VOVE ID

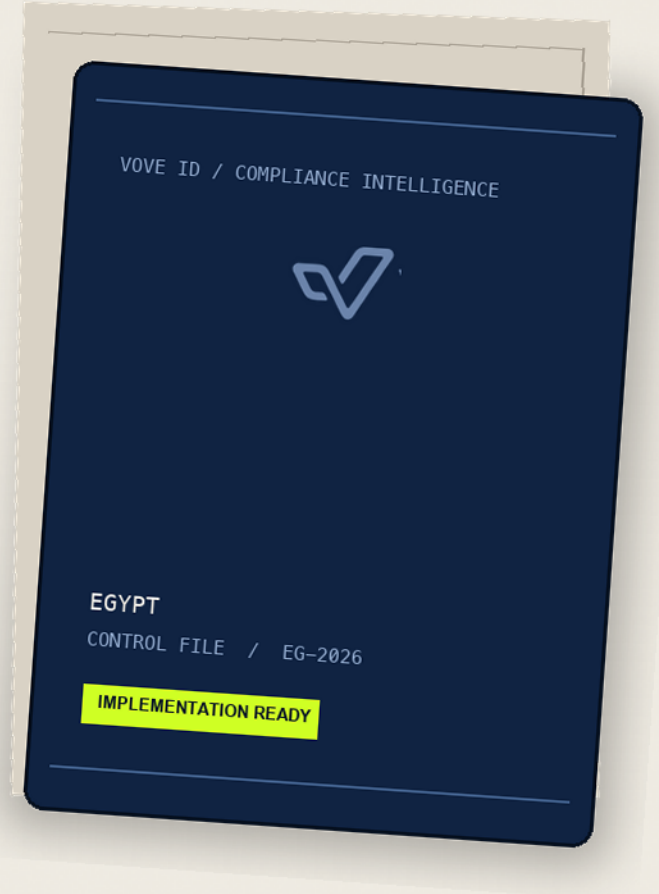
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

EGYPT

EGYPT / EG



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Egypt KYC, KYB and AML compliance checklist

A general Egypt implementation baseline under Anti-Money Laundering Law No. 80 of 2002 and its Executive Regulations, with separate Central Bank of Egypt and Financial Regulatory Authority overlays. It is not a complete sector checklist; banks, payment and remittance businesses, foreign-exchange companies, non-bank financial institutions and DNFBPs must apply the rules and reporting instructions issued for their regulated activity.

Financial intelligence unit	**EMLCU / Egyptian FIU**
Core framework	**AML Law 80/2002 and Executive Regulations**
Record retention	**At least 5 years**
Suspicion reporting	**Immediately once suspicion exists**

Scope and legal framework

Anti-Money Laundering Law No. 80 of 2002, as amended, and its Executive Regulations; Terrorist Entities and Terrorists Lists Law No. 8 of 2015, as amended; Anti-Terrorism Law No. 94 of 2015; FRA Decision No. 161 of 2024 for non-bank financial activities; and Personal Data Protection Law No. 151 of 2020 with Executive Regulations issued by Ministerial Decision No. 816 of 2025.

FATF context

Egypt was not named in FATF's jurisdictions under increased monitoring or jurisdictions subject to a call for action statements published on 19 June 2026. This is not a low-risk designation and does not replace the institution's documented customer, ownership, product, channel and geographic risk assessment.

IMPORTANT

This is a general Egypt baseline, not legal advice or a complete sector checklist. Confirm whether the activity is supervised by the CBE, FRA or another authority; obtain the current Arabic legal text, EMLCU customer-due-diligence procedures, sector circulars, reporting forms and portal instructions before implementation. Where an English translation differs from the Arabic official text, the official Arabic text controls.

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. APPLICABILITY AND GOVERNANCE

Applicability and governance

Determine the regulated activity and make the national and sector-specific AML framework operational.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map AML scope by activity	Document whether each product is a bank, payment, money-transfer, foreign-exchange, securities, financing, insurance or other financial activity, or a covered designated non-financial business or profession. Do not infer the rule set from the fintech label alone.	Activity, license and AML-scope memorandum	AML Law, art. 1; Executive Regulations
Identify the competent supervisor	Map each activity to its statutory supervisor. The CBE supervises banks, foreign-exchange companies, money-transfer entities, payment-system operators and payment-service providers. The FRA supervises insurance, capital markets, central depository and clearing, mortgage finance, financial leasing, factoring, consumer finance and MSME finance. The Ministry of Communications supervises Egypt Post's financial services other than payment systems and services. The Ministry of Trade and Industry supervises covered real-estate brokers; the Ministry of Supply and Internal Trade supervises covered precious-metals and precious-stones dealers; the Ministry of Tourism supervises covered casinos; the Egyptian Bar Association supervises covered lawyers; the Commercial Professions Syndicate supervises covered accountants; and GAFI supervises covered trust and company service providers. The EMLCU supervises covered institutions or DNFBPs for which no other supervisor applies.	Activity-to-supervisor matrix, licence inventory, applicability memo and named rule owner	AML Law, art. 1; Executive Regulations, definitions and art. 22 bis A
Apply the exact DNFBP activity and threshold scope	Apply the AML framework to real-estate brokers when buying or selling property for clients; precious-metals and precious-stones dealers conducting cash transactions of USD 15,000 equivalent or more, including linked transactions; casinos conducting transactions of USD 3,000 equivalent or more, including linked transactions; and professional trust and company service providers performing the activities listed in the Executive Regulations. Lawyers and accountants are covered only when preparing or executing for clients the purchase or sale of real estate; management of funds, securities or other assets; management of bank, savings or securities accounts; organisation of contributions for forming, operating or managing companies; or creation, operation, management, purchase or sale of legal persons, arrangements or businesses. Do not extend this automatically to ordinary litigation or legal advice. When a lawyer, accountant or similar agent supplies CDD information, professional secrecy cannot be invoked to avoid the CDD requirement.	DNFBP applicability assessment, linked-transaction aggregation, client-matter classification and CDD evidence	AML Law, art. 1; Executive Regulations, definitions and art. 22 bis A

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Appoint an AML/CFT manager and alternate	Appoint a responsible AML/CFT manager and qualified alternate from senior management. Give both the independence, confidentiality, authority and access required by Articles 35 to 37, and notify the EMLCU of their names and contact details. FRA-supervised legal persons must also comply with Decision 161/2024, register the manager and alternate in the FRA register, notify both the EMLCU and FRA of their contact details, and notify both authorities immediately when either person changes. Notify FRA within one week when the alternate assumes responsibility because of absence or when the manager leaves the institution. Apply any additional CBE or sector-specific approval and fitness requirements.	Appointments, register entry, EMLCU and FRA notifications, change log and sector approval	Executive Regulations, arts. 35-37; FRA Decision 161/2024, arts. 14-21
Approve a risk-based AML program	Maintain board-approved policies, procedures and systems covering institutional risk assessment, CDD, beneficial ownership, PEPs, targeted financial sanctions, monitoring, internal escalation, EMLCU reporting, records, training and assurance.	Approved AML/CFT program mapped to controls	Executive Regulations, art. 32; FRA Decision 161/2024, arts. 3 and 5
Assess institutional and technology risk	Conduct and document an institution-wide ML, TF and proliferation-financing risk assessment proportionate to the institution's size and activities. Cover customers, countries and geographic areas, existing and new products, services, transactions, delivery channels, business practices and technologies before use. The board must approve the assessment. Update it at least annually and whenever material change requires it, and provide the assessment and supporting material to the EMLCU or supervisor on request. Before offering a new product or service relying on modern technology, identify and assess its ML/TF risks, implement proportionate controls and coordinate with the EMLCU before launch.	Board-approved annual assessment, methodology, trigger log, launch assessment, controls and EMLCU coordination	Executive Regulations, arts. 22 bis C(6) and 29 bis
Apply the stricter sector overlay	Add current EMLCU CDD procedures, CBE or FRA rules, license conditions, reporting instructions and product-specific controls. Resolve any conflict against the binding Arabic instrument and obtain local advice where scope is uncertain.	Sector-overlay and legal-change register	Applicable regulator rule and official Arabic text

2. KYC FOR NATURAL PERSONS

KYC for natural persons

Identify the customer and representative before service, understand the purpose and keep the profile reliable.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Prohibit anonymous or fictitious relationships	Do not open or maintain accounts, accept deposits or funds, or provide covered services under anonymous, false or fictitious names.	Onboarding prohibition and exception report	AML Law, art. 8; Executive Regulations, art. 33
Identify the natural person	Collect the full legal name, official identification details, date and place of birth, nationality, address, occupation or business, contact details and other data required by the applicable EMLCU and sector procedure.	Completed customer profile	AML Law, art. 8; applicable CDD procedure
Verify with reliable independent evidence	Verify the identity before the relationship or occasional transaction using valid official documents and reliable independent data or information. Record authenticity, expiry, liveness or non-face-to-face controls where relevant.	Identity evidence and verification audit trail	Executive Regulations, art. 22 bis A
Verify representatives and authority	Identify and verify each person acting for a customer, confirm the authority to act and retain the mandate or other reliable authority evidence.	Representative KYC and authority record	Executive Regulations, art. 22 bis A(5)
Understand purpose and expected activity	Record the nature and purpose of the relationship, expected products, volumes, counterparties, geographies and source of funds needed to understand normal activity and risk.	Purpose and expected-activity profile	Executive Regulations, art. 22 bis A(2); sector CDD procedure
Resolve failed CDD	If required CDD cannot be completed, do not open the account, start or continue the relationship, or execute the transaction. Consider and document whether the reasons require an immediate suspicious-transaction report to the EMLCU.	Decline or exit and STR decision	Executive Regulations, art. 22 bis C(1)

3. KYB AND BENEFICIAL OWNERSHIP

KYB and beneficial ownership

Verify legal existence and authority, then trace ownership and control to natural persons.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify the legal entity	Obtain and independently verify the registered name, legal form, commercial-registration number and status, incorporation or governing documents, registered and operating addresses, tax details where required and regulated licenses through GAFI, the Commercial Registry, ITDA or the competent registry.	Current registry evidence and formation documents	Executive Regulations, art. 22 bis A; GAFI and ITDA procedures
Understand business activity	Document the business model, products, operating locations, expected counterparties, transaction profile and source of funds, and corroborate material claims with reliable evidence.	Business and expected-activity profile	Executive Regulations, art. 22 bis A
Verify directors, representatives and authority	Identify and verify authorized representatives and the natural persons relevant to management or control, and confirm signing, account and transaction authority using current resolutions, powers or mandates.	Connected-person KYC and authority chain	Executive Regulations, art. 22 bis A
Apply the beneficial-owner cascade	Identify and reasonably verify the natural persons with controlling ownership, then persons exercising control through other means. Only when neither can be identified after reasonable measures, identify the natural person holding the senior-management position and record why the fallback was used.	Ownership and control chart with BO rationale	Executive Regulations, art. 22 bis B(1)-(2)
Resolve legal arrangements and layers	Trace all intermediate entities and nominees. For trusts or similar arrangements identify and verify the settlor, trustee, protector, beneficiaries or class of beneficiaries and any other natural person exercising effective control.	Full structure chart and arrangement documents	Executive Regulations, art. 22 bis B(3)
Keep BO information current	Update customer and beneficial-owner data periodically and continuously, with closer attention to higher-risk customers and trigger events. Reconcile declarations against current registry, constitutional and ownership evidence and investigate inconsistencies.	BO refreshes and discrepancy outcomes	Executive Regulations, art. 22 bis C(4)-(5)

4. RISK, PEPS AND TARGETED FINANCIAL SANCTIONS

Risk, PEPs and targeted financial sanctions

Use a documented risk model for CDD and EDD while treating list-based freezing as an immediate legal control.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Assign and explain customer risk	Assess customer, ownership, product, service, channel, geography and transaction risk and retain the score, rationale, reviewer and approval. Reassess when facts or external risk information change.	Customer risk assessment and decision	Executive Regulations, art. 32; FRA Decision 161/2024, art. 3
Identify PEP exposure	Determine whether the customer or beneficial owner is or was entrusted with a prominent domestic, foreign or international-organization function. Extend the assessment to family members, close associates, persons acting on their behalf, and controlled legal persons or arrangements.	PEP screening and relationship mapping	Executive Regulations, definition and art. 32 bis
Apply mandatory PEP controls	For covered PEP relationships, obtain senior-management approval before establishing or continuing the relationship, take reasonable measures to establish source of wealth and source of funds, and apply enhanced continuous monitoring.	Approval, source analysis and monitoring plan	Executive Regulations, art. 32 bis
Screen UN and domestic designation lists	Register for EMLCU updates and monitor the relevant UN Security Council terrorism, terrorist-financing and proliferation-financing lists daily. Screen prospective and existing customers, beneficial owners, representatives and transaction parties before onboarding, before transactions and immediately after every list update. Apply Egypt's domestic terrorist-entity and terrorist lists separately under Law 8/2015.	Subscription, daily update log, screening results, alert decisions and quality assurance	FIU Decision 1/2024; Executive Regulations, arts. 52 and 53 bis A
Freeze the complete UN-designated asset perimeter	For a confirmed UN designation, freeze without delay and without prior notice all funds or assets owned or controlled directly or indirectly, wholly or jointly, including assets derived from them and assets held by persons or entities acting on behalf of or at the direction of a designated person. Do not make funds, assets, economic resources, financial services or related services available directly or indirectly to those persons or entities.	Match validation, freeze record, blocked transaction, asset-scope analysis and non-availability control	FIU Decision 1/2024; Executive Regulations, arts. 52 and 53 bis A
Apply domestic-list freezing and financing prohibitions	For domestic designations, immediately freeze the listed person's or entity's funds and assets, including jointly owned funds and generated proceeds. Prohibit direct or indirect financing, collection, receipt, transfer and similar financial services.	Domestic-list match, freeze record, financing block and legal escalation	Law 8/2015; FIU Decision 1/2024
Report every TFS implementation action immediately	Immediately notify the EMLCU and competent supervisor of every freeze, unfreeze, attempted transaction and other implementation action. Preserve the related records and release or deal with frozen assets only under an authorised exemption, delisting or unfreezing decision.	Immediate notification, receipt, attempted-transaction record, release authority and case file	FIU Decision 1/2024; Executive Regulations, arts. 52 and 53 bis A

5. ENHANCED DUE DILIGENCE

Enhanced due diligence

Increase information, verification, approval and monitoring in proportion to identified higher risk.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Collect additional information	Obtain further customer, ownership, control, business, geography, purpose and transaction information needed to understand and mitigate the higher risk.	EDD information pack	Risk-based CDD procedures and sector controls
Corroborate identity and activity	Use additional reliable independent sources to verify identity, legal existence, ownership, expected activity, source explanations and the reason for complex or unusual features.	Independent corroboration record	Executive Regulations, arts. 22 bis A-C
Establish source of funds and wealth	Establish and, where risk requires, corroborate source of funds and source of wealth. Apply the specific source and approval controls required for PEPs.	Source evidence and plausibility analysis	Executive Regulations, art. 32 bis
Obtain senior approval	Require documented senior-management approval for PEP relationships and other higher-risk relationships specified by the institution's policy or sector rule, including conditions for acceptance or continuation.	Approval and conditions	Executive Regulations, art. 32 bis; internal risk policy
Increase ongoing scrutiny	Set tighter refresh cycles, monitoring scenarios, alert thresholds and escalation requirements proportionate to higher risk and record how the measures reduce that risk.	EDD monitoring plan and reviews	Executive Regulations, arts. 22 bis C and 32 bis

6. ONGOING DUE DILIGENCE AND FINTECH CONTROLS

Ongoing due diligence and fintech controls

Keep customer knowledge current and connect onboarding data to monitoring, investigations and product change.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor throughout the relationship	Monitor transactions and behavior for consistency with the customer's identity, business, ownership, risk, expected activity and source of funds, and identify attempted as well as completed suspicious activity.	Monitoring rules, alerts and case outcomes	Executive Regulations, arts. 32 and 36
Refresh on risk and trigger events	Update CDD, beneficial ownership, authority and risk information periodically and when ownership, management, product use, geography, behavior, sanctions or other material facts change.	Review schedule and event-driven reviews	Executive Regulations, art. 22 bis C(4)-(5)
Examine unusual activity promptly	Route unusual and internally reported activity to the AML/CFT manager through secure channels, investigate promptly and retain the facts, analysis and reporting or closure rationale.	Investigation file and decision	Executive Regulations, art. 36; FRA Decision 161/2024, art. 6
Govern technology and outsourcing	Document data coverage, model or rule logic, alert handling, access, change control, testing and human oversight for automated KYC, screening and monitoring. Assess reliance on third parties without outsourcing accountability.	System inventory, tests, vendor controls and change records	Executive Regulations, art. 22 bis C(6); FRA Decision 161/2024, arts. 3 and 5
Maintain a linked audit trail	Ensure monitoring and case teams can retrieve onboarding purpose, expected activity, ownership structure, risk rating, screening history and prior reviews so KYC is not treated as a static file.	Linked customer, monitoring and case record	Recommended implementation control; lifecycle obligations
Apply payment and messaging updates	Banks operating in Egypt must apply the CBE's ISO 20022 migration for SWIFT messaging used in interbank financial transfers from 21 June 2026. Do not extend this announcement to non-bank payment businesses unless a separate binding CBE circular or licence condition applies to their service.	Bank-scope decision, migration evidence, message validation and any separate non-bank CBE authority	CBE ISO 20022 announcement, 21 June 2026
Apply the CBE PSO and PSP licensing transition	Map payment-system-operator and payment-service-provider activities to the CBE Rules for Licensing and Registration issued in June 2025. Existing payment institutions were required to regularise their position and apply for a CBE licence within the one-year transition ending in June 2026; do not continue covered activity without the required licence, registration or documented CBE status.	Activity classification, transition assessment, CBE application or licence, governance and remediation	CBE PSO/PSP Licensing and Registration Rules, 17 June 2025

7. REPORTING, RECORDS, PRIVACY AND ASSURANCE

Reporting, records, privacy and assurance

Report immediately, prevent tipping off, retain retrievable evidence and align privacy implementation with the 2025 regulations.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
File suspicious-transaction reports immediately	The AML/CFT manager must notify the EMLCU immediately once suspicion exists, regardless of transaction value, including attempted transactions. Internal review must be prompt and must not be used to delay reporting.	STR reference, decision and timeline	Executive Regulations, art. 36(3); FRA Decision 161/2024, art. 6
Use the prescribed secure channel	Use the current EMLCU form and secure electronic channel assigned to the institution. Confirm the supervisor's current portal instruction; CBE's 16 April 2026 circular specifically requires foreign-exchange companies to implement goAML.	Portal registration, filing receipt and channel matrix	EMLCU instructions; CBE circulars; FRA STR forms
Prevent tipping off	Do not disclose directly or indirectly to the customer, beneficiary or unauthorized persons that a suspicious report, examination, investigation or related measure exists. Restrict access to need-to-know personnel.	Access controls and communications guidance	AML Law, art. 11; Executive Regulations, art. 34 bis A
Retain retrievable AML records	Keep transaction, customer, representative and beneficial-owner records for at least five years from account closure or completion of an occasional transaction, and longer when requested by the EMLCU or investigating authorities. Preserve reports, analysis, screening, freezing, training and assurance records under applicable rules.	Retention schedule and retrieval evidence	AML Law, art. 9; Executive Regulations, art. 34; FRA Decision 161/2024, arts. 8-9
Submit governance and sector returns	Prepare the AML/CFT manager's report at least annually for the board and EMLCU. FRA-supervised entities must also meet Decision 161/2024 reporting requirements, including the semiannual suspicion-statistics report to FRA within one week after the period ends and applicable annual reports.	Board reports, EMLCU submission and FRA returns	Executive Regulations, art. 38; FRA Decision 161/2024, art. 6
Implement the PDPL transition	Complete the PDPL transition no later than 1 November 2026. Map each processing purpose to a lawful basis, including legal-obligation processing required for AML compliance rather than relying on blanket consent. Obtain the controller, processor, sensitive-data and other PDPC licences or permits applicable to the processing. A legal-person controller or processor must appoint and register a qualified DPO and maintain accessible DPO contact details. Before a cross-border transfer, determine whether a statutory exception applies. Otherwise obtain the required PDPC licence or permit, confirm the destination's adequacy, obtain the data subject's consent and implement the required contractual, security and record controls. Notify the PDPC within 72 hours after becoming aware of a personal-data breach, immediately when national-security considerations are involved, and notify affected data subjects within three business days after notifying the PDPC. Preserve AML records where AML legislation overrides an erasure or ordinary retention request.	Transition plan, lawful-basis register, licences, registered DPO, transfer assessment, contracts, breach chronology and AML retention override	PDPL 151/2020; Ministerial Decision 816/2025; official PDPC and DPO guidance

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Train, test and remediate	Where FRA Decision 161/2024 applies, train relevant employees at least annually. Require the internal-audit function to prepare a report for each calendar year on the AML/CFT manager's work and the institution's compliance. Prepare that report within 15 days after the reporting period, submit it to the board for approval, and provide the approved report to FRA within 45 days after the period ends, together with the external-auditor report. Engage an external auditor registered with FRA to review the internal-control environment, the internal-audit report and compliance with AML/CFT/CPF requirements. The external auditor must provide an annual report to both the institution and FRA within 45 days after the reporting period ends. For institutions outside FRA supervision, apply the training, internal-review and independent-assurance requirements imposed by the applicable sector rule. Independent assurance is recommended only where no binding rule makes it mandatory.	Annual training records, internal-audit report, board approval, FRA submission receipt, registered external-auditor appointment and annual external-auditor report	FRA Decision 161/2024, arts. 7 and 10-11

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.

Anti-Money Laundering Law No. 80 of 2002, current Arabic consolidated text
Financial Regulatory Authority · primary
Open official source

Executive Regulations of Anti-Money Laundering Law No. 80 of 2002, current Arabic text
Financial Regulatory Authority · primary
Open official source

Anti-Money Laundering Law No. 80 of 2002, historical English translation
General Authority for Investment and Free Zones · primary
Open official source

Egyptian AML/CFT system and sector-supervisor map
Central Bank of Egypt · primary
Open official source

AML/CFT regulations for banks and foreign-exchange companies
Central Bank of Egypt · primary
Open official source

CBE compliance guidance and record-retention FAQ
Central Bank of Egypt · primary
Open official source

CBE circulars, including the 16 April 2026 goAML requirement for foreign-exchange companies
Central Bank of Egypt · primary
Open official source

FRA AML/CFT system, legislation, forms and guidance
Financial Regulatory Authority · primary
Open official source

FRA Decision No. 161 of 2024 on AML/CFT controls for non-bank financial activities
Financial Regulatory Authority · primary
Open official source

FIU Decision No. 1 of 2024 on targeted financial sanctions
Egyptian FIU via Financial Regulatory Authority · primary
Open official source

Company incorporation and company-amendment services
General Authority for Investment and Free Zones · primary
Open official source

Commercial Registry legislation and procedures
Internal Trade Development Authority · primary
Open official source

Official PDPC Data Subject Consent Guidelines citing Law No. 151/2020 and Decision No. 816/2025
Personal Data Protection Center · primary
Open official source

CBE Rules for Licensing and Registration of PSOs and PSPs, 17 June 2025
Central Bank of Egypt · primary
Open official source

Egypt's Economic Rise and KYB's Role
VOVE ID - contextual reading · context
Open official source

Egyptian Personal Data Protection Center official portal
Personal Data Protection Center · primary
Open official source

Official Data Protection Officer guidance
Personal Data Protection Center · primary
Open official source

ISO 20022 migration announcement, 21 June 2026
Central Bank of Egypt · primary
Open official source

Jurisdictions under Increased Monitoring, 19 June 2026
FATF · primary
Open official source

Document control

Version 1.0 / Published 15 July 2026 / Last reviewed 15 July 2026 / Owner: VOVE ID Compliance Research

This is a general Egypt baseline, not legal advice or a complete sector checklist. Confirm whether the activity is supervised by the CBE, FRA or another authority; obtain the current Arabic legal text, EMLCU customer-due-diligence procedures, sector circulars, reporting forms and portal instructions before implementation. Where an English translation differs from the Arabic official text, the official Arabic text controls.