AGEM ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

1. Introduction

AGEM (hereinafter, “AGEM” or the “Company”), fully aware of the importance of preventing the use of the company as a vehicle for channelling resources of illicit origin or intended for criminal purposes, adopts through this **Corporate Policy on the Prevention of Money Laundering and Terrorist Financing** (hereinafter, the “Policy”) a firm and explicit commitment to **zero tolerance** for any practice that, directly or indirectly, could be linked to the commission of money laundering or terrorist financing offences.

Preventing such conduct is a priority objective for AGEM, not only because of the evident criminal, administrative and reputational liabilities that could arise for the company and the individuals who form part of it, but also because of the ethical and social obligation to act at all times with the utmost integrity, diligence and transparency. The Company's involvement in criminal activities of this nature would be incompatible with its corporate principles and values, would seriously affect the trust of customers, suppliers and authorities, and would jeopardise its own business viability.

AGEM therefore expressly declares that it will not tolerate direct or indirect participation, whether voluntary or through omission, in any activity that could give rise to a money laundering process, understood as the process by which economic resources of criminal origin are given an appearance of legality, nor in activities related to terrorist financing, consisting of providing, collecting or using funds for the purpose of committing terrorist acts or to be used, in whole or in part, by terrorist organisations.

This Policy is adopted in compliance with **Law 10/2010, of 28 April**, on the prevention of money laundering and terrorist financing, its implementing Regulation approved by Royal Decree 304/2014, of 5 May, as well as **Directives (EU) 2015/849 and 2018/843** and the Recommendations of the Financial Action Task Force (FATF). It is also aligned with the requirements of Article 31 bis of the Spanish Criminal Code regarding the criminal liability of legal entities and with **UNE Standard 19601:2025** on criminal compliance management systems, forming an essential element of AGEM's Criminal Compliance System.

AGEM's Sole Director, as the company's highest governing body, assumes ultimate responsibility for the approval, implementation, monitoring and continuous improvement of this Policy, compliance with which will be mandatory for all employees, executives, representatives and third parties acting on behalf of or for the Company, or who, by the nature of their commercial or contractual relationship, could expose it to money laundering or terrorist financing risks.

2. Purpose and objectives of the Policy

This Policy aims to establish a coherent, uniform and effective internal regulatory framework intended to prevent, detect and, where applicable, report any transaction, relationship or conduct that could be linked to money laundering or terrorist financing.

In compliance with applicable legislation and international standards, AGEM pursues, through this Policy, the following fundamental objectives:

First, to ensure that all economic, commercial and financial transactions in which the Company participates are carried out with full transparency, traceability and compliance with the law, so that in no case may they serve, even unintentionally, to channel illicit resources or resources intended for criminal purposes.

Second, to establish internal due diligence procedures for the proper identification and knowledge of customers, suppliers, contractors, intermediaries and business partners, in order to verify their integrity, reputation, financial capacity and, where applicable, the lawful origin of the funds they manage or transfer within the framework of their relationships with AGEM.

Likewise, the Policy aims to define clear and effective mechanisms for detecting and reporting suspicious transactions, so that any employee, executive or third party linked to the Company has secure, confidential and protected internal channels to immediately report facts or indications that could be contrary to applicable regulations.

Finally, this Policy seeks to foster a corporate culture of prevention and compliance regarding money laundering and terrorist financing, ensuring that all members of AGEM receive adequate training, are aware of their legal and internal obligations, and act with the utmost diligence in the performance of their duties.

3. Scope of application and obligated parties

The Policy will be mandatory for AGEM as the parent company, for all its subsidiaries and branches, both in Spain and abroad, for the Sole Director, the Compliance Officer, all employees, executives and representatives of the Company, as well as for all third parties — suppliers, contractors, intermediaries, commercial agents, strategic partners — whose activities, by their nature or volume, could pose money laundering or terrorist financing risks for AGEM.

All these parties must act within the framework of this Policy with diligence, integrity and transparency, expressly assuming the obligation to cooperate in the application of the internal due diligence procedures, risk detection, training and reporting of suspicious transactions provided for herein.

4. Guiding principles

AGEM's conduct regarding the prevention of money laundering and terrorist financing is based on a series of guiding principles that form the ethical, legal and operational basis of this Policy, ensuring its correct application at all levels of the organisation and in all jurisdictions where the Company carries out its activity.

First, the **principle of legality** requires strict compliance with all provisions contained in Law 10/2010, its implementing Regulation and applicable European Directives, as well as with the recommendations of the relevant international bodies, such as the Financial Action Task Force (FATF), the International Monetary Fund or the European Central Bank, to the extent that these may affect the Company's operations, products or services.

The **principle of due diligence** requires the application of controls proportionate to risk, based on adequate identification, verification and monitoring of customers, suppliers and business partners, particularly in cases where factors increase exposure to potentially unlawful transactions, such as presence in high-risk jurisdictions, the financial complexity of the transaction, or the use of significant amounts of cash.

For its part, the **principle of prevention** requires the Company to adopt organisational, training and technological measures aimed at avoiding, before they materialise, any transaction likely to be used for money laundering or terrorist financing purposes, ensuring an early and effective response to detected risks.

The **principle of transparency and traceability** implies that all economic, financial and commercial transactions in which AGEM participates must be recorded, documented and retained in accordance with applicable regulations, so that they can be subject to verification, audit and, where applicable, reporting to the competent authorities without undue delay.

The **principle of active cooperation** establishes AGEM's obligation to cooperate loyally and diligently with judicial, police and administrative authorities, in particular with the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (SEPBLAC), facilitating the immediate reporting of suspicious transactions and the provision of information and documentation requested in the exercise of their legal functions.

Finally, the **principle of confidentiality and whistleblower protection** guarantees that all internal communications relating to suspicious transactions or breaches of this Policy will be treated with the utmost confidentiality and security, expressly prohibiting any form of retaliation, sanction or discriminatory treatment against those who make such reports in good faith, in line with the provisions of Law 2/2023 and Directive (EU) 2019/1937 on the protection of persons who report breaches of regulations.

5. Due diligence and internal control measures

AGEM will implement a **Due Diligence System** comprising the identification, verification and ongoing monitoring of all customers, suppliers, contractors, intermediaries and business partners with whom the Company establishes commercial or professional relationships involving relevant economic or financial transactions.

The formal identification of individuals and legal entities with which AGEM interacts will include, at a minimum, obtaining and verifying their name, corporate name, address, activity, ultimate beneficial ownership, corporate structure and, where applicable, the existence of politically exposed persons (PEPs) directly or indirectly linked to the transaction or business relationship.

Compliance with the “know your customer” (KYC) principle will require obtaining sufficient and reliable information on the nature of the customer's or supplier's professional or business activity, the lawful origin of funds, the purpose and nature of the business relationship, and any other data relevant to assessing the money laundering or terrorist financing risk associated with the transaction or contractual relationship.

In cases where aggravating risk factors are present, such as complex cross-border transactions, use of fiduciary structures, presence in non-cooperative jurisdictions, unusually high amounts, or the involvement of politically exposed persons, AGEM will apply enhanced due diligence measures, including additional documentary verifications, requests for supplementary information, prior authorisations from the Sole Director, and specific monitoring by the Compliance Officer.

All transactions will be subject to **ongoing monitoring**, in order to detect unusual patterns, atypical transactions or behaviour that deviates from the customer's, supplier's or business partner's ordinary operations. This monitoring will be supported by technological tools and periodic review of available information, ensuring its constant updating and consistency with the evolution of the commercial or contractual relationship.

6. Identification, reporting and cooperation procedures with the authorities

When any employee, executive or third party linked to AGEM has indications, suspicions or knowledge that a transaction, business relationship or operation could be linked to money laundering or terrorist financing, they will have the immediate obligation to report it confidentially and securely to the Compliance Officer, through the internal channels established for this purpose.

The Compliance Officer, upon receiving the report, will urgently assess the suspicious transaction or operation, and may request additional information from the areas involved, adopting, where appropriate, precautionary measures such as the temporary suspension of the transaction until the internal review is completed.

If, in the judgement of the Compliance Officer and the Sole Director, the transaction shows reasonable indications of being related to money laundering or terrorist financing, AGEM will proceed to report it immediately to SEPBLAC, in accordance with the provisions of Law 10/2010 and its implementing regulations, providing all available documentation and information and cooperating loyally and diligently with that body and with any judicial or police authorities that may undertake the investigation.

Under no circumstances will the internal or external reporting of suspicious transactions constitute a breach of the duty of confidentiality protecting the whistleblower, nor will it give rise to labour, contractual or professional retaliation against anyone who has made the report in good faith, even if the reported facts are ultimately not confirmed.

7. Individual obligation of prior control and verification of transactions

In addition to the general system of prevention, supervision and control established in this Policy and the functions assigned to the Sole Director and the Compliance Officer, any AGEM employee or executive who receives, processes, authorises or executes payments, transfers or economic or financial transactions of any kind is subject to the **individual obligation of prior and diligent verification** of each transaction before it is processed or recorded.

This obligation is intended to establish a first level of decentralised control, at the point closest to the specific transaction, so that no payment or transfer can be executed unless the person directly responsible for its processing has verified, under their professional responsibility, that there are no objective grounds for suspecting its unlawful origin, lack of economic justification, or possible connection to criminal activities or terrorist financing.

Individual verification will include, at a minimum, checking:

- The identity of the payer and the beneficiary, comparing their consistency with the available contractual or commercial information.
- The consistency of the amount and description of the transaction with the nature and background of the existing commercial relationship.
- The consistency and sufficiency of supporting documentation, including invoices, contracts, payment orders and any other supporting evidence.
- The absence of indications of irregularity, such as payments to or from high-risk jurisdictions, opaque corporate structures, unusually large amounts of cash, or unjustified splitting of transactions.

If, during this individual verification, the responsible person detects any anomaly, inconsistency or suspicious indication, they will be obliged to suspend the transaction as a precaution and to report the incident immediately and confidentially to the

Compliance Officer through the established channel, refraining from proceeding with its execution until receiving express instructions to the contrary.

Failure to carry out this prior verification, processing transactions without due diligence, or failure to report suspicious indications will constitute a **serious breach** of this Policy, which may give rise to disciplinary or contractual measures, without prejudice to any administrative or criminal liability that may arise in the event of the commission of offences.

All verified transactions must be documented and recorded in AGEM's internal systems, expressly recording the identity of the person who carried out the verification, the date and time thereof, any incidents detected and, where applicable, any reports made to the Compliance Officer or the competent authorities.

Through this mechanism, AGEM effectively strengthens its commitment to the active prevention of money laundering and terrorist financing, ensuring that due diligence is not limited to centralised supervision, but permeates all stages and levels of the Company's operational and financial activity.

8. Staff training and awareness

The effectiveness of the money laundering and terrorist financing prevention system depends to a large extent on the level of knowledge, awareness and training of all persons who form part of AGEM. For this reason, the Company will implement an **ongoing training programme** aimed at all its employees, executives and collaborators, tailored to the nature of their duties, their level of responsibility and the risk exposure inherent to their positions.

The training will cover not only the legal and regulatory aspects of preventing money laundering and terrorist financing, but also the practical application of internal procedures, including the identification of suspicious transactions, the use of the established reporting channel, the required documentation, and the obligations of confidentiality and cooperation with the competent authorities.

The Compliance Officer will be responsible for designing and coordinating the training programmes, ensuring their periodic updating in line with regulatory developments, the guidelines of supervisory bodies, and lessons learned from audits, inspections or internal investigations.

Courses, workshops and training sessions will be documented through attendance records and performance evaluations, in order to demonstrate, in the event of inspections or judicial proceedings, that AGEM has fulfilled its legal obligation to adequately train its staff in this matter.

Training will be mandatory for all staff, and will also be included in the onboarding process for new employees and in the engagement of third parties whose activity could entail money laundering or terrorist financing risks.

9. Disciplinary regime and consequences of non-compliance

Failure to comply with the obligations arising from this Policy, Law 10/2010 and its implementing regulations will be considered a **serious breach** of AGEM's internal rules and may give rise to disciplinary, contractual or legal measures, depending on the nature, severity and significance of the conduct detected.

In the case of the Company's employees and executives, breaches will be sanctioned in accordance with applicable labour legislation, the applicable collective bargaining agreement and AGEM's internal disciplinary regime, and may consist of written warnings, suspension of employment and pay, or, in the most serious cases, termination of employment, without prejudice to any civil or criminal liability the offender may incur.

With regard to third-party contractors, suppliers or business partners, non-compliance with this Policy will constitute grounds for **immediate termination** of the contractual relationship, regardless of any legal action AGEM may take to claim damages, as well as the obligation to report to the competent authorities where there are indications of criminal offences.

All disciplinary and contractual measures adopted will comply with the principles of **proportionality, legality and respect for fundamental rights**, always guaranteeing the right of the alleged offender to be heard and to defend themselves, and the written documentation of the entire disciplinary process.

10. Supervision, monitoring and internal control

The Compliance Officer, under the direct supervision of the Sole Director, will be responsible for verifying the correct implementation of and compliance with this Policy, as well as periodically assessing the effectiveness of the internal procedures for preventing money laundering and terrorist financing.

To this end, an **Annual Supervision and Audit Plan** will be drawn up, including periodic reviews of the Risk Map, checks on the adequacy of internal procedures, analysis of unusual or suspicious transactions, and assessments of staff training and awareness levels.

The results of internal audits, as well as reports received through the established channel, measures adopted and any incidents detected, will be compiled in periodic reports that the Compliance Officer will present to the Sole Director, who will adopt the

necessary decisions to strengthen the prevention system and ensure its continuous improvement.

Likewise, whenever relevant regulatory changes occur, changes to the corporate structure, the opening of new subsidiaries in high-risk jurisdictions, or significant incidents related to the prevention of money laundering or terrorist financing, the Compliance Officer will propose the immediate review of the Policy, ensuring its continued adequacy to applicable legislation and international best practices.

11. Approval, entry into force and update

This Policy will be formally approved by AGEM's Sole Director, who assumes ultimate responsibility for its effective implementation, the allocation of the human, technological and financial resources necessary for its compliance, and the supervision of the money laundering and terrorist financing prevention system.

Once approved, the Policy will enter into force on the date indicated in the approval agreement and will be mandatory for all employees, executives, representatives and third parties linked to the Company, without exception.

The Policy will be reviewed periodically at least once a year, or more frequently when required by legislative changes, recommendations from the competent authorities, changes in AGEM's structure or activity, or when deficiencies in its practical application are detected.

Any modification or update to the Policy will likewise be approved by the Sole Director and communicated immediately to all recipients, ensuring its full accessibility through the corporate intranet, AGEM's website and the corresponding internal training processes.

Annex I – Operational Procedure for the Prevention of Money Laundering and Terrorist Financing

In order to ensure the correct application and operability of AGEM's Money Laundering and Terrorist Financing Prevention Policy (AML/CFT), the following mandatory internal procedure is implemented, establishing the specific responsibilities, measures and controls to be complied with in developing relationships and transactions with customers, suppliers, intermediaries and business partners.

1. Identification and Verification of Customers and Third Parties (KYC/KYB)

1.1. Identification Obligation

Before formalising any relevant transaction or business relationship, the full identity of the individual or legal entity must be verified by obtaining the following minimum documentation:

- Legal entities: Deed of incorporation, registration details, up-to-date articles of association, tax ID, corporate structure, identification of beneficial owners, and declaration of activity.
- Individuals: Valid identity document (national ID, foreign resident ID or passport), address, and professional or business activity.

1.2. Verification of Beneficial Ownership

In any relationship with companies, foundations or other legal structures, it will be mandatory to verify the identity of the individuals who directly or indirectly control more than 25% of the capital or voting rights, or who exercise control by other means.

1.3. Background Review

A basic check of reputational and disciplinary background and ownership of the entity will be carried out using public databases and sanctions lists (for example, EU, UN or FATF lists), including the identification of Politically Exposed Persons (PEPs).

2. Third-Party Risk Classification

Proper classification of the risk associated with customers, suppliers, financial intermediaries and business partners is an essential tool for preventing situations that could involve AGEM in money laundering or terrorist financing activities. This assessment will be based on a risk-based approach, considering both the intrinsic characteristics of the third party and those of the transaction and geographical environment.

2.1. Risk assessment factors

a) Risk inherent to the customer or third party

- Legal nature: companies with complex or recently established corporate structures, with no prior operating history or with a broad or ambiguous corporate purpose.
- Economic activity: high-risk sectors such as foreign trade, financial advisory services, import/export, foundations, real estate, etc.
- Opaque corporate structure: use of trusts, fiduciary accounts or unknown beneficiaries.
- Reputational history: presence in sanctions databases, media coverage of financial scandals, declarations of insolvency or bankruptcy.

b) Risk associated with the business relationship

- Volume and nature of transactions: contracts with significant amounts, unusual transactions, or payment through non-traceable instruments.

- Duration and frequency: occasional or intermittent contacts pose a higher risk than ongoing relationships with a transparent history.
- Payment method: the use of cash, cryptocurrencies, bearer cheques or accounts in opaque jurisdictions increases the risk level.

c) Geographical risk

- Countries included on FATF black or grey lists, with high levels of corruption, or where criminal or terrorist organisations operate.
- Jurisdictions sanctioned by the United Nations or the European Union.

2.2. Risk categories

Based on the above assessment, the third party will be classified into one of the following categories:

- Low Risk: public entities, recurring suppliers, companies with established practices, complete documentary verifications and justified activity.
- Medium Risk: new third parties with no prior history with AGEM, single relevant transactions, or customers with justifiable cross-border activity.
- High Risk: parties located in high-risk countries, PEPs, transactions with complex ownership structures, or cash or opaque payments.

Enhanced measures and staged authorisations will be applied to third parties classified as high risk.

3. Due Diligence Measures

Due diligence aims to verify the identity and activity of the third party, ensure the lawfulness of the origin of the funds and the transaction, and detect possible money laundering or terrorist financing risks before formalising the business relationship.

3.1. Standard Due Diligence

Applicable to third parties with a low or medium risk profile. It will include:

- Complete documentary verification.
- An initial check against sanctions lists.
- Confirmation of the purpose and expected volume of the business relationship.
- Assessment of available tax and accounting data.
- Review of consistency between the projected transaction and the third party's ordinary activity.

3.2. Enhanced Due Diligence

Mandatory for third parties classified as high risk or when aggravating factors are present (transactions exceeding €50,000, fiduciary structures, cash payments).

Additional Mandatory Documentation

- Bank certificates of the origin of funds.
- Declarations regarding beneficial ownership and ultimate beneficiaries.
- Notarial or banking verification for fiduciary structures.

Enhanced Authorisation and Supervision

- Complete prior review of all documentation by the Compliance Officer.
- Prior approval by the Sole Director.
- Inclusion of additional control and compliance clauses in contracts.

Additional Controls

- Quarterly periodic monitoring of the volume and nature of the relationship.
- Ongoing monitoring of executed transactions and changes in circumstances.
- Annual request for updated documentation.

3.3. Exemption from Due Diligence Obligations

May apply in justified cases such as relationships with:

- Public administrations or financial entities subject to supervisory regulations.
- Listed companies with verified publicly available information.

4. Ongoing Monitoring of Transactions

- All transactions must be reviewed to detect indications of irregularity.
- Transactions exceeding €50,000 or involving bank accounts of third parties in high-risk countries must receive special attention.
- Any deviation from expected activity must be documented and reported to the Compliance Officer.

5. Reporting of Suspicious Transactions

- Any employee who observes indications of money laundering or terrorist financing must report it immediately and confidentially to the Compliance Officer through the ethics channel.
- The Compliance Officer will assess the case and, where applicable, report the transaction to SEPBLAC.

- It is prohibited to disclose to the customer or third party the existence of an internal investigation or external report (“prohibition of tipping-off”).

6. Training Obligation

AGEM will guarantee initial, annual and post-regulatory-change training for its employees on the prevention of money laundering and terrorist financing, focusing on the most exposed areas (administration, purchasing, sales, international contracts, finance).

7. Retention of Documentation

All documentation obtained in application of this procedure must be retained for a minimum of 10 years, as established by Law 10/2010 and Royal Decree 304/2014.

8. Review of the Procedure

This Annex will be reviewed every 12 months by the Compliance Officer, or earlier if there are changes in applicable legislation, recommendations from supervisory bodies, or operational incidents.