



POLICY FOR ANTI-CORRUPTION AND BRIBE, MONEY LAUNDERING AND TERRORIST FINANCING

Approved at the Board of Directors meeting held on 23/03/2026

| External Version

Document Datasheet

Responsible Functional Area	Corporate Compliance Department
ME version	1.6
Approval Body	Board of Directors

History		
Version	Approval Date	Changes
1.1	2015	Original version
1.2	2017	Version 2
1.3	2019	Version 3
1.4	2020	Version 4
1.5	2022	Version 5
1.6	23-03-2026	- Complement to Chapter 12; - Change in the order of chapters 12 and 13; - Added Annex III - Sanctions

The Mota-Engil Group is governed by a Policy of monitoring and continuous improvement of its Policies and Procedures. Thus, the information contained in this Policy is subject to updating, and Mota-Engil reserves the right to update it, whenever necessary.

TABLE OF CONTENTS

1.	INTRODUCTION.....	4
2.	DEFINITIONS.....	5
3.	POSITIONS AND RESPONSIBILITIES	5
4.	RESPONSIBILITIES.....	5
5.	MONEY LAUNDERING AND TERRORIST FINANCING	6
6.	BRIBERY AND CORRUPTION	7
7.	GIFTS AND HOSPITALITY	10
8.	FACILITATING PAYMENTS AND BACKHANDERS.....	10
9.	CHARITABLE CONTRIBUTIONS, SPONSORSHIP AND CORPORATE SOCIAL RESPONSIBILITY	11
10.	POLITICAL DONATIONS.....	11
11.	LOBBYING	11
12.	OBLIGATIONS RELATING TO PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING	12
13.	DUTIES OF IDENTIFICATION AND DUE DILIGENCE TO THIRD PARTIES/COUNTERPARTIES.....	14
14.	RECORD KEEPING.....	17
15.	REPORTING, FAIR TREATMENT AND NON-RETALIATION.....	17
16.	CONSEQUENCES OF THE INFRINGEMENT.....	18
17.	TRAINING AND COMMUNICATION.....	19
	ANNEX I DEFINITIONS.....	20
	ANNEX II POSITIONS AND RESPONSIBILITIES.....	23
	ANNEX III SANCTIONS.....	24
1.	PURPOSE	24
2.	SANCTIONS AND RESTRICTIVE MEASURES.....	24
3.	GENERAL PRINCIPLES	25
4.	IDENTIFYING SANCTIONS RISKS	25
5.	GOVERNANCE	27
6.	DISCIPLINARY MEASURES AND PENAL SANCTIONS	27
7.	SUPPORT LINKS	28

1. INTRODUCTION

1.1. The Mota-Engil Group (hereinafter, the "Group") is committed to conducting all business and partnerships with integrity and professionalism, in a fair and honest manner, complying with all applicable legislation.

1.2. The Group has adopted a zero-tolerance policy towards acts of corruption, bribery, money laundering and terrorist financing, and prohibits such acts in any form, whether directly or through third parties, anywhere in the world. The offering or accepting of bribes of any kind is not tolerable anywhere we operate. We recognise that our reputation for integrity is one of our most valuable assets and that any wrongdoing is a threat to the business and our values.

1.3. The policy purposes:

- ✓ Establishing mutual responsibilities between the Group and those who work for us, in complying and defending our position against corruption, bribery, money laundering and terrorist financing;
- ✓ Ensuring compliance with anti-corruption, bribery and anti-money laundering and terrorist financing laws, rules and regulations, in any country where we may conduct business; and
- ✓ Providing information and guidance on how to recognise and deal with corruption, bribery, money laundering and terrorist financing issues.

1.4. This policy reflects our continued commitment to the fight against corruption and bribery, money laundering and terrorist financing and our responsibility to the markets where we operate.

1.5. In some jurisdictions, if the Group is found to have taken part in corruption, money laundering or terrorist financing, it may be subject to considerable fines, be excluded from public or private tenders and face reputational damage. Employees may also be subject to legal proceedings and receive jail sentences.

1.6. In addition, the Group frequently works on projects affiliated with international development banks, such as the World Bank and other similar entities. These institutions have strict anti-corruption and bribery, anti-money laundering and terrorist financing guidelines, and they need the companies they work with to abide by such guidelines and business ethics practices. Companies involved in corruption, money laundering or terrorist financing may be excluded or blacklisted by the World Bank and other similar entities for several years - such exclusion means that the company can no longer work or implement contracts with projects affiliated with the World Bank or other similar entities.

1.7. This policy supersedes any previous policy on the same scope and may be updated at any time.

1.8. If you have any questions or doubts about these rules, you should contact the Compliance Department,

Mota-Engil's Compliance Helpline¹ or the Legal Department.

2. DEFINITIONS

See Annex I.

3. POSITIONS AND RESPONSIBILITIES

See Annex II.

4. RESPONSIBILITIES

4.1. This policy applies to all of us, including:

- ✓ Employees;
- ✓ All companies, subsidiaries, branches, delegations and representative offices of the Group; and
- ✓ Other individuals or entities that collaborate with Mota-Engil and with the other companies of the Group.

4.2. It is the Group's policy to only work with reputable third parties who do business legally.

4.3. The prevention, detection and reporting of bribery and other forms of corruption is the responsibility of everyone, including each and every employee and all those who work for us or under our control. We are duty-bound to avoid any activity that could lead to, or suggest, a violation of this policy.

4.4. Employees must confirm that they have read, understood, and comply with this policy.

4.5. The Executive Committee must ensure that this policy complies with legal and ethical obligations, and that all those under the Group's control comply with it.

4.6. Management bodies at all levels must ensure that all those under their remit are made aware of and understand this policy, and that they receive appropriate and regular training on it.

4.7. The Compliance Department has the primary and day-to-day responsibility for implementing this policy and for controlling its use and effectiveness.

¹ compliance@mota-engil.com
External version

5. MONEY LAUNDERING AND TERRORIST FINANCING

5.1. This policy strictly prohibits the Group, its employees or its counterparties from engaging in illegal activities related to money laundering and terrorist financing.

5.2. The crime of money laundering is committed by anyone who converts, transfers, assists or facilitates any operation of conversion or transfer of advantages, obtained by himself or by a third party, directly or indirectly, with the purpose of concealing his illicit origin, or with the purpose of preventing the perpetrator or participant of these offenses from being criminally prosecuted or subjected to a criminal reaction.

5.3. The crime of money laundering is also committed by anyone who conceals or conceals the true nature, origin, location, disposition, movement or ownership of the advantages, or the rights related thereto.

5.4. In addition, the crime of money laundering is committed by anyone who, not being the perpetrator of the crime that gave rise to the advantages, acquires, holds or uses, knowingly, at the time of acquisition or at the initial moment of possession or use, of that quality (of the advantages of a crime).

5.5. Terrorist financing is considered to be the supply, collection or possession of funds or property of any kind, as well as proceeds or rights that may be transformed into funds, with the intention of being used or knowing that they may be used in the planning, preparation or commission of criminal activity by terrorist groups, organisations or associations.

5.6. Terrorist financing consists of the supply, collection or holding of funds/goods/products/rights that can be transformed into funds for terrorist activities.

5.7. Activities related to money laundering and terrorist financing may generate not only criminal and economic sanctions for individuals involved in such acts, but also administrative, criminal and economic sanctions for companies, which may cause serious damage to the Group's reputation and the level of trust of customers and other stakeholders, as well as to its assets and business.

5.8. Both money laundering and terrorist financing have similar techniques when it comes to concealing and concealing origins and purposes. The difference between the two crimes lies in the fact that money laundering has funds involved whose origin is always illicit, while in terrorist financing they can be licit or illicit. Examples of lawful sources are donations to organisations or foundations that use them to support terrorist activities or organisations.

Risk Activities

5.9. Following activities and businesses may present greater risks of money laundering and terrorist financing: real estate activities, transaction of goods or provision of services against cash payment, provision of auditing, accounting, tax consultancy, legal, paralegal or notary services to third parties.

5.10. Group companies carrying out occasional transactions similar to those indicated above or whose core business is of that nature must implement identification and due diligence measures laid down in the procedure for third parties in the business relationships or occasional transactions they establish with their customers.

5.11. The Group's companies must also bear in mind that they may be subject to additional duties enshrined in local legislation/host countries to fight against money laundering and terrorist financing.

5.12. All Group employees, regardless of the activity or business carried out by their respective employers, shall cautiously launch the identification and due diligence procedures provided for in the procedure for third party procedure whenever they identify indicators of suspicion related to the customer or the transaction.

5.13. For more information and guidance on indicators of suspicion, please refer to the Third-Party Procedure available only on the Group's in-house website.

Cash transactions

5.14. It is forbidden to enter into or in any way participate in any business originating receipt of cash amounts exceeding EUR 1,000 or the equivalent amount in local currency.

5.15. No cash payment exceeding EUR 150 or the equivalent amount in local currency is allowed.

5.16. These limits apply regardless of whether the transaction is carried out through a single transaction or several transactions that are related to each other.

5.17. Cash is also understood to be payments or receipts made through a means of payment that makes it impossible to identify the recipient, for example the use of bearer cheques or those endorsed by third parties.

6. BRIBERY AND CORRUPTION

6.1. This policy strictly prohibits the Group, its employees and its counterparts, while on duty or as result of their duties, from soliciting, accepting, giving or promising to give an asset or non-asset gain and, in return, from soliciting or accepting to perform any act or omission contrary to the duties of the position they hold. It is also forbidden to accept or request any asset or non-asset gains when they are not due, even if the act or omission is not contrary to office duties.

6.2. Bribery also exists namely when:

- ✓ The employee convinces or attempts to convince another person, by means of a gift or offer of asset or non-asset gains, to make false statements in his or her party statement, to give false information or to do false translations;

- ✓ The employee convinces someone to perform certain acts by obtaining asset or non-asset gains in return.

6.3. The behaviour described above may constitute the commission of a crime and, consequently, result in the liability of both natural and legal persons.

6.4. Employees must reject any offer or request for asset or non-asset gains in exchange for any act or omission contrary to their duties or positions they hold.

6.5. Any such occurrences must be immediately reported to the Compliance Department or the Ethics Channel. In case of doubt, you should contact the Compliance Helpline, as indicated in the Code of Ethics and Business Conduct and Whistleblowing and Non-Retaliation Policy.

6.6. Bribery is often disguised through false invoices or false records, or when payments are improperly called "consultant' fees" or similar. This is one of the reasons why the Group has implemented strict internal control methods and accounting requirements.

6.7. Cash payments shall an exception rather than a rule and any cash in or cash out operations must be approved and documented. Should there be no option left but to make cash payments, the operation must be justified and detailed (including recipient's name, amount and name of the transaction). A payment receipt must be issued, duly approved in writing and processed according to Cash Procedures available on the Group in-house website.

6.8. The payment or acceptance of bribes or any undue consideration may result in the criminal liability of the employee, namely, but not exclusively, for both active or passive corruption, unfair advantage or bribery.

Prohibition to bribe civil servants

6.9. This policy prohibits the Group, its employees and representatives/intermediaries from offering a financial or non-financial gains to civil servants, directly or indirectly, including, for example, giving something of value to a civil servant, through a counterparty, close relatives or people close to the civil servant' family or people recognised as closely related.

6.10. Under this policy no offers or bribe promises are allowed, regardless of whether the civil servant rejects the offer, or fails to accomplish the desired result.

Prohibition of guaranteeing undue benefits to civil servants

6.11. Prohibition of payments to secure undue benefits or to obtain or retain business are defined broadly to include any commercial or financial benefit, payments to secure a sale or a contract. For example, a payment

to persuade a government official not to levy a fine or tax, or to reduce a tax or penalty would be a breach of the policy, as would a payment made to avoid enforcement of an applicable piece of legislation or regulation.

6.12. Similarly, payments made to influence a civil servant's decision regarding the granting of an authorisation or license, or to facilitate customs clearance, violate this policy.

Prohibition of bribery and corruption in the private sector

6.13. Under this policy the Group, its employees and representatives/intermediaries shall not make offers or promise to give asset or non-asset gains to a private sector employee, directly or indirectly, with the intention of obtaining or retaining a business, contract or other undue advantage or for the latter to perform an act or omission that constitutes a breach of functional duties.

6.14. Likewise, no offers or promises of bribes are allowed regardless of whether the private sector employee rejects the offer or fails to deliver the desired result.

6.15. Regarding business with private sector entities and their employees, and bearing in mind good faith, reasonable, appropriate and advertising-related expenses shall be allowed to promote the Group's services and products. Please, refer to section 6 below for rules dealing with such expenses.

Prohibition to accept bribes

6.16. Under this policy, the Group or the employees shall never accept any advantages whatsoever, or asset or non-asset gains, even in a disguised manner.

6.17. Any attempt to bribe an employee must be immediately reported to the Ethics Channel. In case of doubt, please call Mota-Engil's Compliance Help Line.

6.18. When employees are involved in making business decisions on behalf of the Group, their decisions must be based on judgments that are uncompromising, objective and put the interests of the Group first.

6.19. Employees must never accept or ask for any bribe, even if disguised, from a counterparty or any other third party. Employees must make this policy known to the third party that offers such advantages and make every effort to refuse or return said advantages.

6.20. If it is not possible to decline or return the bribe, the affected employee must immediately report the case to the Ethics Channel. In case of doubt, please call Mota-Engil's Compliance Help Line.

7. GIFTS AND HOSPITALITY

Gifts, meals, travel and entertainment granted to civil servants, government officials or private sector entities

7.1. Mota-Engil allows corporate gifts up to EUR 100.00/person or equivalent in local currency and up to EUR 500.00/entity or equivalent in local currency as well as reasonable hospitality and entertainment from the Company's customers and third parties.

7.2. Gifts shall be previously registered through the Gift Registration Form.

7.3. For further details, please refer to the Gifts and Hospitality Procedure, available on the Group's in-house website.

Acceptance of offers and hospitality

7.4. Under this policy, employees shall not accept offers, hospitality or other benefits if their judgment about the business or decisions about the business could be affected.

7.5. For further details, please refer to the Offers and Hospitality Procedure, available on the Group's in-house website.

8. FACILITATING PAYMENTS AND BACKHANDERS

8.1. Employees are prohibited from making facilitating payments or "backhanders", and from accepting commissions of any kind. All employees should avoid any activity that could lead to, or suggest, that a facilitation or commission payment will be made or accepted.

8.2. Civil servants are obliged to carry out their work without receiving additional payments to speed it up. Activities carried out by public officials may include: issuing licenses, permits, or other official documents, issuing visas, granting work visas and other immigration documents, releasing goods held at customs, obtaining public records for real estate or vehicles, or obtaining services (e.g., electricity, water, gas, telecommunications, or security).

8.3. If you are asked to make a payment on behalf of the Group, you should always be aware of the reason for the payment and whether the amount requested is proportionate to the goods or services provided. You should always ask for a receipt that details the nature of the payment. If you have any suspicions, concerns, or questions about any payment, you should raise them with the Ethics Channel. If you have any questions, you should contact Mota-Engil's Compliance Help Line.

9. CHARITABLE CONTRIBUTIONS, SPONSORSHIP AND CORPORATE SOCIAL RESPONSIBILITY

9.1. The Group may provide contributions and sponsorship that support activities of public interest, carried out by recognised entities and non-profit organisations. Such support shall not be used to reward the recipient for current, past or future support of the Group's projects, nor result in a bargaining advantage.

9.2. Charitable contributions or sponsorships may be approved if the social or charitable project operates in an area of social importance to the Group. Contributions of a charitable nature or sponsorships may be granted by or on behalf of the Group, for charitable, educational, non-profit, sports or cultural purposes, and when the activities promoted are in line with the Group's business objectives, values and ethical principles.

9.3. For more information, you can consult the Donations and Corporate Social Responsibility Procedure, available on the Group's in-house website.

10. POLITICAL DONATIONS

10.1. Regarding public policies, the Group does not usually take sides, directly or indirectly, nor does it make any contributions to political organisations.

10.2. The Group is bound by national and international legislation in force in any market where it operates. You must not give, promise to give or offer payments, gifts or hospitality to a civil servant to facilitate or expedite any business activity.

10.3. For further details, please refer to the Donations and Corporate Social Responsibility Procedure, available on the Group's internal website.

11. LOBBYING

11.1. Although not directly involved in party politics, the Group recognises the importance of being involved in the political debate, on matters of legitimate concern, which are related to its business, employees, customers and the communities in which it operates. Any employee lobbying on behalf of the Group must comply with all legal and regulatory requirements, including laws and regulations relating to registration and whistleblowing.

12. OBLIGATIONS RELATING TO PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

12.1. Group companies with shares admitted to trading on the regulated market in Portugal, or any other bound by the provisions of Act No 83/2017, of 18 August (Money Laundering Act), must to comply with the obligations contained in the applicable laws and regulations regarding the prevention of money laundering; this may include the need for periodic reporting to regulators, namely the CMVM, IMPIC or other relevant sectoral agency, depending on the specific sector of activity of the company in question.

Duty of Control

12.2. The Group implements a systematic and mandatory sanctions *screening process* to prevent business, financial or operational relationships with individuals, entities or countries subject to international sanctions. This verification is an integral part of due diligence and must be carried out prior to any contractual or transactional commitment and throughout the business relationship.

12.3. This process is detailed the Group's Third-Party Procedure.

Duty of Identification and Due Diligence

12.4. The Mota-Engil Group abides by identification and due diligence procedures as set out in applicable laws, and in sync. with the Group's Third-Party Procedure.

Duty of Communication

12.5. At Mota-Engil Group, whenever there is suspicion or reasonable grounds to suspect that the funds or assets have illicit origin or are related to money laundering or terrorist financing activities - including all operations suggested, attempted, in progress or already launched – those will immediately be reported to relevant authorities, and according to applicable laws.

Duty of Abstention

12.6. The Mota-Engil Group refrains from carrying out any operations that it knows, suspects or has reasonable grounds to suspect are associated with funds or other assets derived from or related to criminal activities, money laundering or terrorist financing, as well as with third parties included in sanctions lists.

Duty of Refusal

12.7. At the Group, the duty of refusal shall apply to any new business relationship or an on-going relation, or at any occasional transaction or any other operation, whenever following occurs:

- ✓ It is not possible to obtain the identification and supporting evidence from the customer, its representative or the beneficial owner, including the information needed to confirm such status and to understand the applicable ownership and control structure;
- ✓ Adequate information is not obtained on the nature, object and purpose of the business relationship;
- ✓ It is not possible to comply with identification and due diligence procedures, including procedures for updating information and documentation.

Duty of Retention

12.8. The Group ensures long-lasting, safe and available storage means of all original documents, copies, records, references or any other elements provided by customers, partners or other counterparties within the scope of the identification, verification and due diligence procedures.

12.9. This obligation also covers records of operations carried out, as well as internal analyses, risk assessments, supporting documentation and other evidence proving compliance with applicable legal, regulatory and in-house provisions. The Group ensures that such data remain properly organised, traceable and auditable, in line with its Integrity and Compliance Programme.

Duty of Review

12.10. The Group conducts deep review whenever conducts, activities or operations are identified as possibly being related to funds or other assets, derived from criminal activity, or in connection with money laundering and/or terrorist financing. In such cases, the Group shall strengthen the degree and type of monitoring, ensuring a thorough and permanent assessment of risks involved.

Duty of Collaboration

12.11. The Group will cooperate promptly, fully and transparently with relevant authorities.

Duty of non-disclosure

12.12. The Group and its employees, internal or external, are expressly prohibited from disclosing to counterparties any information related to communications made, or to be made, to relevant authorities. This

restriction also includes requests for information received from those authorities, as well as ongoing investigations, inquiries, investigations, reviews or other legal proceedings.

12.13. Likewise, the Group and employees may not disclose to counterparties any information relating to the analysis of operations considered particularly suspicious and must refrain from taking any steps that may, directly or indirectly, raise suspicions about the existence of internal processes aimed at assessing potential practices associated with money laundering and/or terrorist financing.

Duty of Training

12.14. The Mota-Engil Group ensures continuous and mandatory training for teams exposed to risks, according to best practices, geographical areas, maturity and the sector where they operate.

13. DUTIES OF IDENTIFICATION AND DUE DILIGENCE TO THIRD PARTIES/COUNTERPARTIES

13.1. Before initiating a business relationship or an occasional transaction with a third party, a procedure for the identification, risk assessment and *due diligence* of the third party must be carried out. New and existing third parties must be duly approved in accordance with the Third-Party Procedure before any transaction with that third party can be carried out.

13.2. The "Third-Party Procedure" applies to all counterparties and aggregates what in best practice is called "*Know Your Customer*", "*Know Your Supplier*" and "*Third-Party Agreement*".

13.3. Each Mota-Engil business unit, responsible for the *due diligence* procedure, must take the appropriate measures to be sure that third parties do not provide false statements. If any employee has reason to believe that a third party has provided false identification, false information or any other false documentation, they must report it to the Compliance Department or to Mota-Engil's Compliance Help Line.

13.4. The Group encourages its employees to take the initiative to raise any concerns to a member of the management, the Compliance Department or Mota-Engil's Compliance Help Line.

Risk-based approach

13.5. In assessing the corruption, bribery, money laundering and terrorist financing risks associated with a business relationship or occasional transaction, the Group's companies shall consider the relevant risk factors.

13.6. The risk factors that, alone or in combination, may increase or reduce the risk of corruption, bribery, money laundering or terrorist financing constituted by a business relationship or occasional transaction, are [External version](#)

the following:

- ✓ Type of business or activities of counterparties;
- ✓ Geographic location of the counterparty;
- ✓ Source of funds;
- ✓ Means of payment to be used in the transaction;
- ✓ Registration of politically exposed persons in the counterparty or among their beneficial owners;
- ✓ reputation of the counterparty and its beneficial owners;
- ✓ Record of sanctions, ongoing investigations or convictions in criminal proceedings against the counterparty, management bodies, key staff or beneficial owners;
- ✓ Refusal of the counterparty to include all or part of the anti-corruption, bribery, anti-money laundering and counter-financing clauses

13.7. In the weighting of risk factors, the business relationship or occasional transaction will be categorised according to three levels of risk: high, medium and low.

13.8. For each level of risk, due diligence measures will be developed, and these measures may be simplified or strengthened, allowing Group companies to better understand the risk associated with business relationships or occasional transactions. Due diligence measures will be proportionate to the level of risk of the business relationship or occasional transaction.

Aspects to consider when establishing a contractual relationship with third parties

13.9. All new and existing third parties shall be made aware of this policy and of the prohibitions against corruption, bribery, money laundering and terrorist financing practices as required by applicable law.

13.10. It is the responsibility of the employees who deal with third parties to ensure that, prior to their involvement, the third parties are duly informed about this policy and that they agree not to engage in acts of corruption, bribery, money laundering and terrorist financing. This policy must be made available to third parties before the Group commences any business relationship by providing the third party with a scanned or printed copy of this policy.

13.11. The Group's contracts with third parties must be in writing and must detail the services to be performed, the basis for the counterparty's remuneration, the amounts to be paid and statements that the counterparty will continue to comply with all relevant anti-corruption laws and this policy. This will allow the Group to audit it periodically and notify the third party in the event of any breach of compliance. The amounts paid must be in accordance with the agreed terms and constitute a fair market value.

13.12. If third parties are unable or unwilling to comply with these contractual provisions, the reasons must be recorded and, if deemed legitimate, submitted to a new risk analysis by the Compliance Department and

evaluation by the corresponding approving structure, which will assess whether the third party can be hired in the specific circumstances. A third party who does not agree with the Code of Ethics and Business Conduct and this policy should not be hired.

13.13. Third parties must raise their concerns about any matter or suspected violation of this policy as soon as possible. Third parties may direct their concerns to their commercial contact in the Group's company, to the Compliance Department or to Mota-Engil's Compliance Help Line. All such concerns will be investigated as described in item 15 below.

13.14. The Group may be requested by business partners or local governments to contribute to public works or other projects in the relevant local jurisdictions in which it operates ("clearing partners"). This may include, for example, capacity building or local infrastructure, such as painting a road adjacent to a bridge project, or building local infrastructure in the vicinity of a construction project. Such practices are often referred to in the industry as "compensation" agreements. Depending on all the surrounding circumstances, such practices may be legitimate.

13.15. Any requests for personal favours or works involving the personal property of civil servants are prohibited.

Duty to abstain and refuse

13.16. Group companies shall refrain from carrying out any transaction or set of transactions, whether present or future, which they know, or suspect may be associated with funds or other property derived from or in connection with criminal activities or the financing of terrorism.

13.17. Group companies shall refuse to enter into business relationships, occasional transactions or carry out other operations, when they do not obtain the identifying elements of the counterparties, their representatives and beneficial owners, the ownership and control structure of the counterparty; or information about the nature, subject matter and purpose of the business relationship when the counterparty is a customer.

13.18. In the event that it is confirmed that the business relationship or occasional transaction is an attempt to launder money, corruption or may constitute an act of bribery or terrorist financing, the deal must be refused.

13.19. In the event that entities or individuals flagged on official restrictive lists are found to be participating in the business relationship or occasional transaction, the business shall be refused.

13.20. For further details and guidance, please refer to the Third-Party Procedure, available on the Group's internal website.

14. RECORD KEEPING

14.1. The Group will maintain an appropriate system of internal accounting controls permitting to enforce compliance with this policy, which will be reviewed periodically by the Group's Internal Audit Area, in order to provide reasonable assurance that:

- ✓ Transactions are carried out according to the needed approvals (which may be delegated to directors or other bodies within the Group company);
- ✓ Transactions are recorded as necessary in order to:
- ✓ Enable the preparation of the financial statements in accordance with accepted international accounting principles or any other criteria applicable to those statements;
- ✓ Maintain the accounting records of the assets of the Group's company; and
- ✓ Access to the company's assets and resources is only allowed with specific authorisation from company directors.

14.2. All accounts, invoices, memoranda and records relating to transactions with third parties must be accurate and complete in all relevant respects. This documentation must be kept for a minimum of five years, after the termination of the business relationship with the third party.

14.3. No payments or transactions shall be kept "off the books" to facilitate or conceal undue payments. There shall be no accounting entries or records of expenditure relating to any payments which are false or misleading.

14.4. Employees must ensure that all expense records related to hospitality, gifts or third-party expenses are submitted for approval, in accordance with our policies and procedures, and specifically include the reason for the expense.

14.5. The Group companies shall retain for seven years as from the moment the identification of the counterparty was processed or, in the case of a business relationship, after the end of such relationship, all documents, copies, reviews and electronic data relating to each business relationship or occasional transaction.

15. REPORTING, FAIR TREATMENT AND NON-RETALIATION

15.1. Employees are encouraged to raise their concerns about any matter or suspicion of misconduct as early as possible. If employees are unsure whether a particular act constitutes corruption, bribery, money laundering or terrorist financing, or if they have any other questions, they should contact the Corporate Department or the Local Compliance Teams, use Mota-Engil's Compliance Helpline or the Legal Department. Concerns must be reported, following Mota-Engil's Ethics Channel, provided for in our Code of Ethics and Business Conduct. A copy of the Code of Ethics and Business Conduct is available on the Group's official website.

15.2. Any person who becomes aware, within the scope of their professional activity, of a possible violation of

this policy must immediately report it through the Ethics Channel.

15.3. It is important that any employee communicates via the Ethics Channel, to Mota-Engil's Compliance Help Line or to the Legal Department, as soon as possible, if they are offered a bribe by a third party, if they are invited to take a bribe, suspect or have sufficient reasons to suspect that certain funds or other assets, regardless of the amount or valuables involved, they originate in criminal activities or are related to terrorist financing or if you believe that you are the victim of some type of illegal activity.

15.4. Employees who refuse to accept or offer any bribe, to participate in money laundering transactions, terrorist financing, or those who raise concerns about or report wrongdoing by others, are sometimes concerned about possible repercussions. We want to encourage communication and support anyone who raises genuine concerns in good faith under this policy, even if they finally realise that they were mistaken. However, those who knowingly or in good faith make false accusations, or those who fail to report wrongdoing or suspicions of which they are aware, may be subject to disciplinary measures.

15.5. We are committed to ensuring that no one is subject to detrimental treatment as a result of refusing to participate in acts of corruption, bribery, money laundering or terrorist financing, or for having reported, good faith, their suspicions of any actual or potential bribery or any other corruption behaviour that has occurred, or that may occur in the future.

15.6. If you believe that you have been the victim of any such behaviour, you must report the case through Mota-Engil's Ethics Channel and retaliation, including, but not limited to intimidation, discrimination, disciplinary actions, withholding or suspension of salary payments, is expressly prohibited.

15.7. A breach of trust or retaliation against any employee who has reported a concern or helped in the investigation process will also be treated as a breach of this policy and the Group's Code of Ethics and Business Conduct.

15.8. Employees may also follow the instructions established in the Reporting of Irregularities and Non-Retaliation Policy, and, in the event of a complaint, benefit from the whistleblower protection regime (e.g., in Portugal by Act No 93/2021, of 20 December), provided that the conditions on which such protection depends are met.

16. CONSEQUENCES OF THE INFRINGEMENT

16.1. Giving, offering or receiving a bribe or backhand, engaging in acts of corruption, money laundering, terrorist financing, "turning a blind eye" not to prevent such activity, the violation of this policy or any applicable law may result in serious consequences, including but not limited to the following:

- ✓ Disciplinary, civil, criminal and misdemeanour liability of the employee;

- ✓ Civil, criminal and misdemeanour liability of any of the Group's companies;
- ✓ Reputational damage to the Group, which may result in an adverse opinion of the competition and the general public and leading the Group to be in a competitive disadvantage;
- ✓ Loss of business.

16.2. Employees cannot avoid being held liable for "turning a blind eye" when the circumstances indicate a possible breach of the Group policy. If any employee has doubts or questions about whether their conduct is correct under the terms of this policy, that a violation of this policy is occurring or will occur, they should consult with their line manager, the Compliance Department or ask Mota-Engil's Compliance Help Line.

16.3. The Group's relations with its shareholders, joint venture partners, auditors, creditors, suppliers and customers may be adversely affected by violations of this policy.

17. TRAINING AND COMMUNICATION

17.1. The Group has established a continuous training programme to provide employees with a clear understanding of this policy and strategy for implementation purposes.

17.2. Our zero-tolerance approach to corruption, bribery, money laundering and terrorist financing shall be communicated to all third parties/counterparties with whom the Group company has trade relations.

ANNEX I | DEFINITIONS

1.1 "**Sanctioning Authority**" means:

- ✓ The European Union;
- ✓ The United Nations;
- ✓ Countries that have jurisdiction over the Group's activities (USA, UK, France, etc.) or
- ✓ The government of a country where the Group operates.

1.2 "**Adverse Media**" means negative press reports reported in public sources of information, relating to investigations, charges or judicial decisions related to cases of corruption, bribery, financial crimes, organised crime, terrorism, drug trafficking or other crimes.

1.3 "**Employees**" (and the terms "we", "us" and "our") means all individuals working at all levels and categories of the Group, including officers, directors, employees (permanent, fixed-term or temporary), consultants, contractors, subcontractors, trainees, seconded staff, home-based, casual and interim workers, volunteers, trainees, agents, sponsors or any other person associated with the Group, branches, delegations or representative offices or with their staff, directors and employees, regardless of their location.

1.4 "**Commissions**" are payments made in exchange for a favour or a business advantage.

1.5 "**Director**" means an employee who leads or supervises a specific area, a programme or a project of a Group company. The Director generally reports to the executive body of each company (Ex: COMEX).

1.6 "**Sanctioned Entity**" means an entity:

- ✓ Located in, incorporated under the laws of, or owned or controlled (directly or indirectly) by, or acting on behalf of, a party located in or organised under the laws of a country or territory subject to sanctions;
- ✓ Contained in, owned or controlled by a party to, or acting on behalf of, a party on any Sanctions List;
or
- ✓ Subject to sanctions of any kind.

1.7 "**Enhanced Due Diligence**" means the process of in-depth investigation that collects detailed integrity data and enhanced background checks on any entity.

1.8 "**State-owned enterprises**" are enterprises over which a government or state authority has significant

control, through a full, majority, or significant minority stake. The stake can be direct or indirect but is generally understood to amount to at least 10% of the company ownership.

1.9 "**Civil servant**" is defined broadly and means:

- ✓ Anyone involved in the performance of public duties in a government entity. It includes any official elected, appointed or serving a government entity, at any level, including national or local entities. It also includes members of legislative, administrative and judicial bodies, as well as lower-level employees of government entities, such as clerical workers;
- ✓ Any employee or collaborator of governmental or state-controlled entities, including state-owned entities operating in the trade sector, such as employees of state-owned enterprises;
- ✓ Any employee or staffer of an international public organisation (such as the United Nations, the World Bank or the International Monetary Fund);
- ✓ Any person who serves in an official position for a government, government entity, or state-owned company (for example, someone who has been given authority by a government entity to assume official duties);
- ✓ Any political party, party staffer or political candidate;
- ✓ The expression "civil servant" must also include up to third degree relatives or equivalent affective relationship of the civil servant in question.

1.10 "**Group**" means all subsidiaries, branches, delegations or representative offices, directly or indirectly, in whole or in part, owned or controlled by Mota-Engil SGPS, S.A.

1.11 "**List of Approved Counterparties**" means the list of entities approved to carry out business with the Group.

1.12 "**Blocked Counterparty List**" means the list of entities not approved to conduct business with the Group.

1.13 "**Sanctions List**" means a list of sanctioned individuals issued by a Sanctioning Authority.

1.14 "**Offers and hospitality**" includes meals, entertainment, hotels, travel and general items accepted by the employees of the Group company or offered to third parties.

1.15 "**Facilitation payments**" or "**backhanders**" are generally small payment or offers made to secure or expedite routine non-discretionary administrative actions, typically performed by lower-level government officials.

1.16 "**Individuals**" means any third party who is not a civil servant.

1.17 "**Politically Exposed Person**" or "**PEP**" is an individual who holds an important public office, a family member or a known associate of that person. Examples include heads of state, political leaders, government officials, judicial or military officials, senior executives of state-owned enterprises, and representatives of political parties. A PEP generally poses a higher risk of potential involvement in bribery and corruption by virtue of the position it holds and the influence it may have. Known family members or associates of PEP include family members (including marital and consanguineous relationships), close associates (including professional and social associates), and relevant members of the same association (including political parties, civil organisations, and trade unions).

1.18 "**PEP Registration**" means the list of Politically Exposed Persons identified during background screening and with whom a Group company transacts.

1.19 "**Sanctions**" means legal instruments imposed by entities such as the UN, EU, OFAC (USA) or national authorities, applicable to countries, legal entities or natural persons.

1.20 "**Offer Registration System**" means the IT tool managed by the Compliance Department for the registration and approval of offers and hospitalities.

1.21 "**Bribe**" means an inducement or reward offered, promised or provided in order to obtain an unlawful commercial, contractual, regulatory or personal advantage.

1.22 "**Line manager**" means an employee who directly manages/coordinates other employees and operations, and reports to a direct manager.

1.23 "**Third Party**" or "**Counterparty**" means any individual, organisation, partnership, partner, company, association, consortium or other entity, other than an affiliate, with whom an employee comes into contact, during the course of his or her work within the Group. For the purposes of this policy, this definition includes, without limitation, actual and potential customers, suppliers, distributors, partners, business contacts, consultants, government and public agents and bodies, including their advisors, representatives and employees, politicians and political parties.

ANNEX II | POSITIONS AND RESPONSIBILITIES

1.1 "**Compliance Department**" means the market department responsible for enforcing the compliance programme locally or the region's Compliance Department if this function does not exist in the market.

1.2 "**Initiating Department**" is the department that initiates a business relationship with the counterparty. It includes the Business Development Department, Commercial Department, the Purchasing Department or any other department in the relevant jurisdiction. The Initiating Department is responsible for conducting a background check on the counterparty in order to identify and verify each new counterparty. When applicable, the Initiating Department must ask the company's Compliance Officer or, in his absence, the region's Compliance Department, to issue the screening tool report.

1.3 "**Legal Department**" means a department under the guidance of the Executive Committee of each region.

It shall, namely:

- ✓ Provide support to the commercial function along with legal support, in the negotiation and development of strategic partnerships, in the negotiation and implementation of transactions, as well as in financing operations or any other issues involving relevant risks and obligations;
- ✓ Formulate legal opinions and reviews on all contracts or documents binding on the region; and
- ✓ Assess contractual risks in the bidding and contract management phase, after contracts have been awarded.

1.4 "**Shared Services Centre**" or "**CSP**" means the entity or department(s) responsible for the performance of specific administrative support tasks, such as reporting, accounting, taxation, finance and human resources.

ANNEX III | SANCTIONS

1. PURPOSE

This Annex establishes the principles, rules and procedures Mota-Engil Group will abide by in complying with sanctions and restrictive measures imposed by international organisations, governments and other relevant authorities, ensuring that all Group companies abide by the legal requirements applicable and the ethical standards featuring on the Integrity and Compliance Programme.

2. SANCTIONS AND RESTRICTIVE MEASURES

International sanctions correspond to restrictive measures applied to individuals, entities, jurisdictions or bodies with the aim of preserving or restoring international peace and security. These measures also aim to protect human rights, safeguard democracy and the rule of law, guarantee national sovereignty and independence, and defend other fundamental interests of states. Sanctions are also an essential tool in preventing and combating terrorism and the proliferation of weapons of mass destruction.

An international sanction is a restrictive and temporary measure that limits the exercise of certain rights by imposing specific prohibitions or obligations.

Restrictive measures are applied by States or international organisations that maintain lists of designated individuals, groups or entities. This is namely the case of the European in the context of the *Common Foreign and Security Policy* (CFSP), the Sanctions Committee established by United Nations Security Council (UNSC) Resolutions, the *Office of Foreign Assets Control* (OFAC) and the *Office of Financial Sanctions Implementation* (OFSI).

NOTE: The European Union adopts restrictive measures both to comply with binding UN Security Council resolutions and on its own initiative. While the European Union is obliged to follow the terms of Security Council resolutions, it can choose to apply more comprehensive or demanding measures.

Restrictive measures usually fall into two categories:

- *Targeted*: aimed at specific individuals, entities or sectors, and may include restrictions on trade in certain goods;
- *Non-targeted*: applicable to countries, jurisdictions or territories in their entirety.

Sanctions or restrictive measures may be aimed at:

- Freezing of funds: aims to prevent the movement, transfer, alteration, use or management of funds – as well as access to them – whenever such operations may alter their value, location, ownership,

nature or destination. This measure also covers portfolio management and other financial instruments.

- Freezing of economic resources: prevents the movement, transfer, disposal or encumbrance of tangible or intangible assets, movable or immovable, which do not constitute funds but can be used to obtain funds, goods or services, for example through their sale, lease or mortgage.
- Embargoes: can be adopted by supranational organisations – such as the United Nations Security Council or the European Union – or by individual states, with the aim of restricting trade in certain goods and services (e.g. arms, dual-use goods or petroleum products) with the target state. Embargoes may be motivated by political, military, social or economic considerations. NOTE: It should be stressed that embargoes always target states or territories, so they are never imposed on natural persons.

The enforcement of sanctions that shall have been imposed constitutes an obligation for both the public and private sectors, shape up the conduct of business by the Group.

3. GENERAL PRINCIPLES

The Group undertakes to:

- ✓ Fully comply with all applicable sanctions and restrictive measures;
- ✓ Prevent doing business with sanctioned entities, reinforcing due diligence as set out by in-house policies;
- ✓ Maintain high ethical standards in line with the Code of Ethics and Business Conduct and the Integrity and Compliance Programme;
- ✓ Promote a culture of integrity and prevention of legal risks, as reinforced in compliance and internal communication meetings.

4. IDENTIFYING SANCTIONS RISKS

To ensure strict compliance with international sanctions and prevent direct or indirect involvement in prohibited activities, the Group adopts a risk-based approach. Early identification of risk factors and red flags is essential to establish the level of due diligence to be applied and to determine when a case needs to be escalated for further enhanced analysis.

Risks relating to non-compliance with Sanctions

Risks relating to non-compliance with sanctions include, but are not limited to:

- ✓ Legal Risk: heavy fines, administrative penalties, operational restrictions or criminal liability of the entities and employees involved;
- ✓ Financial Risk: financial losses resulting from the suspension of projects, blocking of payments or the impossibility to do business with regulated entities;
- ✓ Reputational Risk: damage to the Group's image, loss of trust from customers, partners and financial institutions;
- ✓ Operational Risk: disruption or delay in operations, projects, or supply chains due to violations or sanction-related investigations.

Risk Assessment Criteria

Exposure to sanctions should be assessed, namely considering following factors:

- ✓ Geography:
 - Countries subject to full or partial sanctions issued by the EU, UN, OFAC, UK or other relevant authorities.
 - Countries with frequent changes or regulatory instability.
- ✓ Counterpart:
 - Persons or entities featuring on sanctions lists or designated as *Specially Designated Nationals* (SDN).
 - Opaque or complex shareholder structures, which make it difficult to identify beneficial owners.
 - Entities with a negative record or involvement in risk sectors.
- ✓ Transaction or Activity:
 - Payments, financial or logistical operations linked to risk countries.
 - Use of intermediaries, agents or third parties without clear justification.
- ✓ Supply Chain:
 - Suppliers, distributors or subcontractors operating in sensitive regions.

5. GOVERNANCE

The governance model is aligned with the organisation of the Integrity and Compliance Programme.

Executive in charge of the Group's Regulatory Compliance

The Regulatory Compliance Officer is in charge of coordinating this regime within the Group, and shall:

- ✓ Monitor legislative changes and the updating of restrictive lists;
- ✓ Revise this Policy;
- ✓ Provide support to the business units in interpreting and enforcing the rules;
- ✓ Ensure the communication and reporting of incidents related to non-compliance.

Corporate Compliance Department and/or Local Compliance Teams

The Compliance Department shall:

- ✓ Monitor legislative changes and the updating of restrictive lists;
- ✓ Develop, update and disseminate this policy and its annexes;
- ✓ Provide support to the business units in interpreting and enforcing of the rules;
- ✓ Support due diligence and screening processes for counterparties and employees.

In-house Teams

All employees must:

- ✓ Carry out mandatory sanctions checks on established processes, including but not limited to KYC, due diligence, contracting out, selection of partners and customers, creation of banking entities, sales or equipment acquisitions);
- ✓ Immediately report any potential matches identified;
- ✓ Suspend operations in case of alert;
- ✓ Follow guidelines from the Corporate Compliance Department and Local Compliance Teams;
- ✓ Take part in compulsory training.

6. DISCIPLINARY MEASURES AND PENAL SANCTIONS

Failure to comply with this policy may result in:

- ✓ Internal disciplinary actions as referred to in item 16 of the policy;
- ✓ Civil and criminal liability;
- ✓ Reputational consequences for the Group.

The sanctions provided for in the legislation and corresponding implementing decrees may be imposed to the Group and to all individuals who are members of the corporate bodies, who exercise leadership or hold managerial positions, who act on its behalf, and to all employees and other individuals who provide permanent or occasional services.

7. SUPPORT LINKS

Financial Action Task Force (FATF/GAFI):

[Countries](#)

United Nations:

<https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>

<https://main.un.org/securitycouncil/en>

European Union:

https://www.eeas.europa.eu/eeas/european-union-sanctions_en

https://eu-sanctions-compliance-helpdesk.europa.eu/index_en

https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures_en

United States of America:

<https://ofac.treasury.gov/>

<https://ofac.treasury.gov/sanctions-list-search-tool>

<https://ofac.treasury.gov/sanctions-programs-and-country-information>

<https://ofac.treasury.gov/additional-ofac-resources/ofac-information-for-industry-groups>

United Kingdom:

<https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation>

<https://www.gov.uk/guidance/uk-financial-sanctions-guidance>

<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets>

MOTAENGIL

Um Mundo de Inspiração

