AGEM ETHICS CHANNEL POLICY / INTERNAL INFORMATION SYSTEM

1. Introduction

AGEM Auxiliar General de Electromedicina, S.L. ("AGEM" or the "Company") has a **Code of Ethics and Conduct** that defines the principles of integrity, legality and transparency governing its actions and that constitute the framework of conduct required of all persons who form part of the Organisation and of those who interact with it within its value chain. In furtherance of this framework, and with the aim of preventing, detecting and responding to doubts, discrepancies or irregularities in compliance with the Code and applicable regulations, AGEM establishes and regulates through this Policy its **Internal Information System** (hereinafter, the "System"), comprising:

(i) the Ethics Channel as the preferred means of communication;

(ii) the Ethics Channel Management Procedure, which sets out the processing stages; and

(iii) the System Manager, endowed with sufficient powers and functional autonomy to ensure its effectiveness.

The architecture and purpose of this System are designed in line with best corporate practices reflected in comparable sector policies, ensuring alignment with **Law 2/2023, of 20 February**, and with **Directive (EU) 2019/1937**, as well as with AGEM's own organisational requirements (structure with a Sole Director and Compliance Officer).

2. Objective

The objective of this Policy is to establish the principles, guarantees and operating rules governing AGEM's **Ethics Channel** and the management of all communications received through the System, enabling the early identification and diligent handling of conduct presumed to be contrary to the law, the Code of Ethics, internal policies and the good governance commitments undertaken by the Company.

The Channel ensures confidential and secure access for reporting — including anonymously — and for enquiring about potentially irregular conduct, with effective protection against retaliation and processing in accordance with Law 2/2023 and data protection regulations.

3. Scope of application

This Policy is mandatory for AGEM and, where applicable, for its subsidiaries or branches, with global scope over the activities of its value chain, regardless of the territory in which they are carried out. It is binding on all AGEM personnel (employees, executives, the Sole Director and temporary or equivalent staff) and applies, to the

extent relevant, to business partners, suppliers, agents, distributors and other third parties that collaborate with the Company.

The Ethics Channel is the preferred means for reporting irregularities within AGEM's scope; if the information transmitted affects exclusively the personnel of an unrelated entity, AGEM will forward the communication to that entity where appropriate, always preserving confidentiality and whistleblower protection.

4. Conduct to be reported through the Ethics Channel

Actions or omissions that constitute or may constitute a breach of applicable law, the Code of Ethics, internal policies and procedures, or AGEM's corporate commitments must be reported through the System.

By way of illustration, and without limitation, this includes: **corruption and fraud** (public or private sector bribery, undue payments or advantages, accounting manipulation, disloyal management), **money laundering and terrorist financing**, breaches of competition and procurement rules (collusion, market sharing, influence peddling), violations relating to personal data and information security, labour and occupational risk prevention infringements, workplace or sexual harassment and discrimination, environmental damage, violations of intellectual or industrial property rights, breaches of the health, traceability and product safety framework specific to AGEM's activity, as well as any other internal or external breach of a similar nature.

5. Reporting breaches: channels, access and timeframes

All AGEM personnel have a duty to report conduct individually or collectively observed in the professional sphere that may contravene the Code, this Policy or the rest of the Company's Compliance System, regardless of whether it originates from a hierarchical superior. The Channel allows anonymous reports and enquiries regarding the interpretation of regulations or internal policies.

Reporting channels. AGEM will provide, at a minimum, a secure digital channel — an encrypted electronic mailbox at canal.etico@grupo-agem.com — integrated into the Internal Information System.

Preference for the internal channel and external channels. The Internal System is the preferred means of communication. Notwithstanding this, any person may resort to the external channels provided for in Law 2/2023 (the Independent Whistleblower Protection Authority or the competent regional authorities) whenever they consider it appropriate.

6. Principles and guarantees of the Ethics Channel

AGEM's Ethics Channel is governed by the following material and procedural principles and guarantees:

- The obligation to report based on reasonable indications; **full confidentiality** of communications and the case file.
- Protection of the whistleblower and **prohibition of retaliation** against good-faith reports.
- The whistleblower's right to be informed of the status and outcome, and the right of the affected person to be heard, with respect for their presumption of innocence.
- Diligence and speed in processing.
- Suitability, necessity and proportionality of investigative measures; full respect for the law, including data protection regulations and cooperation with authorities.
- Confidentiality and professional secrecy during the investigation, with AGEM entitled to decide on the submission of the case file or information to any judicial or administrative proceedings that may arise, in defence of the Organisation.

7. Management of the Ethics Channel: procedural stages

Management of the Ethics Channel is the responsibility of the **System Manager** (AGEM's Compliance Officer), who acts with independence and functional autonomy from operational areas. The corporate management procedure will comprise, as a minimum, the following stages:

Stage 1: Receipt and registration

- Enabled channels: a secure, confidential digital platform, and in-person or remote meetings upon request.
- Anonymity: anonymous submissions are permitted, without prejudice to processing.
- Acknowledgement of receipt: the Compliance Officer must acknowledge receipt to the whistleblower within a maximum of 7 calendar days.
- Registration: every communication is registered with a unique code in the internal system, classified by date, origin, type and risk level.

Stage 2: Preliminary review

- Admissibility is reviewed: relevance to the scope of the Code of Ethics, internal policies or legislation; minimum information needed to allow processing.
- If information is insufficient, additional information is requested from the whistleblower (if not anonymous).

- If the report is manifestly false or made in bad faith, it is documented and closed with a reasoned report.

Stage 3: Internal investigation

- An investigation team is appointed (Compliance Officer and, where appropriate, external legal counsel or internal audit).
- Investigative actions are carried out: interviews, document review, digital forensic analysis, requests for evidence.
- Confidentiality and whistleblower protection are guaranteed throughout the stage.
- The affected person is informed and has the right to be heard, except where there is a risk of destruction of evidence.

Stage 4: Report and decision

- The Compliance Officer issues a final report including: established facts; evidence obtained; proposed measures (closure, disciplinary measures, corrective actions, contract termination or reporting to authorities).
- The Sole Director approves final decisions where they involve sanctions or external legal action.

Stage 5: Communication of the outcome

- The whistleblower receives a final response within a maximum of 3 months (extendable to 6 in complex cases).
- The final communication is documented and the case file is archived with appropriate security measures.

Cross-cutting principles of the procedure

- **Absolute confidentiality**: the identity of the whistleblower, the affected person and witnesses is protected by technical and organisational means.
- **Prohibition of retaliation**: any adverse action motivated by a good-faith report will be subject to disciplinary sanction.
- **Data protection**: compliance with the GDPR and applicable national data protection law throughout the processing of personal information.
- **Traceability and documentation**: all stages are recorded for internal audit purposes and, where applicable, for the competent authority.
- **Periodic review**: the procedure is reviewed annually or whenever required by regulatory or risk-related changes.

8. Compliance Function: commitments, conflicts of interest and reporting to the governing body

The Compliance Officer and any person appointed to assist in managing the System must act with diligence, independence and confidentiality, refraining from intervening whenever a conflict of interest arises.

If the conflict affects the System Manager personally, they will notify the Sole Director, who will designate, on a case-by-case basis, the person who will assume responsibility for resolving the communication (for example, internal audit or external legal counsel).

Without prejudice to the confidential nature of investigations, the System Manager will periodically inform the Sole Director, through aggregated and anonymised reports, on the operation of the Channel (communications received, types, processing times, measures adopted and improvement actions).

9. Awareness and declaration of conformity

Compliance with this Policy constitutes an organisational commitment and a strategic objective. Accordingly, the following will be required:

1. Acknowledgement and approval by the Sole Director.
2. Express adherence by AGEM personnel, through individual declarations of conformity and their inclusion in the training programme.
3. Inclusion of compliance clauses in contracts with business partners and third parties who access the Channel or may be affected by its operation.

Whenever substantive changes are made to this Policy, adherences will be renewed and its update will be communicated to all affected persons and third parties.

10. Approval, entry into force and update

This Policy will enter into force on the date of its approval by AGEM's Sole Director. It will be reviewed annually and, additionally, on an extraordinary basis whenever there are changes in strategic objectives, external or internal regulatory changes, or when analysis of the Channel's operation reveals the need for organisational or procedural adjustments.

The Compliance Officer will assess proposed amendments and submit any relevant updates for approval by the Sole Director.

11. Dissemination

AGEM will make this Policy available to all personnel through internal corporate media and, where applicable, on its website, and will adopt the necessary measures to ensure its adequate dissemination, awareness and practical accessibility for stakeholders,

including clear signposting of the Channel's reporting routes in internal communications, onboarding policies and contractual documentation with third parties.

12. Control, monitoring and supervision

Control and monitoring. The Compliance Officer will be responsible for the ongoing monitoring of the Channel's operation in accordance with the approved internal procedure, including indicators on acknowledgement and resolution timeframes, investigation quality, corrective measures and training actions.

Supervision. The Sole Director will oversee the System based on periodic reports and may request, whenever deemed appropriate, internal or external audits to verify the Channel's effectiveness, compliance with Law 2/2023, and consistency with AGEM's Criminal Compliance System.

Annex I. Definitions

For the purposes of this Policy, and to ensure consistent interpretation with AGEM's Criminal Compliance System, the following definitions are established, among others:

- **Internal Information System**: the set comprising the Channel, the System Manager, this Policy and the Management Procedure.
- **Ethics Channel**: the channel or set of channels enabled to receive and manage good-faith communications relating to breaches.
- **Whistleblower**: an individual who reports facts within the material scope of the Channel, with the guarantees provided under Law 2/2023.
- **Affected person**: the person to whom the reported facts relate.
- **Retaliation**: any act or omission involving unfavourable treatment causally linked to a good-faith report.
- **Compliance Officer**: a single-person body with functional autonomy responsible, among other functions, for managing the System and verifying its effectiveness.
- **Sole Director**: AGEM's governing body with ultimate responsibility for the approval, resourcing and supervision of the System.