap. 118, ss.6 and 7; FIA Guidance Notes
Control non-face-to-face onboarding	Apply additional document-authenticity, liveness, device, fraud and impersonation controls so remote verification is reliable and risk-based.	Remote-onboarding standard, test results and exception queue	AMLA risk-based CDD duties; Data Protection and Privacy Act 2019

4. KYB AND BENEFICIAL OWNERSHIP

KYB and beneficial ownership

Verify the legal person, its authority structure and the natural persons who ultimately own, control or benefit from it.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal existence	Obtain and independently verify incorporation or registration, legal form, registered office, business address, tax details, directors and current status with URSB or the competent registry.	Registry extract, constitutional documents and status check	AMLA Cap. 118, s.6; AML Regulations 2015
Identify the natural-person beneficial owners	Trace ownership and control through every layer to the natural persons who ultimately own or control the customer, the natural person on whose behalf a transaction is conducted, and natural persons who exercise ultimate effective control over a legal person or arrangement; do not rely only on nominees or directors.	Ownership chart, transaction-beneficiary analysis, declarations and independent corroboration	AMLA Cap. 118 as amended in 2017; s.6
Verify ownership and control	Corroborate shareholding, voting rights, appointment rights, agreements and other means of influence; resolve discrepancies before onboarding.	Share registers, filings, agreements and discrepancy log	AMLA Cap. 118; Companies (Beneficial Owners) Regulations 2023, as amended
Check and maintain the company BO register	Obtain evidence that the company keeps its BO register, files an updated consolidated register annually, reports changes or discrepancies in writing as soon as known and designates at least one Uganda-resident natural person to cooperate with competent authorities.	Certified BO register, annual consolidated filing, discrepancy notices, resident-contact designation and URSB receipts	Companies BO Regulations 2023; Amendment Regulations 2024, S.I. 35/2024
Verify directors and authorised signatories	Identify and screen directors, senior managers, account signatories and persons authorised to instruct the relationship.	KYC files, board resolution and mandate matrix	AMLA Cap. 118, s.6; AML Regulations 2015
Understand the business and funds	Establish business model, operating footprint, licences, expected activity, source of funds and, for higher risk, source of wealth.	Business profile, licence checks and financial evidence	AMLA Cap. 118; FIA Guidance Notes
Refresh KYB on change	Monitor registry, ownership, control, directors, licences and activity; repeat CDD after material change, doubt or suspicion.	Event monitoring and updated KYB pack	AMLA ongoing CDD obligations; BO Regulations 2023/2024

5. PEPS, SANCTIONS AND TARGETED FINANCIAL SANCTIONS

PEPs, sanctions and targeted financial sanctions

Apply enhanced PEP controls and execute targeted financial sanctions without delay.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify PEP exposure	Screen customers, beneficial owners and controllers for domestic and foreign PEP status and relevant family members or close associates.	Screening results, relationship map and review log	AMLA Cap. 118, s.6(g)
Apply mandatory PEP controls	Obtain senior-management approval, establish source of wealth and source of funds, and conduct enhanced ongoing monitoring.	Approval, source evidence and enhanced monitoring record	AMLA Cap. 118, s.6(g)
Screen within four hours	Screen customers, beneficial owners, controllers, payers and payees against applicable designations within four hours after receiving FIA information or a directive and keep authoritative lists and subscriptions current.	FIA receipt time, four-hour screening completion, list inventory and alert cases	Anti-Terrorism Regulations 2025, S.I. 75/2025
Freeze, stop and report without delay	For a match, without delay freeze or seize funds and economic resources, stop transactions and prevent direct or indirect availability. Report to FIA immediately after freezing and complete the full TFS process within 24 hours.	Match validation, freeze and stop records, immediate FIA report and 24-hour completion clock	Anti-Terrorism Regulations 2025, S.I. 75/2025
Control unfreezing and false positives	Release assets only under competent authority, delisting or applicable legal process; preserve documented false-positive and name-resolution decisions.	Legal authority, release approval and case file	Anti-Terrorism Regulations 2025, including delisting, unfreezing and court-authorisation provisions [10]

6. TRANSACTION MONITORING AND REPORTING

Transaction monitoring and reporting

Detect unusual activity and file prescribed reports through FIA channels without tipping off.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor transactions continuously	Use scenarios and investigations calibrated to the customer's expected activity, products, channels, counterparties, geography, cash and fraud risk.	Scenario inventory, tuning evidence and alert outcomes	AMLA Cap. 118, s.7; AML Regulations 2015
File STRs within the exact clocks	File without delay and no later than two working days from formation of suspicion. Report TF or PF suspicion without delay. Submit supplemental information as soon as possible and within two working days after discovery.	Suspicion time, MLCO decision, STR, supplements and goAML receipts	AMLA Cap. 118, s.9; FIA reporting requirements; FIA STR Guidance Note effective 1 December 2024 [24][25]
Prevent tipping off	Restrict STR information, communications and case access; do not disclose that a report or investigation exists.	Access controls, scripts and training records	AMLA Cap. 118
Record and report large cash conservatively	Configure UGX 20 million or more to reconcile the Act's 'exceeding' language with regulation 39(3) and Form A's 'equivalent to or exceeding' wording. Record on the same day; aggregate multiple transactions by or on behalf of one person during one day; apply the supervised-accountable-person own-account exception only where its conditions are met; retain Form A for 10 years; and file the prior week's reports weekly by Tuesday through the current FIA channel.	Threshold rationale, same-day log, aggregation, exception record, Form A retention and weekly receipt	AMLA Cap. 118, ss.7-8; AML Regulations 2015, reg.39; FIA reporting requirements [24]
Carry and control complete wire information	Ensure complete originator and beneficiary fields accompany domestic and cross-border wires throughout the chain; verify both parties; monitor and report incomplete transfers; restrict or terminate persistently non-compliant counterparties; freeze designated-person wires and notify FIA immediately.	Message specification, verification, repair/reject queue, counterparty action and FIA reports	AML Regulations 2015, regs.34-35
Report covered international wires	Apply FIA international-wire reporting to accountable persons facilitating those transfers. Use the exception only for financial-institution-to-financial-institution transfers where both institutions act on their own behalf.	Report file, receipt and documented exception rationale	FIA reporting requirements for international wire transfers [24]
Apply the foreign-funding payout control where section 25 applies	If the institution is licensed under an Act of Parliament to facilitate cross-border money transfers and is therefore a supervised institution under the Protection of Sovereignty Act 2026, do not pay money to an agent of a foreigner unless that agent declares the source of funds and submits proof of the declaration required under section 22(1). Submit a monthly report to the relevant regulator covering funds transferred through the institution to an agent of a foreigner, in accordance with regulations prescribed by that regulator. Do not apply this control universally to institutions, recipients or transfers outside those statutory definitions.	Licence and applicability assessment, agent-of-a-foreigner status record, source-of-funds declaration, proof of the section 22(1) declaration, payout decision, monthly regulatory report and submission receipt	Protection of Sovereignty Act 2026, ss.1, 22(1) and 25; commenced 22 May 2026 [26][27]

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Control outbound and inbound cross-border declarations	Embed procedures for currency or negotiable bearer instruments equivalent to or exceeding 1,500 currency points. For outbound movement, require Form C to be presented to a customs officer at the port of exit. For inbound movement, document the current textual conflict: AMLA section 10 and FIA operational guidance specify Form D, while regulation 10(1)(b), as substituted in 2023, states Form C. Follow current FIA operational guidance, seek written clarification where practicable and retain the guidance, advice and declaration evidence supporting the form used. Escalate a failure, refusal, neglect or false declaration under the prescribed process.	Customer notice, direction-specific workflow, completed declaration, retained FIA guidance or written clarification, customs handoff and escalation record	AMLA Cap. 118, s.10; AML Regulations 2015, reg. 10(1)(b) as substituted by AML (Amendment) Regulations 2023, reg. 10; FIA reporting guidance [01][02][20][24]
Respond to FIA and supervisor requests	Preserve search capability, legal review, secure production and an auditable response log for information requests, directives and examinations.	Request register, production package and approvals	AMLA Cap. 118, ss.20-21; sector supervisory powers

7. RECORDS, ASSURANCE AND TRAINING

Records, assurance and training

Uganda's AMLA section 7 uses record-specific trigger dates and an express whichever-is-later rule. Configure retention from the statutory event, not merely from file creation.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply the AMLA section 7 retention rule	Keep account files, business correspondence, analysis results, identity and beneficial-owner evidence, CDD information, transaction records and written findings for at least ten years from the date identity evidence was obtained, the date of the relevant transaction or correspondence, or the date the account is closed or business relationship ceases, whichever is later.	Retention schedule; trigger-date fields; automated legal hold; deletion approvals; sampled files showing the latest applicable trigger.	Anti-Money Laundering Act 2013 s.7, as substituted by Act 3 of 2017 [01][03]
Keep records reconstructable and immediately available	Maintain records sufficient to reconstruct each transaction for account holders and non-account holders, including amount and currency, and in a form that can be supplied immediately to the FIA or law-enforcement agencies.	Indexed archive; transaction reconstruction test; authority-request SLA test; access and integrity logs.	Anti-Money Laundering Act 2013 s.7(2), (4) and (6) [01]
Preserve specific cash and wire records	Keep Form A cash and monetary transaction records for ten years from transaction date, while also applying section 7's later-trigger rule to overlapping account, identity, correspondence and relationship records. Preserve wire-chain information and reporting evidence under the applicable regulations.	Form A archive; wire-message archive; overlap analysis; retrieval test.	Anti-Money Laundering Act 2013 ss.7-8; AML Regulations 2015 as amended [01][02]

8. PAYMENT SYSTEMS AND FINTECH OPERATIONS

Payment systems and fintech operations

Apply Bank of Uganda licensing and prudential controls to payment services, systems and fintech delivery.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Obtain the correct NPS licence	Classify each service or system under the National Payment Systems Act and Regulations and obtain the required payment-service-provider or payment-system-operator licence before operation.	Classification memo, application, licence and approved activities	National Payment Systems Act Cap. 59; NPS Regulations 2021
Meet capital and fit-and-proper requirements	Maintain the category-specific capital and ownership conditions and ensure directors, controllers and key officers satisfy current fit-and-proper requirements and approval processes.	Capital calculation, ownership chart, fit-and-proper files and BoU approvals	NPS Act Cap. 59; NPS Regulations 2021
Operate risk, conduct and transparency controls	Maintain governance, enterprise risk management, AML, fraud, complaints, pricing and disclosure controls proportionate to the service and BoU licence.	Policies, customer terms, fee disclosures, complaints and risk reports	NPS Act Cap. 59; NPS Regulations 2021; BoU Oversight Framework 2025
Govern agents and safeguard customer funds	Approve and monitor agents under the applicable rules, segregate or safeguard customer funds as required, reconcile balances and prevent use of safeguarded funds for the provider's own account.	Agent register, due diligence, safeguarding account, daily reconciliation and exceptions	NPS Act Cap. 59; NPS Regulations 2021
Maintain resilience and BoU reporting	Operate security, business continuity, incident response, outsourcing, recovery and data controls and submit all applicable operational, prudential, incident and statistical reports to BoU.	Resilience tests, incidents, vendor oversight and BoU receipts	NPS Regulations 2021; BoU Oversight Framework 2025

9. DATA PROTECTION AND DIGITAL OPERATIONS

Data protection and digital operations

The Data Protection and Privacy Act 2019 and Regulations 2021 govern collection, processing, security, rights, breaches and transfers. Cross-border processing has two statutory routes under section 19.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Register and assign privacy accountability	Register with the PDPO where required, keep registration current, appoint accountable privacy leadership, maintain a processing inventory and complete the required annual compliance reporting and change notifications.	PDPO certificate; renewal calendar; privacy appointment; processing inventory; annual report and change notices.	Data Protection and Privacy Act 2019; Regulations 2021; PDPO organisation guidance [13][14][15]
Process lawfully and transparently	Document a lawful basis and purpose for identity, biometric, screening and monitoring data; provide required notices; minimise collection; keep information accurate; implement retention controls; and support authenticated data-subject rights.	Privacy notices; lawful-basis register; consent records where used; rights log; DPIAs; retention schedule.	Data Protection and Privacy Act 2019 ss.7-18; Regulations 2021 [13][14]
Notify every covered security breach immediately	Where there is reason to believe personal data has been accessed or acquired by an unauthorised person, notify the PDPO immediately and follow the prescribed response process. Do not add an unsupported materiality or qualifying-breach threshold.	Incident register; PDPO notice and timestamp; containment and investigation record; data-subject communications where directed.	Data Protection and Privacy Act 2019 s.23; PDPO organisation guidance [13][15]
Use only the section 19 cross-border routes	Before processing or storing personal data outside Uganda, ensure the destination has adequate protection at least equivalent to Uganda's Act or obtain the data subject's consent. Do not rely on contract performance or an unspecified statutory condition as a section 19 transfer ground.	Destination adequacy assessment or valid consent; transfer inventory; processor contract; security review.	Data Protection and Privacy Act 2019 s.19 [13]

SOURCES AND FURTHER READING

Verify against current official material

Primary law and regulator guidance control. Contextual VOVE ID reading is included to help teams operationalize the requirements and is not legal authority.

01
Uganda Legal Information Institute (ULII) · Anti-Money Laundering Act 2013, consolidated with 2017 amendments
Open official source

02
Uganda Legal Information Institute (ULII) · Anti-Money Laundering Regulations 2015, with amendment history
Open official source

03
Uganda Legal Information Institute (ULII) · Anti-Money Laundering (Amendment) Act 2017
Open official source

18
Parliament of Uganda · Anti-Money Laundering (Amendment) Act 2022 (Act 18), official Acts 2022 collection
Open official source

22
Ministry of Justice and Constitutional Affairs Uganda · Official government record confirming the Anti-Money Laundering (Amendment) (No. 2) Act 2022 (Act 23); Parliament's public 2022 collection does not currently expose the Act 23 text
Open official source

19
Uganda Legal Information Institute (ULII) · Anti-Money Laundering (Amendment) Regulations 2022, S.I. 15 of 2022
Open official source

20
Financial Intelligence Authority Uganda · Anti-Money Laundering (Amendment) Regulations 2023, S.I. 2 of 2023
Open official source

21
Uganda Legal Information Institute (ULII) · Anti-Money Laundering (Amendment of Schedule 2) Instrument 2025, S.I. 17 of 2025
Open official source

04
Financial Intelligence Authority Uganda · Current accountable-person registration instructions
Open official source

05
Financial Intelligence Authority Uganda · Current goAML registration and STR information
Open official source

24
Financial Intelligence Authority Uganda · Direct reporting requirements for suspicious transactions, large cash transactions and international wire transfers
Open official source

25
Financial Intelligence Authority Uganda · Guidance Note on Suspicious Transaction Reports for Accountable Persons, effective 1 December 2024
Open official source

06
Financial Intelligence Authority Uganda · Current online registration guidelines
Open official source

07
Uganda Legal Information Institute (ULII) · Companies Act, current consolidated text
Open official source

08
Uganda Legal Information Institute (ULII) · Companies (Beneficial Owners) Regulations 2023
Open official source

09
Uganda Legal Information Institute (ULII) · Companies (Beneficial Owner) (Amendment) Regulations 2024, S.I. 35 of 2024, gazetted instrument record
Open official source

10
Uganda Legal Information Institute (ULII) · Anti-Terrorism Regulations 2025, SI 75 of 2025
Open official source

11
Uganda Legal Information Institute (ULII) · National Payment Systems Act, Cap. 59
Open official source

12
Uganda Legal Information Institute (ULII) · National Payment Systems Regulations 2021 and amendment history
Open official source

13
Uganda Legal Information Institute (ULII) · Data Protection and Privacy Act 2019
Open official source

14
Uganda Legal Information Institute (ULII) · Data Protection and Privacy Regulations 2021
Open official source

15
Personal Data Protection Office Uganda · Current organisational compliance and breach guidance
Open official source

16
Financial Action Task Force · Uganda removed from increased monitoring, February 2024
Open official source

17
Bank of Uganda · National Payment Systems Oversight Framework 2025
Open official source

26
Ministry of Internal Affairs Uganda · Protection of Sovereignty Act 2026 (Act 7 of 2026), official publication page
Open official source

27
Ministry of Internal Affairs Uganda · Protection of Sovereignty Act 2026 (Act 7 of 2026), enacted Act PDF
Open official source

Document control

Version 1.9 / Published 15 July 2026 / Last reviewed 15 July 2026 / Owner: VOVE ID Compliance Research

Operational guidance, not legal advice. Requirements vary by licence, activity and supervisor. Confirm the current consolidated laws, FIA directives, Bank of Uganda conditions and sector-specific rules before implementation.