MEMBER OF
BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

OPERATING RULES FOR THE INTERNAL REPORTING CHANNEL OF AZTI FOUNDATION

1. Introduction

AZTI FOUNDATION (FUNDACIÓN AZTI FUNDAZIOA), hereinafter "AZTI", has had a compliance programme in place for several years, primarily aimed at preventing offences. A key component of this programme is the whistleblowing channel or information channel, which is intended to enable the secure reporting—among other matters—of potential criminal offences and/or possible breaches of the Code of Conduct arising in the course of our activities. Since its initial implementation, our channel and the management procedure have fully complied with the best standards in this area.

However, during 2023, Law 2/2023 of 20 February, regulating the protection of persons who report regulatory infringements and combating corruption (hereinafter "Law 2/2023"), was approved and entered into force. This legislation, which was initially intended to transpose a 2019 European Union Directive into national law, has gone much further than the Directive envisaged in several respects, introducing numerous changes and requirements affecting both public- and private-sector entities.

As expected, AZTI—using specialised external advice and following consultation with the legal representatives of employees—has implemented various changes to its channel and procedure, adapting them to the obligations arising from Law 2/2023.

We have an Information System and a first-level AZTI Internal Reporting Channel. Below we summarise the most relevant features of the Channel and the procedure for managing the information received.

2. What can be reported through the Internal Reporting Channel?

Information (lawfully obtained in the course of a work or professional activity in or with AZTI) may be reported if it relates to one or more of the following actions or omissions (hereinafter, the alleged "Infringements"):

(i) Any action or omission that may constitute an infringement of European Union law, provided that it: falls within the scope of application of EU acts; affects the financial interests of the European Union; or impacts the internal market.

(ii) Any breach of AZTI's Code of Conduct, as well as any alleged breach of the other protocols or internal rules that make up AZTI's Compliance system.

(iii) Any criminal offence.

(iv) Any serious or very serious administrative infringement, mainly (though not exclusively) those that could affect state, provincial/foral, local or regional tax authorities, or the Social Security system.

(v) Any serious or very serious infringement relating to occupational health and safety, including situations that may be considered harassment.

3. Which conflicts are expressly excluded?

Law 2/2023 protects only those persons who report situations that have a broader impact on the organisation or on third parties, excluding personal conflicts that have no legal or administrative relevance.

In this regard, for example, a workplace dispute between two employees—even with different roles or positions—based solely on personal conflicts (poor relationship, competitiveness, etc.) should not be reported through this Internal Reporting Channel.

4. Who can use the Internal Reporting Channel?

Any member of AZTI—understood to mean all persons professionally linked to the entity, whether as employees (under any arrangement), shareholders, executives or members of the Board of Directors—may submit information about alleged Infringements through the Internal Channel, either directly or through a representative.

In addition, external third parties such as self-employed persons, supplier companies, contractors and subcontractors (and their employees) may also report the Infringements referred to above through this Channel, fully subject to its requirements and procedure.

5. How can an alleged Infringement be reported?

Our System and Channel provide various forms and means of reporting, at the informant's choice:

(i) **Written report:**
Via the email address enabled by AZTI for this purpose: **canal@azti.es**

(ii) **Verbal report:**
By telephone on: **667 174 291** (asking for the System Manager / Compliance Officer).

(iii) **In-person meeting or video conference:**
Additionally, if the informant wishes, they may request an in-person meeting or a video conference (MS Teams or similar) to provide the information.

The routes just described refer to AZTI's Internal Reporting Channel. In addition, all potential informants are reminded that they will also have the option to report the alleged Infringements described above through the external reporting channels managed by public authorities, once

these are established.

6. Are anonymous reports permitted? What requirements apply when submitting information about a possible Infringement?

Any informant may choose whether to submit their report anonymously or non-anonymously; this is entirely at their discretion. In any case, it should be noted that, in accordance with the Law, AZTI's Internal Information System guarantees not only confidentiality but also the non-disclosure of the informant's identity (save for the cases provided for in Law 2/2023).

On the other hand, any informant who wishes to receive notifications relating to the information submitted must provide an email address (or another secure means of communication) and undertake to preserve the confidentiality of the content of the notifications received.

Whichever format or route is chosen (anonymous or not; in writing; meeting; telephone, etc.), the informant is required to provide as much information as possible about the alleged Infringement, in particular:

(i) A basic description of the facts. What alleged Infringement may have been committed and how?

(ii) The dates on which it was committed, or approximate dates. When did the Infringement take place?

(iii) The persons suspected of having committed the Infringement, those who participated, and others who may have knowledge of it. Who committed it / helped to commit it / were involved?

(iv) Documents, audio, videos, data or any other sources of information (paper or electronic) that may be used to corroborate or clarify the alleged Infringement. What evidence or indications are available?

7. Key aspects of the procedure for managing information received

7.1 Principles governing the procedure

(i) Confidentiality. Protection of the informant acting in good faith and their right not to suffer retaliation.

(ii) Protection of personal data.

(iii) Protection of the rights and interests of persons affected by the infringement.

7.2 Stages of the procedure

Stage I: Preliminary analysis of the information received
Responsible body: the System Manager.

Stage II: Admission or rejection of the report
Responsible body: the System Manager.

A decision is taken:

(i) Admit the report for processing and open an investigation (Stage III).

(ii) Reject the report, for example, where the facts described:

▪ do not constitute an Infringement.

▪ are wholly implausible.

▪ are manifestly unfounded, or there are reasonable indications that the information or the evidence/initial evidence provided was obtained unlawfully.

▪ do not provide significant new information regarding an Infringement that has already been reported and closed.

Stage III: Investigation and Final Report
Responsible body: the System Manager (who may request support from another department, such as HR).

(i) The appropriate investigative steps are carried out (e.g. statements from affected/investigated persons, witnesses, etc.).

(ii) Preparation of a Final Report following the investigation, proposing:

▪ Continuation of the procedure (it is considered that there are reasonable indications of an Infringement).

▪ The opening of a disciplinary file or labour adversarial procedure (in accordance with the applicable collective agreement), if the System Manager considers there are indications of an employment-related breach (unless proceedings had already been opened previously).

▪ Closure of the procedure:

• it does not constitute an Infringement

• its commission is not sufficiently substantiated

• no known perpetrator has been identified

Stage IV: Final decision
Responsible body: the management body or the body to which it has delegated (e.g. the Managing Directorate).

A prior hearing may be granted to the affected persons. A decision is taken:

(i) Close the file.

(ii) Agree to some or all of the proposals made by the System Manager.

MEMBER OF
BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

8. Closing remarks

Reporting alleged legal infringements in the course of carrying out activities is not only a right; in the case of our professionals, it is also an obligation.

Moreover, it is an essential element of the compliance programme, and an indicator for assessing whether that programme is complete and effective or whether it needs to be improved in certain respects.

If in doubt, any potential informant may request further information by contacting the Compliance Committee or the person responsible for the Information System.