ARQUIMEA GROUP INTERNAL INFORMATION SYSTEM POLICY

ARQUIMEA

V.1 5 July 2023

CONTENT

1. Object of the document

Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption (hereinafter, "**Whistleblower Protection Law**"), which transposes into Spanish law Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, requires companies of a certain nature to have an Internal Information System (hereinafter, "**IIS**") under the terms provided for therein.

The main objectives of the establishment of an IIS are to protect persons who, in an employment or professional context, detect serious or very serious criminal or administrative offences and report them through the mechanisms regulated for this purpose, as well as to strengthen and promote the culture of information as a mechanism for preventing and detecting irregular conduct.

The purpose of this Policy is to set out the general principles that inspire the IIS of ARQUIMEA GROUP, S.A. and of any of the companies comprising the Group (hereinafter, "**Arquimea**" or "the **Group"**), as well as other matters provided for in the aforementioned Whistleblower Protection Act, such as the channel or channel enabled for the receipt of communications relating to breaches, the procedure to be followed for the processing of such communications, the person in charge of the IIS or the protection measures and guarantees established in favour of whistleblowers, which shall only be applicable to the communications referred to in the aforementioned Act.

2. Scope of application

This Policy is applicable to all members of Arquimea and to those informants who, not being members of Arquimea, have obtained information about some type of action or omission in a work or professional context, including in any case:

- Any person working for or under the supervision and direction of Arquimea, its contractors, subcontractors and suppliers.
- Persons who have been members of Arquimea in the past, having terminated their employment or statutory relationship with the Group.
- Volunteers and trainees, paid or unpaid.
- Persons whose employment relationship has not yet started, in cases where information on infringements has been obtained during the selection process or pre-contractual negotiation.

Any of these informants may report, through the procedures provided for in this Policy, of:

- Actions or omissions that may constitute a serious or very serious criminal or administrative offence. In any case, all serious or very serious criminal or administrative offences that involve financial loss for the Public Treasury and Social Security will be understood to be included. Also included are those conducts constituting non-compliance with Law 10/2010, of 28 April, on the prevention of money laundering and financing of terrorism and its implementing regulations, or the policies and procedures implemented to comply with them, committed within the Group.

- Conduct that may imply, by action or omission and on the part of a member of Arquimea, facts that have an effective implication in the professional relationship with Arquimea of the person to whom the communication refers, related to the commission in a work or professional context of any act contrary to the rules of action of the Arquimea Code of Ethics and Conduct or to the other provisions of the Group's internal Regulatory Compliance Programme.

- Any acts or omissions that may constitute breaches of European Union law.

3. Arquimea's Internal Information System

Arquimea's IIS is mainly composed of the Communication Channel enabled for the reception of the communications envisaged in the scope of application of this Policy, the IIS Manager and the procedure to be followed for the processing of the aforementioned communications, called "**Procedure for the management and processing of the information received in the Internal Information System**".

3.1. General Principles

The following general principles apply to Arquimea's IBS:

a. Accessibility: allows all reporting persons to communicate information on breaches under the second paragraph of this Policy, in writing or orally, and may do so anonymously in order to fully safeguard their identity.

b. Integration: Arquimea's Internal Information Channel through which communications are made is perfectly integrated and mimicked in the Group in the IIS.

c. Confidentiality: Arquimea's IIS is prepared and designed to manage in a completely secure manner all the data transmitted through the Internal Information Channel set up for this purpose, so as to guarantee the confidentiality of the data and the identity of the informant and any third party mentioned in the communication, as well as the actions carried out for the management and processing of the same. Likewise, the rights to privacy, intimacy, honour, defence and the presumption of innocence of the persons involved in the investigation process shall be protected and safeguarded at all times.

   The identity of the informant and of the other persons involved in the investigative process may only be communicated to the judicial authority, the Public Prosecutor's Office or the competent Administrative Authority in the framework of a criminal, disciplinary or sanctioning investigation, after the informant or the third party concerned has been informed, provided that this circumstance does not jeopardise the investigation or the judicial proceedings underway.

d. Proportionality: the actions carried out within the framework of an internal investigation shall always be carried out in accordance with criteria of proportionality and objectivity. The person denounced in the communication has the right to be informed of the facts attributed to him/her and to be heard at any time. Once informed, he/she may request to examine the information and documentation contained in the file to which the processing of the communication has given rise, although the necessary measures must be taken to safeguard the identity of the informant.

e. Publicity: both this Policy and Arquimea's Internal Information Channel are made available to informants in a clear and accessible manner through Arquimea's website at the following address: www.arquimea.com.

3.2. Internal Information Channel

Arquimea's Internal Information Channel ("**Whistleblower Channel**") is perfectly integrated into the Group's IIS and is the preferred channel for reporting the conduct envisaged in the second section of this Policy.

Reports of sexual or gender-based harassment made by Arquimea employees in accordance with the Group's Equality Plan will be included in the aforementioned Internal Reporting Channel (and, therefore, in Arquimea's IIS). Consequently, employees may also submit a report of sexual or gender-based harassment directly through the Whistleblower Channelnel, as may any other informant as provided for in the aforementioned second section of this Policy.

The Arquimea Ethical Channel allows:

a. Make written or oral communications, or both, under the conditions provided for in the Whistleblower Protection Act.
b. Include in the communication information such as the address or e-mail address for the purpose of receiving notifications.
c. Submit and process anonymous communications.
d. Inform the informant in a clear and accessible manner about updates on the investigation and external reporting channels to the competent authorities and institutions.

3.3. IIS procedure

Complementing this Policy, Arquimea has developed an internal procedure for the management and processing of communications received through the Whistleblower Channelnel, also integrated in the Group's IIS. This procedure also complies with the requirements established in the Whistleblower Protection Act.

3.4. External information channels

Without prejudice to the preferential channel of Arquimea's Whistleblower Channelnel for the communication of possible breaches of the Whistleblower Protection Act, whistleblowers may also report to the Independent Whistleblower Protection Authority, or to the corresponding regional authorities or bodies, the commission of any actions or omissions included in the scope of application of the Whistleblower Protection Act, either directly or following communication through the corresponding internal channel.

4. Head of Arquimea's Internal Information System

The person responsible for the management of Arquimea's IIS, appointed by the administrative body, is the Managing Partner of the Seville office of CREMADES & CALVO-SOTELO, a single-person body that assumes responsibility for Arquimea's Compliance System.

The designation of the IIS Officer shall be notified to the Independent Authority for the Protection of the informant or, where appropriate, to the competent authorities or bodies of the Autonomous Communities, within the scope of their respective competences.

Arquimea's IBS Manager will diligently assume, and in the absence of a conflict of interest, the resolution of the procedures initiated as a result of the information received through the established Whistleblower Channelnel, ensuring the proper application of the IBS Procedure. In the event of a conflict of interest, the management body shall appoint the person in charge of such resolution, who in the exercise of this function shall be subject to the same obligations and principles as the IBS Manager.

The person in charge of the IIS shall keep a register of the information received and of the investigation files to which it has given rise, guaranteeing the confidentiality of the information at all times.

The Head of the IIS also has all the material and personal resources necessary for the proper performance of his or her duties, which he or she will carry out in full compliance with the general principles of the IIS.

5. Support and protection measures

Individuals who report or disclose breaches through the Arquimea Whistleblower Channelnel will have access to the following support measures:

a. Comprehensive and independent information and advice, easily accessible to the public and free of charge, on the procedures and remedies available, protection against reprisals and the rights of the person concerned.

b. Effective assistance by competent authorities to any relevant authority involved in their protection against reprisals, including certification that they are eligible for protection under this law.

c. Legal assistance in criminal proceedings and cross-border civil proceedings in accordance with Community law.

d. Financial and psychological support, on an exceptional basis, if so decided by the Independent Authority for the Protection of the Informant, I.A.P. following an assessment of the circumstances arising from the submission of the communication.

In addition, based on the provisions of the Whistleblower Protection Act, the following protective measures will be taken:

a. Persons who communicate information about actions or omissions under this Policy or who make a public disclosure under the Whistleblower Protection Act will not be deemed to have violated any disclosure restrictions, and will not incur any liability of any kind in connection with such communication or public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure of such information was necessary to disclose an action or omission. This measure shall not affect criminal liability.

   The provisions of the preceding paragraph extend to the communication of information made by the representatives of the employees, even if they are subject to legal obligations of confidentiality or of not disclosing reserved information. This is without prejudice to the specific rules of protection applicable in accordance with labour legislation.

b. Whistleblowers shall not incur liability in respect of the acquisition of or access to information that is publicly communicated or disclosed, provided that such acquisition or access does not constitute a criminal offence.

c. Any other potential liability of reporters arising from acts or omissions that are unrelated to the communication or public disclosure or that are not necessary to disclose a violation under this law will be enforceable under applicable law.

d. In proceedings before a court or other authority concerning harm suffered by whistleblowers, once the whistleblower has reasonably established that he or she has communicated or made a public disclosure and has suffered harm, it shall be presumed that the harm occurred in retaliation for reporting or making a public disclosure. In such cases, it shall be for the person who has taken the detrimental action to prove that such action was based on duly justified reasons not linked to the public report or disclosure.

e. In legal proceedings, including those relating to defamation, copyright infringement, breach of secrecy, infringement of data protection regulations, disclosure of business secrets, or claims for damages based on employment or statutory law, the whistleblower and those persons to whom whistleblower protection is legally extended shall not incur liability of any kind as a result of communications or public disclosures protected by the Whistleblower Protection Act. Such persons shall be entitled to plead in their defence in such legal proceedings that they have communicated or made a public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure was necessary to expose a violation under the Whistleblower Protection Act.

f. During the processing of the file, the persons concerned by the communication shall have the right to the presumption of innocence, the right of defence and the right of access to the file, as well as the same protection as that established for informants, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure.

Anything not expressly set out in this Policy shall be governed by the provisions of the Whistleblower Protection Act.

6. Book-Register of information and data protection

Arquimea's IIS has a log book where the information received by the Whistleblower Channelnel and the internal investigations to which they have given rise are compiled, guaranteeing, in all cases, the confidentiality requirements set out in the Whistleblower Protection Act.

This register is not public and only at the reasoned request of the competent judicial authority, by means of an order, and in the context of judicial proceedings and under its supervision, may access all or part of the contents of the register be granted.

With regard to the protection of personal data, the processing carried out within the framework of the IIS is done in full compliance with the general principles and obligations laid down in the regulations on the protection of personal data and the Whistleblower Protection Act.

The data collected by the IIS are processed by ARQUIMEA GROUP, S.A. acting as data controller.

ARQUIMEA

arquimea.com