VOVE ID

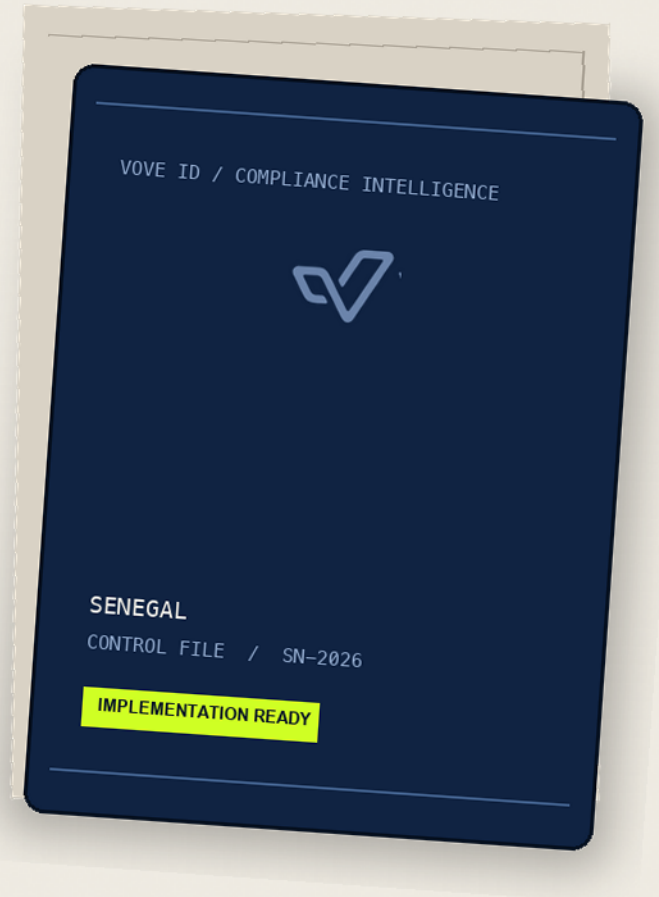
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

SENEGAL

SENEGAL / SN



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Senegal KYC, KYB & AML Compliance Checklist

An implementation-focused checklist for fintechs, payment institutions, financial institutions and other regulated businesses operating in Senegal. It translates Senegal's 2024 AML/CFT/CPF law, BCEAO payment-services rules and data-protection framework into controls, actions and audit evidence.

Primary AML law	**Law No. 2024-08**
FIU	**CENTIF Senegal**
Payments authority	**BCEAO**
Privacy authority	**CDP**
Core record period	**10 years**
FATF status	**Not under increased monitoring**

Scope and legal framework

Law No. 2024-08 of 14 February 2024 on combating money laundering, terrorist financing and proliferation financing; BCEAO Instruction No. 001-01-2024 on payment services in the WAMU; Law No. 2008-12 on personal data protection and Decree No. 2008-721.

FATF context

Senegal exited FATF increased monitoring in October 2024 and, as confirmed by FATF's 19 June 2026 statement, is not under increased monitoring. This does not remove the need for documented, risk-based controls or enhanced measures where customer, product, channel or geographic risk warrants them.

IMPORTANT

This checklist is general information, not legal advice. It is based on official materials available on 15 July 2026. Thresholds, implementing decisions, sector rules and supervisory expectations may change. Confirm applicability with CENTIF, BCEAO, the competent sector supervisor, CDP and qualified Senegalese counsel before launch.

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. CONFIRM SCOPE, AUTHORITIES AND PERMISSIONS

Confirm scope, authorities and permissions

Map every Senegal-facing activity to the applicable reporting-person category, sector supervisor and licensing perimeter before onboarding customers.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Document why the business is or is not a reporting person under Law No. 2024-08.	Map each legal entity, product and customer journey to the law's financial or designated non-financial categories; record the accountable supervisor and CENTIF reporting route.	Signed regulatory perimeter memo; entity-product matrix; counsel or compliance approval.	Law No. 2024-08, scope and reporting-person provisions
Obtain the required BCEAO permission before providing regulated payment services.	Classify account, transfer, acquiring, issuance, remittance and initiation activities against Instruction No. 001-01-2024; do not rely on a technology or agency label to bypass authorisation.	Licence, approval or documented exemption; product-to-permission mapping.	BCEAO Instruction No. 001-01-2024, arts. 4, 9 and 17
Stop unlicensed payment activity where the transition period has expired.	Confirm that the operating entity and any payment partner appear within the current authorised perimeter. BCEAO Notice No. 006-05-2025 extended the transition through 31 August 2025; from 1 September 2025, only authorised payment service providers could operate within the regulated perimeter.	Current BCEAO register check; partner due-diligence file; documented confirmation of authorisation before operation from 1 September 2025; board launch gate.	BCEAO Notice No. 006-05-2025
Treat virtual-asset services as approval-dependent and AML-regulated.	Identify custody, exchange, transfer, issuance-support or other virtual-asset functions and obtain prior approval where applicable before service begins.	Virtual-asset perimeter assessment; approval correspondence; AML control mapping.	Law No. 2024-08, arts. 58–59
Assign named owners for CENTIF, BCEAO, sector-supervisor and CDP obligations.	Maintain a responsibility matrix covering regulatory filings, suspicious transaction reporting, payment safeguarding, privacy formalities and incident escalation.	RACI; appointment letters; committee terms; regulatory calendar.	Law No. 2024-08, arts. 12–15; BCEAO Instruction No. 001-01-2024, art. 32

2. BUILD THE AML/CFT/CPF CONTROL FRAMEWORK

Build the AML/CFT/CPF control framework

The programme should be proportionate to documented risks and embedded in governance, people, systems and assurance.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a documented enterprise-wide risk assessment.	Assess customers, countries, products, services, transactions, delivery channels and new technologies; define methodology, data inputs, residual-risk logic and refresh triggers.	Approved risk assessment; methodology; risk appetite; change log.	Law No. 2024-08, arts. 12–15
Adopt written policies, controls and procedures aligned to identified risk.	Cover onboarding, beneficial ownership, PEPs, sanctions, monitoring, reporting, recordkeeping, outsourcing and control testing, with board or senior-management approval.	Policy suite; approval minutes; control library; annual review record.	Law No. 2024-08, arts. 12–15
Screen integrity and competence of relevant personnel.	Apply risk-based pre-employment checks, conflict declarations and role-specific suitability requirements for compliance-sensitive positions.	Screening standard; completed checks; conflict register.	Law No. 2024-08, arts. 12–15
Provide continuing, role-specific training.	Train the board, customer operations, investigators, product, engineering, sales and agents on their controls, escalation paths and tipping-off restrictions.	Curriculum; attendance; assessment scores; remediation log.	Law No. 2024-08, arts. 12–15 and 63
Evaluate new products and technologies before launch.	Complete AML, fraud, sanctions and privacy risk assessments before introducing material technology, channel or product changes and implement mitigating controls.	Pre-launch risk assessment; architecture review; control acceptance; launch approval.	Law No. 2024-08, arts. 12–15

3. IDENTIFY AND VERIFY CUSTOMERS

Identify and verify customers

CDD must establish who the customer is, who acts for them, who ultimately benefits and why the relationship is being opened.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify the customer and beneficial owner using reliable, independent sources.	Capture identity attributes and verify them against appropriate documents, data or trusted digital sources before the relationship or transaction, subject only to the law's narrow deferral conditions.	CDD record; verification results; source provenance; exception log.	Law No. 2024-08, arts. 16–18
Identify any person acting on behalf of the customer and verify authority.	Verify the representative, mandate and power to act; link the representative to the customer and screen both under the applicable risk rules.	Mandate or power of attorney; representative ID; verification and screening record.	Law No. 2024-08, arts. 17–18
Establish the purpose and intended nature of the relationship.	Collect expected activity, products, counterparties, geographies, source of funds and business rationale sufficient to set a risk rating and monitoring profile.	Customer profile; expected-activity baseline; risk score and rationale.	Law No. 2024-08, arts. 16 and 19–20
Apply CDD at all statutory triggers, including suspicion and relevant occasional transactions.	Configure onboarding and transaction workflows to trigger CDD for relationships, account or custody services, domestic or international transfers, linked cash activity, threshold events and any suspicion regardless of amount.	Trigger matrix; workflow rules; linked-transaction logic; test results.	Law No. 2024-08, art. 17
Use deferred verification only where every legal condition is satisfied.	Complete verification as soon as possible and before the first transaction; document why delay is essential not to interrupt normal business and how risks are effectively controlled under pre-approved procedures.	Deferral policy; case approval; no-transaction control; completion timestamps.	Law No. 2024-08, art. 18
Do not proceed when required CDD cannot be completed and file the mandatory suspicious transaction report.	Do not open the relationship, refuse the occasional transaction or terminate the relationship as applicable; submit a suspicious transaction report to CENTIF as required by article 25 without tipping off the customer.	Decline or exit record; investigation decision; STR filing receipt and restricted case record.	Law No. 2024-08, arts. 22 and 25

4. VERIFY BUSINESSES AND BENEFICIAL OWNERS

Verify businesses and beneficial owners

KYB must establish legal existence, authority, ownership and the natural persons who ultimately own or control the customer.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal name, form, constitutive documents, powers and addresses.	Obtain current registry and constitutional records, registered and principal office, governing documents, tax or sector identifiers and proof of operating status from reliable sources.	Registry extract; statutes; address proof; independent-source checks.	Law No. 2024-08, art. 26
Understand the customer's activity, ownership and control structure.	Map legal and economic activity, directors or equivalent controllers, shareholders, members, intermediate entities and control rights through every layer.	Ownership chart; director register; corporate profile; analyst notes.	Law No. 2024-08, art. 26
Apply the beneficial-owner cascade to natural persons.	Identify the natural person exercising controlling ownership; if none is identified, determine control through other means; only then identify the relevant senior managing official and document why.	BO calculation; control analysis; fallback rationale; verified BO files.	Law No. 2024-08, art. 26
Keep shareholder, member and beneficial-ownership information accurate and current.	Require event-driven notifications, periodic refresh and discrepancy escalation; reconcile customer information against available registries and reliable sources.	Registers; refresh schedule; change alerts; discrepancy cases.	Law No. 2024-08, arts. 76–79
Detect bearer, nominee, trust and similar opacity risks.	Identify nominee arrangements, bearer instruments, trusts and comparable legal arrangements; establish the relevant parties, control and purpose and apply enhanced measures where risk is elevated.	Legal-arrangement questionnaire; party verification; enhanced review.	Law No. 2024-08, arts. 80–83

5. APPLY ENHANCED AND REMOTE DUE DILIGENCE

Apply enhanced and remote due diligence

Higher-risk relationships require deeper evidence, approval and monitoring; lower-risk treatment must be justified rather than assumed.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify domestic, foreign and international organisation PEPs and relevant connected persons.	Use risk-based systems to identify PEP status and apply the statutory treatment to family members and close associates where required.	PEP screening record; relationship analysis; match disposition.	Law No. 2024-08, art. 29
Obtain senior approval and establish source of wealth and source of funds for PEP relationships.	Complete corroborated wealth and funds analysis before onboarding or continuing the relationship and obtain approval at the prescribed senior level.	Source analysis; corroborating records; signed approval.	Law No. 2024-08, art. 29
Apply enhanced, ongoing monitoring and periodically reassess former PEP risk.	Set tighter scenarios and review frequency, and reevaluate PEP profiles at least every three years while retaining risk-based treatment after public functions end.	Monitoring plan; review diary; three-year reassessment record.	Law No. 2024-08, art. 29
Control non-face-to-face identity and impersonation risk.	Use layered document, biometric or equivalent verification, device and fraud signals, liveness where proportionate, channel limits and manual escalation calibrated to risk.	Remote-onboarding standard; vendor assessment; model tests; exception cases.	Law No. 2024-08, art. 22
Document the basis for enhanced or simplified measures.	Apply enhanced controls to higher risks and simplified measures only where lower risk is demonstrated and no suspicion or mandatory enhanced-treatment condition applies.	Risk decision; control variation; approval and review date.	Law No. 2024-08, arts. 84–85

6. MONITOR ACTIVITY AND REPORT SUSPICION

Monitor activity and report suspicion

Monitoring must compare actual behaviour with the known customer and promptly escalate suspicion to CENTIF.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Keep CDD and risk profiles current throughout the relationship.	Refresh on risk-based cycles and events such as ownership change, unusual activity, document expiry, adverse information or material product change.	Refresh rules; event triggers; completed reviews; overdue dashboard.	Law No. 2024-08, arts. 16 and 19–20
Monitor transactions against customer knowledge and expected activity.	Implement scenarios and investigations covering size, frequency, velocity, counterparties, geography, channels, source of funds and unexplained changes.	Scenario inventory; tuning rationale; alerts; investigation files.	Law No. 2024-08, arts. 19–21
Examine complex, unusual or apparently purposeless activity and preserve a written analysis.	Investigate origin, destination, purpose and beneficial owner; create a confidential written report even where suspicion is not ultimately established.	Special-examination report; supporting data; reviewer sign-off.	Law No. 2024-08, art. 21
Report suspected, attempted and relevant proposed activity to CENTIF immediately.	File when there is suspicion or reasonable ground to suspect money laundering, terrorist financing, proliferation financing, a predicate offence or other statutory reporting circumstance; send supplementary information without delay.	STR decision record; filing receipt; supplement log; restricted case file.	Law No. 2024-08, art. 60
Refrain from execution before reporting unless a statutory exception applies.	Pause the transaction where required. If execution cannot be deferred, deferral would obstruct investigation, or suspicion arises afterward, notify CENTIF without delay and document the reason.	Hold decision; exception rationale; filing timestamp; release approval.	Law No. 2024-08, art. 61
Prevent tipping off and implement CENTIF opposition instructions.	Restrict knowledge of filings and inquiries. Operationalise CENTIF's opposition period of up to four days and escalation for judicial extension or provisional seizure.	Confidentiality controls; access logs; hold workflow; legal escalation record.	Law No. 2024-08, arts. 63 and 65

7. CONTROL PAYMENTS, TRANSFERS AND CASH RISK

Control payments, transfers and cash risk

Payment and transfer controls should preserve required originator and beneficiary information and identify linked or unusual activity.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Capture and transmit required originator and beneficiary information.	Map mandatory data fields across domestic, cross-border and intermediary payment flows; reject, suspend or investigate missing or unreliable information according to documented rules.	Data dictionary; message samples; missing-data rules; QA results.	Law No. 2024-08, transfer provisions, arts. 39–46
Detect linked transactions and threshold avoidance.	Aggregate related cash and occasional transactions across channels, accounts, devices, agents and the statutory time window; maintain configurable thresholds set by competent authority.	Aggregation logic; threshold register; scenario tests; cases.	Law No. 2024-08, arts. 17 and 72
Apply enhanced monitoring to unusual or unrelated deposits and cash activity.	Escalate activity inconsistent with the customer's profile, stated business or economic purpose and document source-of-funds inquiries.	Cash-risk rules; source evidence; analyst disposition.	Law No. 2024-08, arts. 21 and 72
Maintain agent and partner controls across the payment chain.	Conduct due diligence, contract for AML and data obligations, train relevant personnel, monitor performance and preserve audit and termination rights.	Partner file; contract clauses; training; monitoring dashboard.	BCEAO Instruction No. 001-01-2024, governance and risk-control requirements
Reconstruct the full payment trail.	Retain identifiers, timestamps, amounts, currencies, channels, account or wallet references, parties, screening results and decision history in an exportable format.	Sample reconstruction; lineage map; retention and access test.	Law No. 2024-08, art. 23

8. IMPLEMENT TARGETED FINANCIAL SANCTIONS

Implement targeted financial sanctions

Freezing measures must operate immediately, without prior notice, and cover funds and economic resources linked to designated persons and entities.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen customers, beneficial owners, controllers and transactions against applicable designations.	Screen at onboarding, list updates, material profile changes and before relevant transactions; include aliases, transliteration and ownership or control analysis.	List inventory; screening configuration; update logs; match files.	Law No. 2024-08, arts. 89–90
Freeze designated funds and economic resources immediately and without prior notice.	Create a 24/7 decision and technical-control path that blocks movement, alteration, use or access once the legal condition is met.	Freeze procedure; system test; incident timeline; approvals.	Law No. 2024-08, art. 89
Prevent funds or economic resources from being made available.	Control direct and indirect availability, including through owned or controlled entities, intermediaries, cards, wallets, agents and refunds.	Control mapping; ownership analysis; blocked-payment tests.	Law No. 2024-08, art. 89
Notify CENTIF and the competent authority immediately.	Maintain a controlled reporting workflow for frozen assets, attempted activity, false positives and subsequent directions.	Notification template; filing receipt; regulator correspondence.	Law No. 2024-08, art. 90
Apply sanctions controls consistently across the group.	Define group-wide minimums, local legal escalation and information-sharing safeguards so Senegal operations receive and implement designations without delay.	Group standard; local annex; update SLA; assurance results.	Law No. 2024-08, art. 89

9. RETAIN RECORDS AND SUPPORT ASSURANCE

Retain records and support assurance

Records should allow authorities and auditors to reconstruct decisions, relationships and transactions over the statutory period.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Keep identity, KYC, profile and analysis records for 10 years after closure or cessation.	Start the retention clock from account closure or the end of the business relationship and preserve documents, data, decisions and special examinations.	Retention schedule; lifecycle rules; sampled archived files.	Law No. 2024-08, art. 23
Keep transaction, accounting and correspondence records for 10 years after the transaction.	Apply transaction-based clocks and preserve sufficient detail for complete reconstruction and evidential use.	Storage configuration; transaction sample; retrieval test.	Law No. 2024-08, art. 23
Preserve corporate and beneficial-ownership records after dissolution.	Contractually and operationally ensure relevant parties keep required company and BO information for at least 10 years after dissolution or the end of the applicable relationship.	Dissolution checklist; archive owner; retention proof.	Law No. 2024-08, arts. 76–79
Protect confidentiality while enabling timely authority access.	Use least privilege, immutable logs, legal holds and controlled exports; separate STR and sanctions files from ordinary customer-service access.	Access matrix; audit logs; legal-hold test; disclosure register.	Law No. 2024-08, arts. 23 and 63
Test control design and operating effectiveness independently.	Set a risk-based compliance monitoring and independent audit plan; track findings to accountable owners and board-visible closure.	Monitoring plan; audit reports; issue register; closure evidence.	Law No. 2024-08, arts. 12–15

10. PROTECT PERSONAL AND BIOMETRIC DATA

Protect personal and biometric data

Identity verification creates high-risk personal-data processing that must be lawful, proportionate, secure and subject to CDP formalities.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map identity, biometric, corporate and monitoring data to a lawful and defined purpose.	Maintain records of processing covering source, purpose, fields, recipients, location, retention, security and rights handling; separate legal obligations from optional analytics or marketing.	Data inventory; processing register; purpose and legal-basis assessment.	Law No. 2008-12 on personal data protection
Complete applicable declarations or prior authorisations with CDP.	Classify each processing operation under CDP formalities, including sensitive or biometric processing, interconnected files and transfers to third countries, before production use where authorisation is required.	CDP filing; receipt or authorisation; processing-to-formality matrix.	CDP, Formalities; Law No. 2008-12 and Decree No. 2008-721
Provide clear notices and operationalise individual rights.	Explain controller identity, purposes, required fields, recipients, transfers, retention and rights; authenticate and log access, correction, objection or deletion requests subject to legal retention duties.	Privacy notice; request workflow; response log; exemption rationale.	CDP, Understanding your rights; Law No. 2008-12
Minimise collection and secure identity evidence.	Limit data to what is necessary, encrypt in transit and at rest, restrict access, test vendors and deletion, and maintain incident detection and response appropriate to identity and biometric risk.	Data-minimisation review; security architecture; access logs; incident plan.	CDP, Business obligations; Law No. 2008-12
Control processors, vendors and international transfers.	Perform due diligence, document instructions, confidentiality, security, sub-processing, audit, return or deletion and transfer safeguards; verify actual data locations.	Vendor assessment; data-processing terms; transfer map; audit record.	Law No. 2008-12; CDP formalities

11. OPERATE BCEAO PAYMENT-SERVICE CONTROLS

Operate BCEAO payment-service controls

Licensed payment operations require governance, safeguarding, operational resilience and customer-protection controls in addition to AML compliance.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain governance, internal control and risk-management arrangements proportionate to payment activity.	Document decision rights, control functions, risk and security frameworks, outsourcing, continuity, incident response, data protection and complaint management, and maintain the ongoing governance arrangements required for authorised payment institutions.	Governance framework; risk register; continuity tests; complaint reports; periodic governance review.	BCEAO Instruction No. 001-01-2024, art. 32
Safeguard and segregate customer funds.	Deposit undelivered customer funds no later than the next business day into cantonnement accounts that are separate and distinct from operating accounts and held at a bank or microfinance institution; reconcile safeguarded balances daily and ensure the funds are protected from claims in the payment institution's insolvency.	Cantonnement account agreements and bank or microfinance institution confirmations; next-business-day deposit records; daily reconciliations; insolvency-protection terms; shortfall escalation records.	BCEAO Instruction No. 001-01-2024, art. 48
Use only authorised institutions and partners.	Check the current BCEAO register at onboarding and periodically; verify the exact licensed entity, services, jurisdictions and restrictions rather than relying on a trading name.	Register extracts; partner licence file; periodic recheck log.	BCEAO list of authorised payment institutions, 28 February 2026
Integrate security, fraud and AML controls.	Share governed signals between fraud, cybersecurity and AML teams; define escalation for account takeover, mule activity, agent abuse and payment anomalies without weakening STR confidentiality.	Integrated scenario map; escalation SLA; incident and case samples.	BCEAO Instruction No. 001-01-2024, art. 32; Law No. 2024-08
Run a documented launch and periodic compliance gate.	Before launch and material changes, confirm licence, AML, safeguarding, privacy, outsourcing, customer terms, complaints, resilience and reporting readiness; repeat on a defined cycle.	Launch checklist; accountable approvals; periodic certification; open-risk log.	BCEAO Instruction No. 001-01-2024; Law No. 2024-08

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.

Law No. 2024-08 of 14 February 2024, Official Journal No. 7716
Republic of Senegal / Vie-Publique.sn · Primary legislation
Open official source

Instruction No. 001-01-2024 on payment services in the WAMU
BCEAO · Primary regulation
Open official source

Payment-services instruction landing page
BCEAO · Official guidance
Open official source

Notice No. 006-05-2025 extending the payment-institution transition period through 31 August 2025
BCEAO · Official notice
Open official source

Authorised payment institutions as at 28 February 2026
BCEAO · Official register
Open official source

Personal data protection legislation
Commission de Protection des Données Personnelles · Official legislation portal
Open official source

Personal data protection regulations
Commission de Protection des Données Personnelles · Official regulation portal
Open official source

Processing declarations and prior authorisations
Commission de Protection des Données Personnelles · Official compliance guidance
Open official source

Business data-protection obligations
Commission de Protection des Données Personnelles · Official compliance guidance
Open official source

Jurisdictions under increased monitoring, October 2024
FATF · Official FATF statement
Open official source

Jurisdictions under increased monitoring, 19 June 2026
FATF · Official FATF statement
Open official source

CENTIF Senegal 2024 annual report
CENTIF Senegal / Vie-Publique.sn · Official report
Open official source

Senegal 2025 national risk assessment
CENTIF Senegal / Vie-Publique.sn · Official risk assessment
Open official source

Compliance in Senegal 2026: BCEAO guide for fintech startups
VOVE ID · Contextual implementation guide
Open contextual guide

Document control

Version 1.2 / Published 15 July 2026 / Last reviewed 15 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general information, not legal advice. It is based on official materials available on 15 July 2026. Thresholds, implementing decisions, sector rules and supervisory expectations may change. Confirm applicability with CENTIF, BCEAO, the competent sector supervisor, CDP and qualified Senegalese counsel before launch.