maatGroup
MADRID – GENEVA – LONDON -ISTANBUL

Code of Business Conduct and Ethics

Individual edition

Review copy for internal validation

13 November 2026

Includes validation notes for regulatory references and statements about implementation.

Code of Business Conduct and Ethics

Purpose and scope

This Code sets the standards for conducting the business of MAAT INTERNATIONAL GROUP, its subsidiaries and controlled affiliates (the Company). Where this Code sets a higher standard than commercial practice or applicable law, follow the higher standard to the extent permitted by law.

The Code applies to directors, officers, employees, commercial agents, consultants and business partners acting in the Company's name or on its behalf. Ask your supervisor or the Legal Department for guidance if you are unsure how to apply the Code.

Reporting and protection against retaliation

Anyone covered by this Code must promptly report known or suspected violations of the Code, Company policies or applicable laws and regulations. Report concerns to your supervisor, who will refer them to the Legal Department for investigation. If you are uncomfortable reporting to your supervisor or receive an unsatisfactory response, contact the Legal Department directly. Reports must be handled sensitively and with discretion.

The Company prohibits retaliation against anyone who seeks guidance or reports a concern in good faith. Retaliation may lead to disciplinary action, up to and including termination of employment.

Conflicts of interest

Avoid personal interests that interfere, or could reasonably appear to interfere, with your ability to act objectively and in the Company's interests. Examples include the following.

- Outside work. Avoid employment, directorships or service arrangements with a material customer, supplier or competitor.
- Personal benefits. Do not use your Company role to obtain improper material benefits or favors.
- Financial interests. Avoid significant financial interests in a material customer, supplier or competitor. A significant interest includes ownership of more than 1% of its equity or an investment exceeding 5% of your total assets.
- Personal transactions. Avoid personal loans, guarantees and other financial transactions with a material customer, supplier or competitor. Arm's-length transactions with banks, brokerages and other financial institutions are permitted.
- Family relationships. Consider whether the actions of a spouse or life partner, sibling, parent, in-law or child could affect your objectivity. This includes relationships by blood or adoption.

Disclose actual, potential or reasonably perceived conflicts to your supervisor or the Legal Department. Ask the Legal Department if you are unsure whether a customer, supplier or competitor is material.

Corporate opportunities

Present opportunities identified through your Company role, information or property to the Company before pursuing them personally. Disclose the proposed terms to MAAT's directors. Your supervisor will consult the Legal Department and relevant management. If the Company waives the opportunity, you may pursue it on the original terms, subject to this Code. Do not use Company resources or your position for personal gain or to compete with the Company.

Confidential information

Protect nonpublic information that could benefit competitors or harm the Company or its customers if disclosed. This duty covers information belonging to the Company and its business partners and continues after your relationship with the Company ends. Disclosure is permitted when authorized or legally required. Refer questions about required disclosures to the Legal Department. Unauthorized disclosure can cause competitive harm and expose the Company and individuals to liability.

Competition and fair dealing

Treat colleagues, customers, suppliers and competitors fairly. Do not gain an unfair advantage by manipulating or concealing information, misusing privileged information or misrepresenting material facts.

Company assets and communications

Use Company funds, property and systems efficiently and for authorized business purposes. Improper or unlawful use is prohibited. Take reasonable care to prevent theft, damage and misuse, and report suspected incidents to your supervisor. Use Company communications services and written materials primarily for business, and safeguard software, records and communications against unauthorized access.

Company systems and business records include electronic, telephone and written communications. Any monitoring or disclosure to authorities is subject to applicable privacy, employment and other laws. [V3]

Books and records

Maintain materially complete, accurate and reliable records, including transaction and booking records, payroll, time records, expense reports, email, accounting and performance data and other business files. Undisclosed or unrecorded funds, payments or receipts are prohibited. Follow the applicable recordkeeping policy and raise questions with your supervisor. [V4]

Compliance with laws and sanctions

Comply with the laws and regulations that apply to your work. These include requirements relating to fraud, bribery, kickbacks, gifts, intellectual property, privacy, insider trading, political contributions, competition, environmental protection, employment, health and safety, financial reporting and misuse of corporate assets. Consult your supervisor or the Legal Department when in doubt.

Follow applicable sanctions and trade restrictions, including relevant programs administered by the U.S. Office of Foreign Assets Control (OFAC). Restrictions may target particular parties, assets or transactions, or apply more broadly. [V2]

Community engagement and political activity

The Company seeks to engage responsibly with the communities in which it operates. Company funds or assets may be used for contributions to political parties or candidates only with prior Legal Department approval and where lawful. Individuals may make lawful contributions using their own funds without reimbursement and may volunteer on their own time outside working hours. Company facilities may be made available for limited political events, such as speeches by public officials or candidates, with Legal Department approval. Make clear that your views and actions are personal, and do not use Company letterhead for personal political activities. [V4]

Foreign corrupt practices and international business

Comply with the U.S. Foreign Corrupt Practices Act (FCPA) where applicable. The FCPA prohibits covered persons and entities from corruptly offering, promising, authorizing or providing anything of value, directly or through an intermediary, to covered foreign officials, political parties, party officials or candidates to obtain or retain business or secure an improper advantage in connection with business. Covered officials may include officials of public international organizations. Violations can carry civil or criminal penalties. [V2]

Company officers must complete the required FCPA training. Promptly report suspected violations to the Legal Department. Reports may be made anonymously where supported by the reporting mechanism and permitted by law. Knowingly violating the FCPA, directing a violation or knowingly allowing a subordinate to violate it may result in discipline, including termination. The Company's FCPA and Anti-Corruption Law Compliance Guide is incorporated by reference, subject to confirmation of the approved version. [V4]

Facilitation payments

The source versions contain different rules. The Code of Business Conduct and Ethics describes prior written approval by the Legal Department and accurate expense recording for potentially permissible payments for routine governmental action. Its examples include arranging telephone service and expediting a shipment through customs. Any statutory exception is narrow and depends on the facts and applicable laws. The Global Code and the Global Anti-Corruption and Anti-Bribery Policy prohibit facilitation payments, with a potential exception where personal safety is at risk. Refer any question to the Legal Department for confirmation of the governing policy. [V1]

Other international requirements

Staff with significant responsibilities for international transactions must understand the laws that apply to their activities. Refer any boycott-related request or concern to the Legal Department for assessment under applicable anti-boycott rules, including U.S. rules where relevant. [V2]

Environment, health and safety

The Company seeks to provide a safe and healthy workplace, prevent harm to people and the environment, and improve its environmental, health and safety performance. Comply with applicable laws and Company policies. Violations may result in legal liability and disciplinary action, up to and including termination. Ask the Legal Department if you need guidance.

Prevent pollution, conserve resources and reduce waste and emissions through measures such as recycling and energy conservation. Promptly report suspected environmental violations and incidents that could release hazardous materials. Take particular care when storing, transporting and disposing of waste, handling toxic materials or managing releases to air, land or water. Report unsafe conditions or tasks immediately to your supervisor or Human Resources.

Employment practices

The Company promotes fair employment practices and asks its major contractors to do the same. Follow applicable labor and employment laws, including rules on discrimination, freedom of association, privacy and collective bargaining. Violations may result in legal liability and discipline, up to and including termination. Direct questions to the Legal Department or Human Resources.

The Company provides equal opportunity and fair treatment based on merit, regardless of race, color, religion, national origin, sex (including pregnancy), sexual orientation, age, disability, veteran status or

any other protected characteristic. Harassment is prohibited whether physical or verbal and whether committed by managers, other staff or third parties. It includes unwanted sexual advances or propositions, verbal abuse, sexually or racially degrading language and sexually suggestive displays. Managers must immediately refer suspected or reported harassment or discrimination to Human Resources.

Status and acknowledgment

This Code sets standards of conduct. It creates no employment contract or guarantee of continuing policy. The Company may amend, supplement or discontinue the Code, subject to applicable law and any required notice.

I acknowledge that I have received, read and understood this Code and agree to comply with its policies and procedures. I understand that I may contact the Legal Department with questions about the Code or reporting a suspected conflict of interest or other violation.

Name _____

Signature _____ Date _____

Validation notes

The numbered references in the text identify statements that require legal or operational confirmation.

V1. Governing rule on facilitation payments

Part I describes prior written approval and expense reporting for a limited category of payments. Parts II and IV prohibit facilitation payments, subject to a potential personal safety exception. Obtain the approval history, identify the governing rule and harmonize the codes and policies. A statutory exception under the U.S. FCPA does not establish permission under other laws or company policy.

V2. Legal applicability

Map legal entities, jurisdictions, activities and transaction flows to applicable anti-bribery, accounting, anti-boycott, trade and sanctions requirements. Confirm the U.S. nexus, including the separate scope of FCPA anti-bribery and accounting provisions. Verify applicable EU and UK measures and relevant national implementing laws. Distinguish legal requirements, conventions, guidance and voluntary standards.

V3. Monitoring, disclosure and privacy

The source asserts that users have no expectation of privacy and that the Company may monitor all communications where lawful. Validate the legal basis, scope, notices, retention, safeguards and disclosure process for each relevant jurisdiction. The revised text conditions monitoring and disclosure on applicable law. Confirm the effective privacy and security controls before external publication.

V4. Policies, reporting and training

Verify approved policies, their owners and effective dates, including the Compliance Handbook, FCPA guide and recordkeeping policy. Confirm how staff access confidential and anonymous reporting, which

teams receive reports, and how non-retaliation, training and investigations are evidenced. Confirm the stated political contribution and facilities approval process and the gifts and hospitality controls.

Official references

U.S. Department of Justice and SEC · FCPA Resource Guide

EUR-Lex · General Data Protection Regulation, including Article 88

maatGroup

MADRID – GENEVA – LONDON -ISTANBUL

Global Code of Business Conduct, Ethics and Compliance

Reviewed English source edition

Review copy for internal validation

13 November 2026

Includes validation notes for regulatory references and statements about implementation.

Global Code of Business Conduct, Ethics and Compliance

1. Purpose and scope

This Code sets the standards of professional conduct for MAAT INTERNATIONAL GROUP, its subsidiaries, affiliates and controlled entities (the Company). It applies to directors, officers, employees, consultants, agents, contractors and business partners acting on behalf of the Company. The Company is committed to complying with the laws that apply in the jurisdictions where it operates.

The compliance framework encompasses this Code, the Global Compliance Handbook, the Anti-Corruption Policy, the AML and Sanctions Compliance Policy, the Third-Party Due Diligence Policy, the Compliance and Governance Structure, and the Regulatory and Compliance Map. [V4]

2. Core ethical principles

- Integrity. Conduct business honestly and transparently.
- Accountability. Take responsibility for your actions and compliance obligations.
- Transparency. Document business activities and maintain accurate records.
- Fair competition. Support open and fair markets.
- Respect for law and society. Respect applicable laws, human rights and environmental standards.

3. International legal and compliance requirements

Follow applicable local and international requirements and Company standards. Relevant legal regimes may include the U.S. Foreign Corrupt Practices Act (FCPA), UK Bribery Act 2010, EU anti-money laundering and anti-corruption measures, national laws implementing Directive (EU) 2019/1937 on whistleblower protection, applicable sanctions, competition and antitrust laws, and the EU General Data Protection Regulation (GDPR). The OECD Anti-Bribery Convention and the United Nations Convention against Corruption are international instruments that inform domestic laws and compliance standards. [V2]

4. Anti-corruption and anti-bribery

The Company prohibits bribery and corruption in both the public and private sectors. Employees and representatives must never, directly or indirectly, offer anything of value to secure an improper business advantage, make improper payments to influence public officials, accept bribes or kickbacks, or use intermediaries to conceal improper payments.

5. Facilitation payments

This Code prohibits facilitation payments regardless of local custom. The only potential exception is a threat to personal safety. [V1]

6. Gifts, hospitality and entertainment

Offer gifts and hospitality only where lawful, reasonable, proportionate, transparently recorded and free of any intent to improperly influence a decision. Excessive gifts, luxury hospitality and concealed benefits are prohibited. [V4]

7. Third-party integrity and due diligence

Conduct risk-based due diligence before engaging agents, consultants, distributors, lobbyists, intermediaries or joint venture partners. Contracts must include anti-corruption representations, compliance obligations, audit rights and termination rights in cases of misconduct. [V5]

8. Conflicts of interest

Avoid conflicts between personal and Company interests. Examples include financial interests in suppliers or competitors, improper benefits, family relationships that influence decisions and outside work that impairs objectivity. Disclose potential conflicts to the Legal or Compliance Department.

9. Books, records and accounting

Document and record transactions accurately under applicable accounting standards. Do not create undisclosed accounts, enter false transactions, hide payments or manipulate records. [V4]

10. Anti-money laundering

The Company is committed to preventing money laundering and terrorist financing. Staff responsible for these controls must verify counterparties' identities, monitor unusual transactions, report suspicious activity and follow applicable anti-money laundering requirements. [V5]

11. Sanctions and international trade

Comply with applicable sanctions, including relevant U.S., EU, UN and UK measures. Do not conduct transactions involving sanctioned persons, entities or jurisdictions where prohibited. [V2] [V5]

12. Confidentiality

Protect confidential Company and client information, trade secrets and strategic information. These obligations continue after employment ends.

13. Fair competition and antitrust

The Company prohibits price fixing, market allocation, bid rigging and other anticompetitive agreements. Follow the competition and antitrust laws that apply to your activities.

14. Whistleblower protection

Report concerns about corruption, fraud, legal violations or ethical misconduct to a supervisor, the Legal or Compliance Department, or an available confidential reporting channel. The Company prohibits retaliation against whistleblowers. [V4]

15. Environmental and social responsibility

The Company seeks to reduce its environmental impact, use resources responsibly, support community development and uphold international human rights standards.

16. Equal opportunity and workplace conduct

The Company promotes equal opportunity and a workplace free from discrimination, harassment, abuse and retaliation. Equal opportunity applies regardless of race, gender, nationality, religion, sexual orientation, disability or age.

17. Compliance program and training

The risk-based compliance program calls for training, risk assessments, internal controls, monitoring, audits and periodic policy updates. Employees must complete required training. [V4]

18. Violations and disciplinary measures

Violations may lead to disciplinary action, including termination, and may result in legal proceedings or civil or criminal liability.

19. Acknowledgment

Employees and representatives must confirm that they received and understood this Code and agree to comply with it.

Validation notes

The numbered references in the text identify statements that require legal or operational confirmation.

V1. Governing rule on facilitation payments

Part I describes prior written approval and expense reporting for a limited category of payments. Parts II and IV prohibit facilitation payments, subject to a potential personal safety exception. Obtain the approval history, identify the governing rule and harmonize the codes and policies. A statutory exception under the U.S. FCPA does not establish permission under other laws or company policy.

V2. Legal applicability

Map legal entities, jurisdictions, activities and transaction flows to applicable anti-bribery, accounting, anti-boycott, trade and sanctions requirements. Confirm the U.S. nexus, including the separate scope of FCPA anti-bribery and accounting provisions. Verify applicable EU and UK measures and relevant national implementing laws. Distinguish legal requirements, conventions, guidance and voluntary standards.

V4. Policies, reporting and training

Verify approved policies, their owners and effective dates, including the Compliance Handbook, FCPA guide and recordkeeping policy. Confirm how staff access confidential and anonymous reporting, which teams receive reports, and how non-retaliation, training and investigations are evidenced. Confirm the stated political contribution and facilities approval process and the gifts and hospitality controls.

V5. AML, sanctions and third-party controls

The Global Code states identity verification and monitoring as obligations. The AML policy uses discretionary language. Confirm the legal triggers, responsible teams, due diligence thresholds, screening sources, escalation procedures, monitoring coverage and external reporting obligations. Verify use of contractual clauses, attestations, audit rights and payment controls with actual records.

Official references

U.S. Department of Justice and SEC · FCPA Resource Guide

maatGroup

MADRID – GENEVA – LONDON -ISTANBUL

Compliance and Governance Structure

English edition from the Spanish source

Review copy for internal validation

13 November 2026

Includes validation notes for regulatory references and statements about implementation.

Compliance and Governance Structure

Corporate compliance framework

MAAT INTERNATIONAL GROUP is committed to integrity, business ethics and compliance in its international operations, trading, digital infrastructure, asset tokenization and blockchain-based activities. The framework sets out the responsibilities and controls to be established or maintained under the Code of Conduct, Compliance Handbook, Anti-Corruption Policy, AML and Sanctions Compliance Policy, Third-Party Due Diligence Policy and this governance document. [V4] [V6]

1. Board of Directors

The Board holds ultimate oversight of corporate governance and regulatory compliance. It approves compliance policies and the anti-corruption and anti-money laundering (AML) programs, monitors regulatory risks and reviews material incidents. The Compliance Committee is to report periodically to the Board on program status and significant risks.

2. Compliance Committee

The Committee oversees the implementation and operation of the compliance program. Its specified membership is one Board member, the Compliance Officer, Legal Counsel and the CFO or Finance Director. It reviews regulatory risk, approves high-risk due diligence and oversees internal investigations. The intended meeting schedule is quarterly and as needed for material incidents. [V6]

3. Compliance Officer

The Compliance Officer implements and oversees the compliance program, monitors regulatory compliance, oversees AML and anti-corruption controls and third-party due diligence, manages the reporting channel and coordinates investigations. The role requires operational independence and direct access to the Board or Compliance Committee. [V6]

4. Legal and Regulatory Affairs

This function works with the Compliance Officer on legal compliance across jurisdictions, contract review, regulatory advice and international sanctions compliance.

5. Risk Management

Risk Management identifies, assesses and manages risks in financial operations, international trading, asset tokenization and blockchain technology. It maintains the risk matrix, assesses regulatory exposure and implements preventive controls.

6. Finance and Internal Controls

This function oversees accounting controls, fraud prevention, payments and financial records. Its responsibilities include transparent accounting, appropriate controls over third-party payments and compliance with applicable FCPA accounting provisions. [V2] [V5]

7. AML and Financial Crime Unit

The unit’s remit covers risks in international trading, digital assets and asset tokenization. Its responsibilities include know-your-customer and know-your-business (KYC/KYB) checks, sanctions

screening, suspicious transaction detection and controls informed by relevant Financial Action Task Force (FATF) standards. [V5] [V6]

8. Third-Party Due Diligence Unit

This unit assesses agents, intermediaries, brokers, technology partners and joint ventures. Its functions include verifying ultimate beneficial ownership, screening for sanctions, conducting reputational checks and approving business relationships under the applicable approval procedures. [V5] [V6]

9. Internal Audit

Internal Audit independently assesses internal controls, regulatory compliance and operational risk, with direct reporting to the Board or the Compliance Committee. [V6]

10. Whistleblower and Ethics Channel

The channel is intended for reports of corruption, fraud, abuse of authority and financial irregularities. Its governing principles are confidentiality, anonymity where feasible and protection against retaliation. [V4]

Reporting structure

The source depicts the Board of Directors, Compliance Committee and Compliance Officer in sequence, with Legal, AML and Risk Management as linked functions and Finance and Due Diligence also shown. The text assigns Internal Audit an independent direct line to the Board or Committee. Confirm the approved hierarchy where the diagram is ambiguous. [V6]

Investigation process

1. Receive and log the report or alert.
2. Conduct a preliminary assessment.
3. Carry out an internal investigation where warranted.
4. Report findings to the Compliance Committee.
5. Take corrective or disciplinary action where appropriate.

Digital Assets Compliance

MAAT may establish a dedicated unit in light of its asset tokenization, digital infrastructure, trade finance and blockchain settlement activities. Its proposed responsibilities include applicable Markets in Crypto-Assets Regulation (MiCA) obligations, travel rule requirements, blockchain analytics, and AML controls for wallets and digital asset transactions. [V7]

The framework draws on practices used in regulated financial technology, international trading and tokenization. Its operation depends on appointments, approved policies and demonstrable controls. [V6]

Validation notes

The numbered references in the text identify statements that require legal or operational confirmation.

V2. Legal applicability

Map legal entities, jurisdictions, activities and transaction flows to applicable anti-bribery, accounting, anti-boycott, trade and sanctions requirements. Confirm the U.S. nexus, including the separate scope of FCPA anti-bribery and accounting provisions. Verify applicable EU and UK measures and relevant national implementing laws. Distinguish legal requirements, conventions, guidance and voluntary standards.

V4. Policies, reporting and training

Verify approved policies, their owners and effective dates, including the Compliance Handbook, FCPA guide and recordkeeping policy. Confirm how staff access confidential and anonymous reporting, which teams receive reports, and how non-retaliation, training and investigations are evidenced. Confirm the stated political contribution and facilities approval process and the gifts and hospitality controls.

V5. AML, sanctions and third-party controls

The Global Code states identity verification and monitoring as obligations. The AML policy uses discretionary language. Confirm the legal triggers, responsible teams, due diligence thresholds, screening sources, escalation procedures, monitoring coverage and external reporting obligations. Verify use of contractual clauses, attestations, audit rights and payment controls with actual records.

V6. Governance and implementation

Verify Board and committee mandates, membership, minutes, appointments and reporting lines, including the names and relationship of the Compliance Committee and Compliance and Risk Committee and of the Compliance Officer and Chief Compliance Officer. Confirm which units exist, their independence, who approves high-risk cases, and which controls, audits and quarterly meetings can be evidenced.

V7. Digital assets and tokenization

Confirm each entity's products, services, jurisdictions and authorization status. Assess MiCA classification and applicability separately from travel rule obligations, including Regulation (EU) 2023/1113 where applicable. Confirm whether the dedicated unit and wallet, custody, exchange and blockchain controls exist or are proposed.

Official references

U.S. Department of Justice and SEC · FCPA Resource Guide

EUR-Lex · Markets in Crypto-Assets Regulation (EU) 2023/1114

EUR-Lex · Transfer of Funds Regulation (EU) 2023/1113

maatGroup

MADRID – GENEVA – LONDON -ISTANBUL

Global Anti-Corruption and Anti-Bribery Policy

Includes the Third-Party Due Diligence and AML and Sanctions policies

Review copy for internal validation

13 November 2026

Includes validation notes for regulatory references and statements about implementation.

Anti-Corruption, Due Diligence and AML Policies

Global Anti-Corruption and Anti-Bribery Policy

1. Purpose and scope

MAAT INTERNATIONAL GROUP and its subsidiaries prohibit bribery and corruption. This policy applies to directors, officers, employees, consultants, agents, intermediaries, joint venture partners and anyone else acting on behalf of the Company.

2. Legal and compliance framework

Comply with applicable anti-bribery laws, including the U.S. Foreign Corrupt Practices Act (FCPA) and UK Bribery Act 2010 where relevant, and applicable EU and national anti-corruption measures. The OECD Anti-Bribery Convention and the United Nations Convention against Corruption inform national anti-corruption laws. ISO 37001 is a reference for anti-bribery management systems. The Company aims to maintain controls consistent with recognized practices. [V2] [V8]

3. Prohibited conduct

Do not offer, promise or accept bribes or improper advantages, give or request kickbacks, make improper payments through intermediaries or improperly influence public officials. This prohibition covers direct and indirect conduct involving cash, gifts, hospitality, travel, job offers or anything else of value.

4. Public officials

Take particular care when dealing with government, regulatory or customs officials, state-owned or state-controlled entities and international organizations. Interactions with public officials must be lawful, transparent and documented.

5. Facilitation payments

This policy prohibits facilitation payments regardless of local custom. An exception may apply only where personal safety is at risk. [V1]

6. Gifts and hospitality

Gifts and hospitality must be modest, reasonable, infrequent, transparent and properly recorded, and must never be intended to influence a business decision improperly. Luxury travel, cash or cash equivalents, significant personal gifts, concealed commissions and undisclosed benefits are prohibited.

7. Third-party corruption risk

Use risk-based due diligence, contractual compliance clauses, anti-corruption certifications and payment monitoring to manage third-party risk. Higher-risk parties may include agents, consultants, lobbyists, intermediaries and distributors. [V5]

8. Books and records

Record all financial transactions accurately and transparently, with adequate supporting documentation. Off-book accounts, hidden payments, false invoices and disguised commissions are prohibited.

9. Reporting violations

Report suspected violations to a supervisor, the Legal Department, the Compliance Officer or an available confidential channel. The Company prohibits retaliation for good-faith reporting. [V4]

10. Consequences

Violations may result in disciplinary measures, termination of employment or contract, civil or criminal liability, and regulatory penalties.

Third-Party Due Diligence Policy

1. Purpose

This policy covers assessment and monitoring of agents, intermediaries, partners, consultants, suppliers and joint ventures. It addresses bribery and AML risks, particularly in international trading, cross-border finance and digital asset arrangements.

2. Risk classification

- Low risk may include standard suppliers and professional service providers.
- Medium risk may include commercial consultants and distributors.
- High risk may include agents who interact with authorities, lobbyists, foreign intermediaries and politically exposed counterparties.

3. Due diligence

Depending on the risk, obtain corporate registration documents, beneficial ownership disclosures and compliance certifications, and perform AML and sanctions screening, litigation checks and reputational reviews. [V5]

4. Contractual requirements

Third-party agreements must include appropriate anti-corruption, AML and sanctions provisions, audit rights and termination rights in the event of misconduct. [V5]

5. Red flags

Unusual commissions, offshore or cash payment requests, refusal to disclose ownership, vague service descriptions and political connections may warrant enhanced due diligence.

AML and Sanctions Compliance Policy

1. Objective

The Company seeks to prevent money laundering, terrorist financing, sanctions violations and illicit financial flows. This policy is particularly relevant to asset tokenization, international trading, digital assets, trade finance and cross-border payments.

2. Legal and compliance framework

Apply relevant AML and sanctions requirements, including national rules implementing EU AML directives, applicable U.S. OFAC programs and EU and UK sanctions measures. Consider the FATF Recommendations as international standards reflected in domestic requirements. [V2] [V5]

3. Customer and partner identification

Apply due diligence before entering into business relationships where required by law or Company policy. Measures may include identity and beneficial ownership verification, sanctions and politically exposed person screening, and adverse media checks. [V5]

4. Transaction monitoring

Monitor transactions where required by law or Company policy. Indicators include unexplained large transfers, circular payment structures, shell companies and links to high-risk jurisdictions. [V5]

5. Sanctions compliance

Do not proceed with transactions involving sanctioned parties or embargoed jurisdictions in breach of applicable restrictions. Check relevant U.S., EU, UK and UN measures as applicable and refer potential matches for review. [V2] [V5]

6. Suspicious activity reporting

Report suspected suspicious activity to the Legal Department and the Compliance Officer. The Company must report to the appropriate authority where required by law and may do so where otherwise appropriate and legally permitted. [V5]

Governance

The Compliance Officer is responsible for monitoring compliance, coordinating internal investigations and supporting training. The Board is to review compliance risks, internal controls and corporate ethics policies periodically. [V6]

Validation notes

The numbered references in the text identify statements that require legal or operational confirmation.

V1. Governing rule on facilitation payments

Part I describes prior written approval and expense reporting for a limited category of payments. Parts II and IV prohibit facilitation payments, subject to a potential personal safety exception. Obtain the approval history, identify the governing rule and harmonize the codes and policies. A statutory exception under the U.S. FCPA does not establish permission under other laws or company policy.

V2. Legal applicability

Map legal entities, jurisdictions, activities and transaction flows to applicable anti-bribery, accounting, anti-boycott, trade and sanctions requirements. Confirm the U.S. nexus, including the separate scope of FCPA anti-bribery and accounting provisions. Verify applicable EU and UK measures and relevant national implementing laws. Distinguish legal requirements, conventions, guidance and voluntary standards.

V4. Policies, reporting and training

Verify approved policies, their owners and effective dates, including the Compliance Handbook, FCPA guide and recordkeeping policy. Confirm how staff access confidential and anonymous reporting, which teams receive reports, and how non-retaliation, training and investigations are evidenced. Confirm the stated political contribution and facilities approval process and the gifts and hospitality controls.

V5. AML, sanctions and third-party controls

The Global Code states identity verification and monitoring as obligations. The AML policy uses discretionary language. Confirm the legal triggers, responsible teams, due diligence thresholds, screening sources, escalation procedures, monitoring coverage and external reporting obligations. Verify use of contractual clauses, attestations, audit rights and payment controls with actual records.

V6. Governance and implementation

Verify Board and committee mandates, membership, minutes, appointments and reporting lines, including the names and relationship of the Compliance Committee and Compliance and Risk Committee and of the Compliance Officer and Chief Compliance Officer. Confirm which units exist, their independence, who approves high-risk cases, and which controls, audits and quarterly meetings can be evidenced.

V8. Claims for external audiences

Validate the named EU anti-corruption and AML instruments, any ISO 37001 conformity or certification claim, and specific governance, ESG, privacy and security standards. The source compares the framework with that of regulated firms. Substantiate any such comparison and all claims of licensing, certification, regulatory coverage or operational implementation before using the dossier for onboarding, fundraising or institutional presentations.

Official references

U.S. Department of Justice and SEC · FCPA Resource Guide

maatGroup

MADRID – GENEVA – LONDON -ISTANBUL

Global Compliance Architecture and Regulatory Map

English edition from the Spanish source

Review copy for internal validation

13 November 2026

Includes validation notes for regulatory references and statements about implementation.

Global Compliance Architecture and Regulatory Map

Global compliance architecture

The governance model assigns responsibilities across the following functions. Validate the reporting lines, approved mandates and operational status before representing this model as implemented. [V6]

Corporate governance

- Board of Directors. Oversees the compliance program, approves policies and reviews strategic risks.
- Compliance and Risk Committee. Oversees regulatory compliance, risk management and compliance incidents. It links the Board and the Chief Compliance Officer.
- Chief Compliance Officer. Implements the program, oversees AML, manages internal investigations and reports to the Committee.

Core control functions

- Legal and Regulatory Affairs. Handles international legal compliance, contract review and regulatory advice.
- Risk Management and Compliance. Identifies risks arising from financial operations, international trading, digital assets and blockchain technology.
- Internal Audit. Independently reviews internal controls, regulatory compliance and operational processes. It reports directly to the Board or the Compliance Committee under the approved mandate.

Operational compliance units

- AML and Financial Crime. Conducts KYC/KYB, sanctions screening, transaction monitoring and fraud detection.
- Third-Party Due Diligence. Performs integrity checks and reviews agents, consultants, brokers, technology partners and joint ventures.

Proposed digital assets and tokenization function

A dedicated function could address applicable MiCA and travel rule requirements, blockchain analytics, wallet AML, oversight of exchanges and custodians, and monitoring of custody, wallet risk and digital asset transactions. Assess scope for real-world asset tokenization, stablecoins, digital trading, blockchain settlement and related infrastructure. [V7]

Global regulatory and compliance map

1. Anti-corruption and ethics

Assess applicable obligations under the U.S. FCPA and UK Bribery Act 2010. Consider the OECD Anti-Bribery Convention, the UN Convention against Corruption and ISO 37001 when designing controls for public and private bribery, improper payments, gifts and hospitality. [V2] [V8]

2. Financial crime prevention

Map controls for money laundering, terrorist financing, financial fraud and sanctions evasion to applicable EU AML requirements and sanctions, U.S. OFAC programs and UK sanctions. Use the FATF Recommendations to inform the assessment. [V2] [V5]

3. Digital assets and tokenization

Assess the EU Markets in Crypto-Assets Regulation, applicable laws implementing travel rule requirements, blockchain AML analytics, custody compliance and digital asset monitoring. [V7]

4. Corporate governance and business ethics

Map controls for transparency, business ethics and whistleblower protection to applicable national rules implementing the EU Whistleblower Directive, relevant competition and antitrust laws, corporate governance practices, and environmental, social and governance (ESG) and sustainability standards. [V4] [V8]

5. Data protection and cybersecurity

Identify applicable obligations under the EU General Data Protection Regulation and map personal data protection, privacy controls, information security and digital infrastructure security. [V3] [V8]

Use of the map

The map can support compliance manuals, investor and institutional presentations, and onboarding with banks, custodians, exchanges and other international partners. Before external use, verify which requirements apply and which controls are supported by evidence. Use the benchmark practices as design references. [V8]

Compliance document set

1. Code of Business Conduct and Ethics
2. Global Compliance Handbook
3. Anti-Corruption Policy
4. AML and Sanctions Compliance Policy
5. Third-Party Due Diligence Policy
6. Compliance and Governance Structure
7. Regulatory and Compliance Map

Validation notes

The numbered references in the text identify statements that require legal or operational confirmation.

V2. Legal applicability

Map legal entities, jurisdictions, activities and transaction flows to applicable anti-bribery, accounting, anti-boycott, trade and sanctions requirements. Confirm the U.S. nexus, including the separate scope of FCPA anti-bribery and accounting provisions. Verify applicable EU and UK measures and relevant national implementing laws. Distinguish legal requirements, conventions, guidance and voluntary standards.

V3. Monitoring, disclosure and privacy

The source asserts that users have no expectation of privacy and that the Company may monitor all communications where lawful. Validate the legal basis, scope, notices, retention, safeguards and disclosure process for each relevant jurisdiction. The revised text conditions monitoring and disclosure on applicable law. Confirm the effective privacy and security controls before external publication.

V4. Policies, reporting and training

Verify approved policies, their owners and effective dates, including the Compliance Handbook, FCPA guide and recordkeeping policy. Confirm how staff access confidential and anonymous reporting, which teams receive reports, and how non-retaliation, training and investigations are evidenced. Confirm the stated political contribution and facilities approval process and the gifts and hospitality controls.

V5. AML, sanctions and third-party controls

The Global Code states identity verification and monitoring as obligations. The AML policy uses discretionary language. Confirm the legal triggers, responsible teams, due diligence thresholds, screening sources, escalation procedures, monitoring coverage and external reporting obligations. Verify use of contractual clauses, attestations, audit rights and payment controls with actual records.

V6. Governance and implementation

Verify Board and committee mandates, membership, minutes, appointments and reporting lines, including the names and relationship of the Compliance Committee and Compliance and Risk Committee and of the Compliance Officer and Chief Compliance Officer. Confirm which units exist, their independence, who approves high-risk cases, and which controls, audits and quarterly meetings can be evidenced.

V7. Digital assets and tokenization

Confirm each entity’s products, services, jurisdictions and authorization status. Assess MiCA classification and applicability separately from travel rule obligations, including Regulation (EU) 2023/1113 where applicable. Confirm whether the dedicated unit and wallet, custody, exchange and blockchain controls exist or are proposed.

V8. Claims for external audiences

Validate the named EU anti-corruption and AML instruments, any ISO 37001 conformity or certification claim, and specific governance, ESG, privacy and security standards. The source compares the framework with that of regulated firms. Substantiate any such comparison and all claims of licensing, certification, regulatory coverage or operational implementation before using the dossier for onboarding, fundraising or institutional presentations.

Official references

U.S. Department of Justice and SEC · FCPA Resource Guide

EUR-Lex · General Data Protection Regulation, including Article 88

EUR-Lex · Markets in Crypto-Assets Regulation (EU) 2023/1114

EUR-Lex · Transfer of Funds Regulation (EU) 2023/1113