PROCEDURE FOR THE MANAGEMENT AND PROCESSING OF COMMUNICATIONS RECEIVED IN THE INTERNAL INFORMATION SYSTEM OF THE ARQUIMEA GROUP

ARQUIMEA

V.1 22 August 2023

INDEX

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, "Law 2/2023"), establishes the need to have an Internal Information System, which is the preferred channel for channelling communications, as it is preferable for information on irregular practices to be known by the organisation itself in order to correct them or repair the damage as soon as possible, without prejudice to the possible liabilities incurred in accordance with the applicable legislation in force.

In this way, diligent and effective action within the organisation itself can paralyse the harmful consequences of the actions under investigation, and after analysis of the possible causes, establish mechanisms to prevent similar practices from recurring.

ARQUIMEA GROUP, S.A. (hereinafter, "**Arquimea**" or "the **Group**"), has an Internal Information System (hereinafter, "SII") in operation to guarantee express compliance with Law 2/2023 and thus 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. Arquimea's SII is made up of the Internal Information System Manager, the Internal Information System Policy, the Internal Information Channel and the procedure developed below for the management and processing of information received through the Internal Information Channel.

The purpose of this document is to establish the procedure for the management and processing of the information received in the Internal Information Channel of Arquimea and of any of the Group companies, which constitutes the preferred channel for the communication of the conduct envisaged in section 2 of the Arquimea Internal Information System Policy.

2. Responsible for the Internal Information System

The Head of Arquimea's Internal Information System and, therefore, the person in charge of investigating the files received through the Internal Information Channel, is the Group's Compliance Officer, and will be the person in charge of managing the proper functioning of said Channel in the investigation phase unless there is a conflict of interest or other impediment, in which case the Head of the Internal Information System will designate another instructor. He/she shall carry out his/her work under the premises of independence, neutrality and impartiality, with honesty and objectivity towards all persons involved. He/she shall ensure that the entire procedure is carried out in accordance with the rules and principles set out in this Procedure and in Arquimea's SII Policy.

The Head of the Internal Information System shall have the following main responsibilities:

1. Receive communications made through the Internal Information Channel;
2. To analyse the communications received and decide on their admissibility;
3. To investigate the corresponding files, in accordance with the rules and principles established in this Procedure, and to submit the corresponding Proposal for Resolution to the Head of the SII or the body responsible for resolving the case;

3. Channels for communicating information

The communication channels included in Arquimea's Internal Information System enable communication in the following ways:

1. Through the "Arquimea Group Internal Information Channel" platform, accessible from the Arquimea website www.arquimea.com/es. Communications made through this platform may be made in writing or verbally, or both. In the case of verbal communications, the informant will be warned that the communication will be recorded and will be informed of the processing of their data, unless they have been previously informed.

2. By sending a written communication to the attention of the Head of the Internal Information System of Arquimea, to the following postal address: Avd. Constitución, 27 1ª planta - 41004 Sevilla (Spain).

At the informant's request made through any of the identified channels, the communication may also be submitted by means of a face-to-face meeting within a maximum of seven days.

Verbal communications, including through face-to-face meetings, should be documented by a recording of the conversation in a secure, durable and accessible format, or by a complete and accurate transcript of the conversation by the staff responsible for handling the conversation.

4. Processing of information received

a) Acknowledgement of receipt of communication and registration

Once the communication has been received in any of the forms provided for in section 3 of this document, the Head of Arquimea's Internal Information System must issue an acknowledgement of receipt to the informant within a maximum period of seven calendar days from its receipt, unless this could jeopardise the confidentiality of the communication, it is not possible due to the anonymous nature of the communication, or the informant has expressly renounced receiving communications relating to the research.

Likewise, within the aforementioned period of seven calendar days, the Head of Arquimea's Internal Information System shall enter the aforementioned communication in the SII's information register-book, giving it an entry number and indicating a date of receipt.

b) Preliminary examination and admission for processing

Within ten working days from the date of entry in the Internal Information System register-book, the person in charge of the SII, with the appropriate personal resources, shall carry out a preliminary analysis of the communication to identify whether it can be accepted for processing, the result of which shall be classified in at least one of the following cases:

1. Inadmissibility of the communication:

    a. When the facts reported lack any credibility.
    b. Where the facts reported do not constitute an infringement of the law falling within the scope of Law 2/2023.
    c. When the communication is manifestly unfounded or there are reasonable grounds to believe that it was obtained through the commission of an offence. In the latter case, in addition to the inadmissibility, a detailed account of the facts deemed to constitute an offence shall be sent to the Public Prosecutor's Office.
    d. Where the communication does not contain significant new information on infringements compared to a previous communication in respect of which the relevant proceedings have been completed, unless there are new factual or legal circumstances that justify a different follow-up.

2. Admissibility of the communication.

3. Immediate referral to the authority, entity or body considered competent to process it, depending on the material or personal scope.

4. Referral to the Public Prosecutor's Office, when the facts could be indicative of a criminal offence.

c) Instruction and resolution

Investigative actions shall comprise all actions aimed at verifying
the plausibility and the facts reported, with the possibility of maintaining communication with the informant and, if deemed necessary, requesting additional information, and concluding in one of the first two cases mentioned in the preliminary analysis.

Respect for the presumption of innocence and the honour of the persons concerned shall be maintained at all times, establishing the right of the persons concerned to be informed of the actions or omissions attributed to them in a succinct manner, to be heard at any time, as well as to be informed of the processing of their personal data. Such communication shall take place at such time and in such manner as is deemed appropriate to ensure the proper conduct of the investigation.

All members of Arquimea are obliged to cooperate loyally in the investigation, and the intervention of witnesses and affected persons is strictly confidential.

The maximum time limit for responding to the investigative actions shall be three months from the date the information enters the register. This period may be extended up to a maximum of a further three months in those cases of particular complexity that so require. This response to the proceedings will be reflected through the issuing of the Resolution of the File, which will contain, at least:

1. A statement of the facts reported together with the identification code of the communication and the date of registration.

2. The actions carried out in order to verify the plausibility of the facts.

3. The conclusions reached in the investigation and the assessment of the proceedings and the evidence supporting them.

In the Resolution of the File it may be agreed:

1. The case will be closed on the grounds that the infringements reported do not exist, and the informant will be notified (unless this is not possible due to the anonymous nature of the communication or because he/she has waived the right to receive communications relating to the investigation) and, where appropriate, the person concerned.

2. That an infringement has been detected, with the adoption of the corresponding sanction.

5. Confidentiality of information

The person submitting a communication has the right not to have his or her identity disclosed to third parties, although the identity may be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or disciplinary investigation.

Disclosures made under this paragraph shall be subject to the safeguards laid down in the applicable rules. In particular, they shall be communicated to the informant before disclosing his or her identity, unless such information could jeopardise the investigation or judicial proceedings. Where the competent authority so informs the informant, it shall send him or her a written statement explaining the reasons for the disclosure of the confidential data concerned.

Arquimea's Internal Information System has appropriate technical and organisational measures in place to preserve the identity and guarantee the confidentiality of the data corresponding to the persons concerned and to any third party mentioned in the information provided, especially the identity of the informant in the event that he/she has been identified.

To this end, the System is set up and managed in a secure manner, so that the confidentiality of all actions carried out in the processing of communications is guaranteed. The information will be contained in a secure database with restricted access.

It should be borne in mind that the informant, by reporting the existence of a criminal or administrative offence, does not have the status of interested party, but of collaborator with the Administration.

ARQUIMEA

arquimea.com