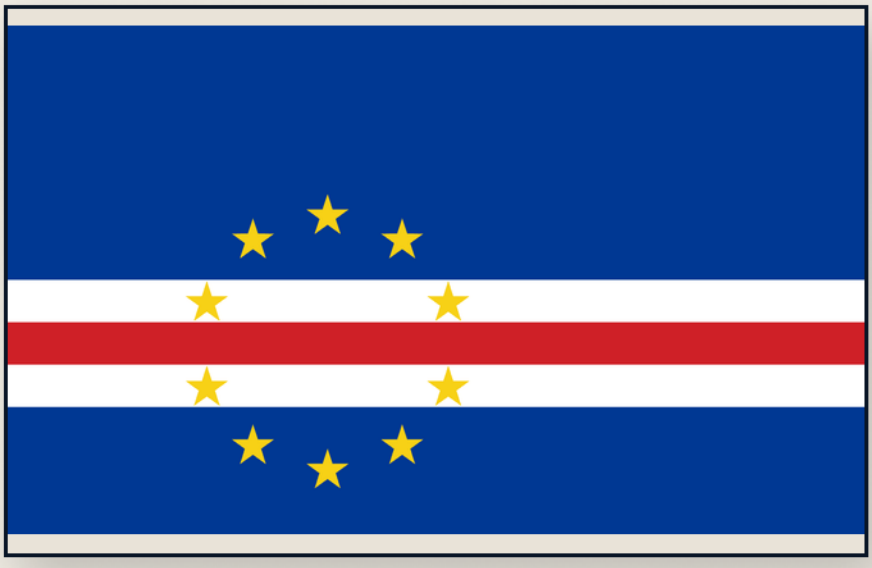
VOVE ID

VOVE COUNTRY CONTROL FILE

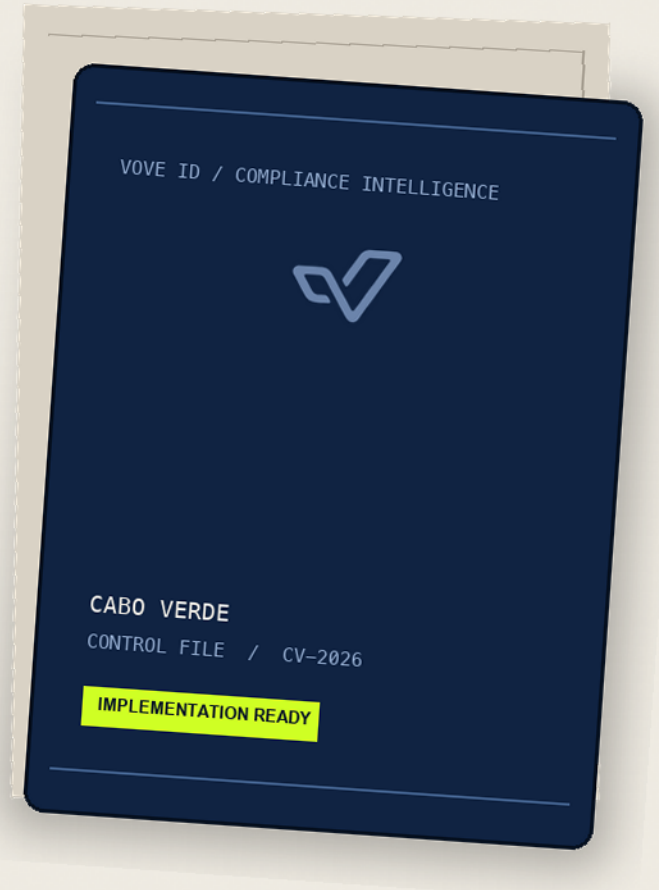
KYC / KYB / AML

2026 EDITION

CABO VERDE



CABO VERDE / CV



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Cabo Verde KYC, KYB & AML Compliance Checklist

An implementation-focused checklist for financial institutions, fintechs, virtual-asset service providers and designated non-financial businesses operating in Cabo Verde under the amended AML/CFT framework, sector rules, company-registration duties and personal-data law.

Primary AML law	**Law No. 38/VII/2009, republished by Law No. 120/VIII/2016**
Financial intelligence unit	**Unidade de Informação Financeira (UIF)**
STR timing	**Immediately on knowledge, suspicion or sufficient grounds**
Cash threshold reports	**CVE 1,000,000 for listed cash operations, including linked operations**
General occasional CDD	**CVE 1,000,000, including apparently linked transactions**
Core AML retention	**At least 7 years under transaction- and relationship-specific clocks**
Beneficial ownership	**Identify the natural person who ultimately owns or controls, or on whose behalf activity occurs**
Financial supervisor	**Banco de Cabo Verde (BCV) for BCV-supervised financial entities**
Privacy authority	**Comissão Nacional de Proteção de Dados (CNPD)**
Data-breach notice	**Notify CNPD within 72 hours unless the breach is unlikely to create risk**
FATF public lists	**Not named in the 19 June 2026 public statements**

Scope and legal framework

Law No. 38/VII/2009, republished with the amendments made by Law No. 120/VIII/2016 of 24 March, is the principal anti-money-laundering statute. Law No. 27/VIII/2013, amended by Law No. 119/VIII/2016, addresses terrorism and terrorist financing. BCV Notice No. 5/2017 applies detailed preventive controls to BCV-supervised financial services. Law No. 30/X/2023 and BCV Notice No. 2/2024 govern registration of virtual-asset service providers. Law No. 133/V/2001, as amended most recently by Law No. 121/IX/2021, governs personal-data processing.

FATF context

As at 28 July 2026, Cabo Verde was not named in FATF's 19 June 2026 statements on jurisdictions under increased monitoring or jurisdictions subject to a call for action. Cabo Verde is a GIABA member. GIABA's May 2025 sixth enhanced follow-up report kept Cabo Verde in enhanced follow-up and recorded 15 Recommendations rated non-compliant or partially compliant; the report assessed progress through 22 November 2024.

IMPORTANT	This checklist is general regulatory information, not legal advice or a licence determination. It reflects primary and authoritative materials reviewed on 28 July 2026. Confirm the live UIF filing route and forms, BCV and sector instructions, targeted-financial-sanctions workflow, company and beneficial-ownership filing requirements, data-protection notifications, product licences and all later legal changes with the competent authority and qualified Cabo Verdean 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.

Minimum review record

Keep a compact decision record for each checklist row so a later reviewer can reconstruct what applied, who decided, and what evidence was inspected.

APPLICABILITY	OWNERSHIP	TRACEABILITY
Applicable, not applicable, or pending legal confirmation, with a short rationale.	Named control owner, reviewer, approval date and next review date.	Evidence link, source version, test result, gap status and remediation ticket.

Scope, authorities and regulated activities

Resolve the entity, activity, supervisor and reporting perimeter before onboarding or launch.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
The AML law applies to listed financial institutions and designated non-financial businesses and professions headquartered in Cabo Verde, including their branches, subsidiaries and other representations at home or abroad.	Map each entity, product, branch, agent, distributor and outsourced function to the statutory list and document the competent supervisor.	Perimeter memorandum, entity-product map, licences and supervisor correspondence.	Law No. 120/VIII/2016, arts. 4, 5 and 7
UIF is the national centre for receiving, requesting, analysing and disseminating information arising from suspicious-trans action reports.	Appoint an authorised reporting contact and obtain the current UIF form, channel, access and acknowledgement instructions before production reporting.	Appointment, access record, reporting procedure, test and acknowledgements.	Decree-Law No. 9/2012; Law No. 120/VIII/2016, arts. 5-6 and 34
BCV regulates and supervises financial institutions for compliance with the AML law and its sector notices.	Classify every financial service and obtain the required BCV authorisation and registration before launch.	Classification, authorisation, registration, conditions and service map.	Law No. 120/VIII/2016, arts. 5-7; Financial System Framework Law and LAIF
Professional virtual-asset activity in Cabo Verde requires prior registration with BCV and remains subject to AML/CFT obligations.	Do not provide exchange, transfer, custody, administration or related virtual-asset services until the BCV registration and any other required approval are effective.	Service analysis, application, BCV registration, conditions and control implementation.	Law No. 30/X/2023, arts. 2-3; BCV Notice No. 2/2024

Governance, risk assessment and control ownership

Build documented, risk-based controls with accountable governance.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Reporting entities must identify, assess, understand, document and keep current their customer, geographic, product, transaction and delivery-channel ML risks.	Approve a methodology, assess risks before launch and on material change, and make the assessment available to the competent authorities.	Risk assessment, methodology, source data, change log and approvals.	Law No. 120/VIII/2016, art. 10(4)-(6)
Written policies, procedures and controls must be approved by senior management and proportionate to the entity's nature, size and activity.	Maintain a control framework covering CDD, BO, PEPs, sanctions, monitoring, reporting, records, training and group controls.	Policy suite, control library, approvals, testing and remediation.	Law No. 120/VIII/2016, arts. 10 and 28
Reporting entities must designate a management-level compliance owner and maintain independent internal control and audit arrangements.	Approve the mandate, authority, resources, access, escalation rights and independent assurance plan.	Appointment, mandate, board reporting, audit plan and reports.	Law No. 120/VIII/2016, art. 28
Employees and managers require continuous, role-appropriate AML training, and training records are retained for five years.	Deliver induction and periodic training, test understanding and retain attendance, content and results for the statutory period.	Training plan, materials, attendance, test results and five-year archive.	Law No. 120/VIII/2016, art. 29

Natural-person identification and CDD

Identify and verify customers, representatives and ultimate actors using valid independent evidence.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Customers and beneficial owners must be identified and verified when opening an account or establishing a business relationship.	Capture the statutory natural-person attributes and verify them against a valid official document bearing photograph and signature.	CDD file, document provenance, verification result, purpose and risk decision.	Law No. 120/VIII/2016, arts. 12 and 14
CDD also applies to occasional transactions and domestic or international transfers at or above CVE 1,000,000, including apparently linked transactions.	Aggregate linked activity across channels and block completion until identification and verification are complete.	Aggregation logic, threshold tests, CDD file and release decision.	Law No. 120/VIII/2016, arts. 12(2) and 15(2)
Suspicion or doubt about previously obtained identification triggers CDD regardless of amount or exemption.	Refresh and independently verify the customer, representative and beneficial owner without applying a monetary floor.	Trigger record, refreshed evidence, investigation and decision.	Law No. 120/VIII/2016, arts. 12(2)(d)-(e) and 15(2)
Anonymous, numbered, coded, fictitious-name and otherwise unidentified relationships are prohibited.	Block activation and transaction capability until the required actors are identified and verified.	Account controls, test results and rejected-case log.	Law No. 120/VIII/2016, art. 12(3)
Representatives must be identified and their authority to act verified.	Verify the representative's identity, mandate, scope, validity and relationship to the customer before accepting instructions.	Identity file, mandate, authority check and expiry monitoring.	Law No. 120/VIII/2016, arts. 12(7), 14 and 15

KYB, authority and beneficial ownership

Verify legal existence, representatives, ownership and ultimate natural-person control.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Legal-person identification includes name, nature and legal form, registered office, managers or directors and persons empowered to bind the entity.	Obtain a current commercial-registry certificate, constitutive documents, tax identifier, governing body and authority evidence; reconcile inconsistencies.	Registry certificate, statutes, NIF, officer list, mandates and discrepancy log.	Law No. 120/VIII/2016, art. 14(3)-(4); Commercial Registration Code
Reporting entities must understand the customer's ownership and control structure and determine the natural person who ultimately owns or controls it.	Trace every ownership and control layer to natural persons and document the statutory conclusion without substituting an unsupported universal percentage.	Ownership chart, control analysis, source records and verified BO files.	Law No. 120/VIII/2016, arts. 2, 12 and 15
Where the customer may be acting for another person, the entity must identify the person or entity on whose behalf the customer acts, including beneficial owners.	Investigate nominee, agency and third-party funding indicators and verify the ultimate actor before proceeding.	Agency analysis, declarations, source evidence and escalation record.	Law No. 120/VIII/2016, art. 12(6)
Commercial-register information must be kept updated, but the reviewed authoritative material does not establish a comprehensive public national BO register with a universal filing percentage.	Verify basic registry information and independently establish ownership and control; confirm current BO filing rules with DGRNI and counsel.	Registry extracts, customer ownership evidence, independent corroboration and update log.	Commercial Registration Code, art. 13; GIABA 2019 MER, Recommendation 24; controlled uncertainty

PEPs, enhanced due diligence and reliance

Apply stronger approval, evidence and monitoring where risk is higher.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
The PEP framework covers domestic and foreign PEPs, relevant international-organisation functions, family members and recognised close associates.	Screen customers, beneficial owners, controllers and representatives at onboarding, list updates and periodic review.	Screening, match rationale, relationship mapping and review record.	Law No. 120/VIII/2016, art. 2 definitions and art. 24
PEP relationships require risk-based identification, senior-management approval, source-of-wealth and source-of-funds measures and enhanced continuous monitoring.	Obtain supported source evidence and senior approval before establishing or continuing the relationship.	Source file, approval, monitoring plan and alert reviews.	Law No. 120/VIII/2016, art. 24
Former PEP controls continue while the person's profile or activity presents increased ML risk; the law does not set a fixed exit period.	Document a risk-based decision before reducing controls and continue enhanced treatment while residual risk remains.	Former-PEP assessment, approval and periodic review.	Law No. 120/VIII/2016, art. 24(2)
Remote and anonymity-favouring activity requires enhanced measures and may be supplemented with additional documents or information.	Authenticate evidence, apply independent checks and escalate higher-risk remote cases without assuming one technology is legally sufficient.	Remote-onboarding standard, vendor review, tests and exceptions.	Law No. 120/VIII/2016, arts. 10(5) and 22(3)-(4)
Reliance on a third party does not transfer the reporting entity's responsibility.	Confirm equivalent obligations and supervision, obtain identity material immediately on request, contract for access and test retrieval.	Third-party due diligence, agreement, retrieval test and exceptions.	Law No. 120/VIII/2016, art. 20

Failed CDD, monitoring and suspicious reporting

Stop unsafe activity, monitor continuously and report suspicion immediately and confidentially.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
If required ownership, control, purpose, identity or source/destination information cannot be obtained, the relationship or operation must be refused or ended and an STR considered.	Operate a controlled block or exit and preserve the confidential STR decision.	Failure reason, block, closure, analysis, STR and acknowledgement.	Law No. 120/VIII/2016, arts. 15(3), 21 and 22(7)
Unusual, complex, high-volume, atypical or apparently purposeless activity requires careful examination and a written record.	Investigate the nature, purpose, frequency, actors, amount, source, destination and payment method and retain the analysis.	Alerts, cases, supporting evidence, written examination and approval.	Law No. 120/VIII/2016, arts. 22 and 26
An STR is sent to UIF immediately when the entity knows, suspects or has sufficient grounds to suspect completed, ongoing or attempted laundering activity.	Timestamp the trigger and submit through the current UIF route without waiting for proof or a completed transaction.	Internal report, analysis, STR, UIF receipt and timeline.	Law No. 120/VIII/2016, art. 34(1)
The entity must abstain from executing suspected activity and notify UIF, subject to the statutory exception where suspension is impossible or could prejudice prevention or investigation.	Govern holds, urgent consultation, lawful post-execution reporting and restricted communications.	Hold decision, exception rationale, UIF contact, receipt and access log.	Law No. 120/VIII/2016, art. 32
The existence of an STR, UIF request or investigation must not be disclosed to the customer or an unauthorised third party.	Restrict access, use neutral customer communications and log every disclosure and escalation.	Tipping-off policy, access controls, communications and testing.	Law No. 120/VIII/2016, art. 33

Wires, thresholds, payments and agents

Keep CDD triggers, cash reports, wire information and product licensing distinct.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Listed cash operations at or above CVE 1,000,000 must be reported to UIF regardless of suspicion, including apparently linked operations and subject to the statutory activity-based exception.	Configure aggregation by customer and connected activity, apply the exact covered categories and retain report receipts and exception rationale.	Configuration, tests, reports, receipts and exception record.	Law No. 120/VIII/2016, art. 34(2)-(4)
Cross-border physical carriage of currency, bearer instruments or electronic money at or above CVE 1,000,000 requires a written customs declaration.	Do not treat the border declaration as an ordinary customer-reporting threshold; give travellers current customs instructions where relevant.	Procedure, declaration guidance and escalation record.	Law No. 120/VIII/2016, art. 11
Domestic wire transfers require specified originator and beneficiary names, account or unique reference data and alternative originator identity information.	Validate mandatory fields before release and preserve the complete payment-chain record.	Field matrix, validation, repair queue, samples and decisions.	Law No. 120/VIII/2016, art. 27(1)-(2)
Cross-border transfers at or above CVE 1,000,000 must carry the required originator information throughout the payment chain; deficient transfers require risk-based execute, reject or suspend decisions.	Implement field validation, repair, reject, suspend, beneficiary verification and follow-up rules.	Payment messages, repair requests, decisions, monitoring and tests.	Law No. 120/VIII/2016, art. 27(3)-(11)
Money or value transfer providers must maintain an up-to-date agent list and include agents within their AML programme and monitoring.	Maintain the regulator-ready agent register, due diligence, training, control testing and termination process.	Agent register, contracts, training, monitoring and remediation.	Law No. 120/VIII/2016, art. 18

Targeted financial sanctions and proliferation risk

Screen, freeze, restrict and report under the current UN and domestic implementation framework.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Relevant UN Security Council resolutions take effect in Cabo Verde's legal order, and terrorist-fund freezes require immediate implementation.	Maintain current UN lists, screen customers and transactions, prevent dealing and escalate true matches immediately.	List inventory, update logs, screening, match decision and freeze record.	Constitution of Cabo Verde, art. 12(3); Law No. 119/VIII/2016; BCV/AGMVM AML/CFT portal
Terrorist-financing and proliferation-financing targeted-sanctions implementation has documented technical-compliance gaps in GIABA assessments.	Obtain current BCV, UIF, prosecutor or other competent-authority instructions for the specific designation and do not invent a notification deadline or release route.	Legal update, authority correspondence, notification, direction and release decision.	GIABA 2019 MER and 2021 FUR, Recommendations 6-7; controlled procedure uncertainty
Virtual-asset service providers are subject to the communications, reporting and monitoring framework applicable to terrorist- and proliferation-related targeted sanctions.	Integrate UN-list screening, asset controls and authority escalation into the registered VASP control framework.	VASP policy, screening configuration, tests, escalation and reports.	Law No. 30/X/2023, art. 3; GIABA sixth enhanced FUR 2025, Recommendation 15

Records, access and assurance

Retain reconstructable records under the correct statutory clock.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identity, beneficial-owner and transaction records and required written reports are retained for at least seven years after the transaction or end of the relationship, as applicable.	Map every record class to its transaction- or relationship-based clock and apply legal holds.	Retention schedule, configuration, samples and deletion tests.	Law No. 120/VIII/2016, art. 25(1)
Financial institutions retain account-opening forms and related correspondence for at least seven years after account closure or the end of the relationship.	Link account records to the relationship closure event and test complete retrieval.	Archive configuration, closure trigger, sample and retrieval log.	Law No. 120/VIII/2016, art. 25(2)
Required records must be supplied to UIF and competent authorities on request.	Index linked identity, transaction, investigation and reporting evidence and test controlled export.	Request register, retrieval tests, access logs and response package.	Law No. 120/VIII/2016, arts. 25(3) and 31
Wire originator and beneficiary information is retained under the general seven-year rule.	Preserve complete payment messages, repairs, screening and disposition evidence for reconstructability.	Wire archive, reconstruction test and exception records.	Law No. 120/VIII/2016, arts. 25 and 27(11)

Privacy, biometrics, breaches and transfers

Apply the amended personal-data framework alongside mandatory AML processing.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Personal-data processing must respect privacy and data-protection rights and have a lawful basis, specified purpose, proportionate scope, accuracy, security and retention controls.	Inventory KYC, BO, screening, monitoring and reporting data and document purpose, basis, recipients, access and retention.	Processing register, basis assessment, notices, access matrix and retention map.	Law No. 133/V/2001 as amended by Law No. 121/IX/2021, arts. 4, 6 and 7
Biometric data are special-category data and processing is prohibited unless a statutory exception or CNPD authorisation applies.	Before facial, fingerprint, liveness-template or comparable biometric use, document the exact exception, necessity, safeguards and notification or authorisation requirements.	Legal assessment, consent where applicable, CNPD filing, encryption and access tests.	Amended personal-data law, arts. 5 and 8
High-risk processing requires a DPIA before processing and before notification to CNPD, including large-scale special-data processing and qualifying automated profiling.	Complete the DPIA, obtain DPO advice where appointed, communicate the result with the required CNPD notification and track remediation.	DPIA, DPO opinion, CNPD submission and remediation.	Amended personal-data law, art. 29
A personal-data breach must be notified to CNPD within 72 hours after awareness unless it is unlikely to create risk; a high-risk breach is communicated to affected people without unjustified delay.	Run a documented breach-triage clock, preserve the risk analysis and issue required notices with consequences and mitigation.	Incident log, awareness time, risk assessment, notices, receipts and remediation.	Amended personal-data law, arts. 27-28
Foreign transfers require an adequate protection level determined by CNPD or a statutory derogation or CNPD-authorised safeguards.	Map hosting, support and vendor destinations and document the adequacy, derogation or authorised contractual safeguards before transfer.	Transfer map, adequacy decision, derogation analysis, safeguards and CNPD authorisation.	Amended personal-data law, arts. 35-36

11. PRACTICAL EVIDENCE PACKS AND CHANGE CONTROL

Practical evidence packs and change control

Make every acceptance, escalation and regulatory decision reconstructable.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A complete customer file links identity, KYB, BO, screening, risk, approval, monitoring and reporting decisions.	Block activation where mandatory evidence or approval is missing and preserve the release decision.	Control checklist, linked file, approvals and release log.	Law No. 120/VIII/2016, arts. 8-34
Thresholds, UIF routes, sanctions directions, registers, licences and privacy procedures are time-sensitive.	Assign owners to monitor UIF, BCV, DGRNI, CNPD, the Official Gazette, FATF and GIABA on a documented schedule.	Legal inventory, source log, change assessment and implementation tickets.	Official sources listed below

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. 120/VIII/2016 republishing the amended AML law
Banco de Cabo Verde · Primary legislation
Open official source

BCV anti-money-laundering framework and supervisory role
Banco de Cabo Verde · Official regulator guidance
Open official source

UIF official role and mandate
Ministry of Justice, Cabo Verde · Official FIU guidance
Open official source

BCV Notice No. 5/2017 AML/CFT preventive controls
Banco de Cabo Verde · Primary regulator rule
Open official source

Law No. 119/VIII/2016 on terrorism and terrorist financing
Official Gazette of Cabo Verde · Primary legislation
Open official source

UN sanctions and AML/CFT resources
Banco de Cabo Verde / AGMVM · Official regulator guidance
Open official source

Law No. 30/X/2023 on virtual assets and digital banks
Banco de Cabo Verde · Primary legislation
Open official source

BCV announcement of Notice No. 2/2024 for VASP registration
Banco de Cabo Verde · Official regulator guidance
Open official source

Company and registry services portal
Ministry of Justice, Cabo Verde · Official registry portal
Open official source

Law No. 121/IX/2021 amending the personal-data regime
Comissão Nacional de Proteção de Dados · Primary legislation
Open official source

CNPD legislation index
Comissão Nacional de Proteção de Dados · Official authority index
Open official source

Cabo Verde sixth enhanced follow-up report - May 2025
FATF / GIABA · Authoritative follow-up assessment
Open official source

Cabo Verde mutual evaluation report - 2019
FATF / GIABA · Authoritative mutual evaluation
Open official source

Jurisdictions under Increased Monitoring - 19 June 2026
FATF · Authoritative public statement
Open official source

High-Risk Jurisdictions subject to a Call for Action - 19 June 2026
FATF · Authoritative public statement
Open official source

Document control

Version 1.1 / Published 28 July 2026 / Last reviewed 28 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general regulatory information, not legal advice or a licence determination. It reflects primary and authoritative materials reviewed on 28 July 2026. Confirm the live UIF filing route and forms, BCV and sector instructions, targeted-financial-sanctions workflow, company and beneficial-ownership filing requirements, data-protection notifications, product licences and all later legal changes with the competent authority and qualified Cabo Verdean counsel before launch.