TRI MARINE
TUNA DONE RIGHT SINCE 1972

1. Scope

Contents

2. Purpose

2.1 Justification for the adoption of this Policy

TRI MARINE (TMI) is convinced that the implementation of an effective Whistleblowing Management System (WMS) will build organizational trust by:

- Demonstrating leadership commitment to preventing and addressing wrongdoing.
- Encouraging people to come forward early with reports of wrongdoing.
- Reducing and preventing detrimental treatment of whistle-blowers and other involved.
- Encouraging a culture of openness, transparency, integrity, and accountability.

Following ISO 37002 guidance, our organization aims to create a whistleblowing management system based on the principles of **trust**, **impartiality**, and **protection**. The system should be adapted to the size, nature, complexity, and jurisdiction of the organizations' activities. The objective of this procedure is not to replace legal avenues for resolving legal disputes.

This Policy has been created to ensure that TRI MARINE (TMI) can respond immediately to any report they receive regarding potential wrongdoing or infringements of the BOLTON GROUP high policies (i.e., the Code of Conduct and the Human Rights Policy). It is defined as the company's means of implementing its whistleblowing channel (the "*Communication & Ethical Channel*", CEC) in a manner adapted to the legislation currently in force, and it is designed to reflect the best practices in the market, and to establish a policy that can comply with the highest international standards currently applicable, or which are expected to become applicable soon.

For reporting channels of this type, it is an essential requirement that they **must be operated in a professional and confidential manner**.

Following ISO 37.002-2021, we define "Whistleblowing" as "the act of reporting suspected wrongdoing or risk of wrongdoing". "Wrongdoing" is defined as "an action(s) or omission(s) that can cause harm. This concept can include, but it is not limited to, the following:

- Breach of law (national or international), such as fraud, corruption including bribery.
- Breach of the organizations or other relevant code of conduct, policies, etc.
- Gross negligence, bullying, harassment, discrimination, unauthorized use of funds or resources, abuse of authority, conflict of interest, gross waste, or mismanagement.
- Actions or omissions resulting in damage or risk of harm to human rights, the environment, public health and safety, safe work-practices, or the public interest."

All of these channels can be used to report suspected or actual wrongdoing, with all whistleblowers being assured that the information they report will reach the appropriate personnel designated by TMI for managing these types of issues, with no need for them to be concerned about retaliation. In summary, the fundamental intention is to give the people included in this Policy's scope the ability to report any possible non-compliances or concerns, all within the framework defined in this Policy on Operation of the CEC.

2.2 Regulatory and legislative context

US Foreign Corrupt Practice Act (1977): "Companies should have in place an efficient, reliable, and properly funded process for investigating the allegation and documenting the company's response, including any disciplinary or remediation measures taken."[1]

U.S. DOJ[2]: "Confidential reporting mechanisms are highly probative of whether a company has "established corporate governance mechanisms that can effectively detect and prevent misconduct." JM 9-28.800; see also U.S.S.G. § 8B2.1(b)(5)(C) (an effectively working compliance program will have in place, and have publicized, "a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation")."

ISO 37001: "Each organization that sets up a whistleblowing system should have a Whistleblowing Management Function, a specific role, even if it is not a dedicated position, with responsibilities for the administration of the whistleblowing system."[3]

An important reference source on this subject includes the legislation about data protection and about protection for whistle-blowers, especially in view of the protection granted under the European Union Directive (EU) 1937/2019 of 23 October 2019, on the protection of persons who report breaches of Union law. The purpose of that Directive is to ensure that whistle-blowers can report, both internally and to public authorities, any infringement of European Union law they become aware of at an organization, by using channels that guarantee their security and allow them to perform such reporting without fear of retaliation by the company.

This Policy complies with the ISO 37001 standard on Anti-Bribery Management Systems, where special reference is made to the process that must be followed when investigating a report, and which also emphasizes the need to develop internal report management processes that guarantee:

- The effectiveness of the actions performed.
- The authority of the persons in charge of the investigation.
- The required involvement and cooperation of other departments.
- Confidentiality for all reports, investigations, and resolution procedures.

[1] *A Resource Guide to the US Foreign Corrupt Practices Act. Second Edition, 2020.*
[2] *U.S. Department of Justice. Evaluation of Corporate Compliance Programs – Guidance Document. Updated: April 2019.*
[3] *ISO 37001, Anti-bribery Management Systems – Requirements.*

The ISO 37301, Standard on Compliance Management Systems, also establishes the need to maintain reporting channels. Specifically, in its section related to reporting concerns, it states: "Even in cases where there are no requirements imposed by local regulations, organizations should consider developing a reporting mechanism that allows anonymity or confidentiality, and which the organization's employees and agents can use to report or seek guidance on Compliance breaches, without fear of retaliation". That standard also makes specific reference to the requirements and recommendations on reporting channels found in the ISO 37002, Whistleblowing Management Systems – Guidelines, which its 2021 version has been used as a basis for developing this, Policy.

For these reasons, and in compliance with the contents of that Directive, TMI has produced this Policy on Operation of the Ethical Channel. Its purpose is to specifically establish the scope and contents of the reporting process and procedures, and to effectively implement both ordinary and alternative internal reporting channels. also, Policy is also specifically subject to implementation through **TMI's Procedure on Investigation of Reported Wrongdoing**, which has been approved by TMI's CEO.

Therefore, in direct relation with said implementing Procedure, this Policy establishes the following specific requirements:

- **It must be possible for reporting to take place both verbally and in writing**, as well as by telephone and/or other electronic means, and also in person if the whistleblower prefers.
- **An acknowledgement of receipt** for the report must be produced within a maximum period of 5 working days.
- **The Whistleblowing Management function must be able to appoint an *ad hoc* Investigation Team**, to remain active until the case has been resolved, along with the appointment of a **Case Manager** who will have the authority to process the report, and to communicate with the whistleblowers in order to request any additional information and respond to the whistle-blowers' concerns.
- **All reports** (including anonymous reports) **must be addressed in a diligent manner**.
- **A general period of 3 months** must be established for giving the whistle-blowers a response regarding the status of the process, counted from the date the acknowledgement of receipt is produced. If, exceptionally, more time is required to close the investigation, the Case Manager shall notify the parties concerned in writing of this circumstance.

Following the requirements of the most relevant legislation on protection necessary, personal data and digital rights in countries such as, but not limited to, Italy, Spain and USA, communications and reports can be **anonymous**; it is recognized the duty to inform employees and third parties about the existence of these reporting systems and it is clearly established that access to information within the system must be restricted to persons with internal control and compliance duties (who may or may not be employed by the company), or to designated data processors (however, access by other persons or disclosure of information to third parties or public authorities may be permissible if required in order to apply disciplinary measures or if necessary in relation to judicial proceedings). It is also notable that **the identities and personal data of the persons**

involved must remain confidential, especially any information regarding the whistleblowers in cases where the report has not been performed anonymously [4] .

3. Terms and Definitions:

Retaliation	"Retaliation" and "retaliatory action" may take different forms but is defined by the International Labor Organization as: "any direct or indirect detrimental action that adversely affects the employment or working conditions of an employee, where such action has been threatened or taken for the purpose of punishing, intimidating or injuring an individual because that individual engaged in a protected activity." For the purposes of this document, the protected activity is reporting a complaint or grievance.
Independent Investigation	Independent investigation signifies that the investigator(s) are neither the subject of the complaint nor compromised in their impartiality by the reporting structure of the operation or undue influence of the employer.
	The definitions below are criteria for the effectiveness of a grievance mechanism[5].
Legitimate	Enabling trust (i.e., feel safe and free from potential retaliation) from the stakeholder groups for whose use they are intended, and being accountable for the fair conduct of grievance processes.
Accessible	Being known and understood (i.e., how to use) to all stakeholder groups for whose use they are intended and providing adequate assistance for those who may face particular barriers to access.
Equitable	Seeking to ensure that aggrieved parties have reasonable access to sources of information, advice, and expertise necessary to engage in a grievance process on fair, informed and respectful terms. This is one of the roles of the Independent Third Party.
Transparent	Keeping parties to a grievance informed about its progress and providing sufficient information about the mechanism's performance to build confidence in its effectiveness.

[4] *However, confidentiality should not prevent the wrongdoing form being fairly and independently investigated.*
[5] *Based on the Seafood Task Force Auditable Standards and UNGP Principle 31*

Abbreviations:

STF	Seafood Task Force
UNGP	United Nations Guiding Principle

4. Responsibility and Authority

4.1 Responsibility and Authority

This Whistleblower Management Policy has been adopted to reinforce that TMI provides a safe and confidential environment where concerns regarding misconduct, impropriety or wrongdoing may be raised without fear of reprisal or detrimental treatment.
This Policy sets out:

a) **When** you will be protected for speaking up about misconduct.
b) The **protections** that may be provided to you if you speak up.
c) **How** disclosures made under this Policy will be handled by TMI.

This Policy is made available on the Resources section of the website of TMI (www.trimarinegroup.com) and in the external Grievance reporting platform www.trimarinegroup.ethicspoint.com.

This Policy also protects those who are entitled to protection under the European or US Whistleblower laws.

The purpose of this Policy is to provide advice and certainty in respect to the decisions a person should make after becoming aware of any possible wrongdoing. The intention of TMI is to firmly establish a principle that is consistent with the sources of law summarized in the previous section: **At TRI MARINE, any retaliation against a whistleblower is prohibited**.[6]

In order to implement this principle, decisions must be made on the following fundamental aspects:

1. Subjective scope of application: Who does this Policy apply to?
2. Objective scope of reports: What can I report? When should I make a report?
3. Using the channel: How do I use the Ethical Channel?
4. Consequences of reporting: What happens when I make a report using the Ethical Channel?
5. At TMI, the Policy on Operation of the Ethical Channel is a universal policy. In other words, it is always applicable at Tri Marine, unless there is some legal justification that creates an exception to its applicability.

[6] *In conformity with Recital 37 of Directive (EU) 1937/2019 on the protection of whistleblowers.*

4.2 Subjective scope of application: Who does this Policy apply to?

This Policy is binding for any person who wants to report a possible non-compliance, infringement, breach, or wrongdoing within a professional context involving TMI's activities or supply chain. This Policy is binding for all directors, executives, and employees associated with companies from the Group, regardless of the legal nature of their relationship ("*persons affected*").

It is also binding for all other persons who become aware of non-compliance or breach during their professional relationship with Tri Marine, even if they are not employed by any of the companies from the Group. It is also binding for all stakeholders involved with TMI, and regarding Contacts and Relations with Shareholders and other Stakeholders.

5. Details of the Policy

5.1 Objective scope of reports: What can I report? When should I make a report?

5.1.1 What can I report by applying this Policy on Operation of the Ethical Channel?

This Policy encourages reporting of any concerns a person has regarding possible non-compliances, infringements, or wrongdoing in relation to applicable legislation or to the Tri Marine Code of Conduct and other high-level Policies such as the Tri Marine Human Rights Policy, in conformity with the scope of reporting defined in Directive (EU) 1937/2019. This means the reporting of breaches in the broadest possible sense, including but not limited to reasonable suspicions, actual or potential breaches, those that have occurred, are occurring and those that seem very likely to occur.[7]

In relation to this, we must emphasize the following potential reasons for reporting:

- To report a situation that could represent a non-compliance on the subject of prevention of money laundering and financing of terrorism.
- To prevent bribery and corruption.
- To improve health and safety in the workplace.
- To prevent conflicts of interest in relation to any type of professional activities.
- To prevent discrimination, as well as sexual and non-sexual harassment.
- To prevent internal fraud.
- To protect fair competition and the rules of international trade.
- To ensure responsible use of the company's assets.
- to safeguard the integrity of the company's taxation procedures, business affairs, and financial records.
- To create a more inclusive and respectful workplace.

[7] *In conformity with Article 5 of Directive (EU) 1937/2019 on the protection of whistleblowers.*

- To protect TMI's sensitive information, disclosure could harm the interests of the companies or the rights of third parties protected by law.
- To protect TMI from hacking or cyber-attacks.
- To allow compliance with the laws and regulations on urban planning and zoning.
- To protect human rights.
- To protect compliance with laws and customary practices globally and locally, with relationships with public-sector authorities being restricted to the professional environment.
- Any other potential reasons.

5.1.2 When should I make a report?

At Tri Marine, we believe that the best way to encourage reporting is to start by generating an environment where people feel comfortable sharing any information that could represent a wrongdoing. Therefore, the company promotes development of a workplace where circumstances involving possible wrongdoing can be openly discussed.

This must be done in line with a principle that applies to all relationships between TMI and their stakeholders: Reporting or whistleblowing must always take place in good faith[8], which is equivalent to the implementation of what is referred to in Directive (EU) 1937/2019 as a "*just culture*". This means that when reporting occurs, the whistleblower must have reasonable grounds for believing that the information being reported is accurate and involves potential non-compliance, breach, infringement, or other wrongdoing.

A "*just culture*" or "*speak-up/listen-to culture*" means to provide a trustworthy two-way environment where any relevant party is sufficiently confident and encouraged to raise concerns about wrongdoing or suspected wrongdoing, and the organization demonstrates its commitment to receiving, assessing, addressing, and concluding whistleblowing cases.

5.1.3 What if it is an urgent matter?

It is clear that in order to process the reports received through the various channels offered, the body responsible for receiving said reports (which are the EthicsPoint System Administrators) must perform their own internal classification, based on the contents of the reports, i.e., a first TRIAGE.

The "*triage*" must be understood as an assessment of the initial report of wrongdoing for the purposes of categorization, taking preliminary measures, prioritization, and assignment for further handling.

This classification will allow reports to be processed in an appropriate manner. The way in which reporting is classified for that purpose is detailed in the TMI's Procedure on Investigation of Reported Wrongdoing.

[8] *In conformity with Recital 32 of Directive (EU) 1937/2019 on the protection of whistle-blowers.*

What is required in all cases is the assurance that the information reported will reach as soon as possible the appropriate hierarchical level endowed with sufficient independence and authority to carry out any investigation and take appropriate action. This will allow each issue to be addressed in the most effective manner in view of the facts and events reported, in accordance with the applicable laws and regulations, and in conformity with the TMI's Procedure on Investigation of Reported Wrongdoing.

5.2 Using the channel: How do I use the TMI Ethical Channel? Can reports be anonymous?

5.2.1 Steps to follow when making a report.

Any type of report covered by this Policy can be performed using one of the channels detailed below:

a) **Ordinary** Channels: TMI encourage the use of open and direct ordinary ways of reporting wrongdoing such as:

1. Reporting to the whistleblower's direct supervisor or a member of management.
2. Reporting to a member of Human Resources function.
3. Reporting to a senior manager.

When employees have confidence, they can make an "open-door" report directly to their manager (rather than keeping it anonymous), it is a sign of a healthy organizational culture. While the companies would like to promote direct reporting to managerial or human resources staff, it should also be understandable that there may be people who do not feel comfortable using these hierarchical channels for whatever reason, from possible conflicts of interest of the recipient of the communication to distrust that the information is treated with due seriousness.

b) **Alternative** Channels: While some people feel comfortable coming forward through an open-door policy, others may not. Some employees are hesitant to reveal their identities – or to report at all – because they fear retaliation or because they assume no one will take action. TMI offers a range of reporting options including:

1. Phone "Hotline"[9];
2. Web-based systems such as NAVEX Ethicspoint Global Website.
3. Mobile app.
4. Face-to-face disclosures.
5. Direct input: in person, including suggestion/complaint boxes[10].

[9] *Available at locations where technologically possible and/or if the site has over 50 employees.*
[10] *As required by the local legislation in the countries in which TMI operates.*

which are able to guarantee confidentiality, or anonymousness when chosen by the whistleblower, constitute the best way to overcome the fear of reporting which some people could feel.

Any person may, in any case, report directly to the competent local, national, or international authorities and/or through any official reporting mechanism to which they have access. TMI will provide contact information for the police, immigration authorities and embassies of employee's and crew member's countries of origin.

5.2.2 What information do I need to provide when using the channel?

TMI would like the information they receive to be as complete and accurate as possible. Therefore, they ask all whistleblowers to share all information they are aware of regarding potential infringements and wrongdoing in the most detailed manner possible. It is also preferable to provide, or clearly refer to, any supporting evidence or documents for the report. This will allow the channel management team to address the case as quickly and effectively as possible.

The management system in place shall ensure that the sender of any communication can receive periodic updates on the status of the grievance or complaint and appropriate feedback as required.

5.2.3 Identification of the whistleblower: anonymity

TMI's Ethical Channel "EthicsPoint" **allows anonymous reporting**.

However, the company encourages all whistleblowers to identify themselves by providing their name, position, and contact information. This will allow the persons handling the case to directly contact the whistleblower to perform any necessary follow-ups. TMI also believes that this is the best way to confirm compliance with its policy of non-retaliation against whistleblowers.

In relation to this, it must be remembered that when (non-anonymous) reports occur, the whistleblowing management team ensures that the entire internal reporting procedure takes place in a secure manner, with confidentiality guaranteed for whistleblowers' identity and any other related information.

5.2.4 What happens when I make a report using the TMI alternative reporting channels?

The general steps of the management process are the following:

1. **Receiving reports of wrongdoing**: the management system specifies how reports can be made and received from all potential users within the scope of the system (see Sec. 2.1).

   In line with the requirements from EU Directive 1937/2019 and US FCPA, TMI uses an **online platform,** NAVEX EthicsPoint, with a centralized database to support use of the alternative channels it offers. Managers and supervisors will also communicate to the management

function any report received through any ordinary channel. These reports will go through the same general management procedure (assessment – addressment – case closing) as the reports received through the alternative channels.

Any reporting that takes place through those alternative reporting channels is stored directly on the platform, which must have robust information security measures implemented, designed to preserve the integrity, availability, and confidentiality of the information. Records of all communications will be maintained for at least three (3) years, and indefinitely in the event that they may be used in legal proceedings at a later date.

The platform allows the reporting person to specify the place, date, and company or function involved, and to identify the people related to report. The platform also offers an **anonymous reporting option**. In addition, it has a feature that allows the whistleblower to attach supporting documentation for the information being reported.

Since it was decided to outsource to an external grievance/whistleblowing provider, both TMI commit themselves to exert sufficient due diligence to ensure the highest available data protection standards are applicable by default and by design.

TMI shall ensure that all members of their organizations have easy access to one of the reporting options implemented. Special attention will be given to those people who, due to their own work, such as fishing vessels' crews, have more limited options to access the service. TMI will ensure that such people have access to one of the reporting channels at least once every 24 hours.

2. **Assessing reports of wrongdoing** (*triage*): the management system specifies the process of assessing received reports, including aspects such as priority, completeness, and relevance of information.

   TMI commits to identify, implement, and maintain process(es) that ensure(s) the impartial assessment, triage, and management of the reports of wrongdoing. Reports will be sorted and prioritized on risk (i.e., the likelihood of wrongdoing and its potential impact). Assessment of received reports shall be performed within ten (10) working days of a communication being submitted. The process is detailed in the TMI's Procedure on Investigation of Reported Wrongdoing.

   The team in charge of evaluating the report received must have the appropriate training and experience for this function. It shall have legal advice to enable the early detection of potentially criminal cases, so that a decision can be made at the appropriate procedural stage on the need to escalate the investigation, refer it to specialized external investigators and/or refer it to law enforcement or regulatory authorities.

   Obviously, the categorization of the wrongdoing can be re-evaluated at any stage of the process, which may require escalation of the procedure to maintain all legal safeguards and integrity of evidence throughout the investigation.

   If a communication is rejected for being out of the scope or for being manifestly not credible,

the sender shall be notified of rejection reason and in written where applicable and afforded with the opportunity to provide additional information and to ask for the revised communication to be assessed again.

3. **Addressing reports of wrongdoing**: the management system will provide for an impartial and timely investigation, as well as effective and timely protective and support measures and monitoring as appropriate for the whistleblower and others involved, including who are subject of the report.

   The Whistleblowing Management Function shall identify, implement, and communicate a process that ensures investigations are conducted impartially by suitably qualified personnel. They should be fair and impartial to the business unit concerned, the whistleblower and the subject(s) of the report. Due process shall be observed in any investigation arising out of a whistleblowing report.
   A multi-disciplinary approach will be taken when required. Professional investigation management includes but is not limited to the following principles:

   - Investigations should be adequately resourced.
   - Clear terms of reference and scope should be defined and documented;
   - The investigation process should be robust enough to withstand administrative, operational, and legal review. An audit trail should be maintained relating investigation activities back to approved plans. The investigation should consider any subject of a report as being presumed innocent.
   - The investigation should not directly or indirectly interfere with a judicial investigation, it should cooperate where appropriate or required.
   - The investigation should secure and protect evidence.
   - Personal data should be managed in line with the highest data protection requirements.
   - The investigation should protect any information that could identify any subject of a report.
   - All investigations should be able to scale and adapt as the circumstances can change as the investigation progresses.
   - Communication should be clear and unambiguous, balancing the interests of organizations and the whistleblower.
   - Organizations should communicate regularly, including at material progress steps, in the form of feedback to the whistleblower.

   TMI will attempt to the best of their ability to have the investigation of any reported wrongdoing conducted by appropriate personnel who are familiar with the local realities of the area affected by the incident. The specific procedure is described in the TMI's Procedure on Investigation of Reported Wrongdoing.

4. **Concluding whistleblowing cases**: the management system will provide a mechanism to close investigations and act in response to recommendations and decisions based on the outcomes of the addressing step. It must also ensure that protective and support measures

can continue and will be monitored as appropriate. Outcomes may be used for management reporting, organizational learning, and other activities (i.e., mitigation remedies).

A whistleblowing case will move into the concluding phase where no action is considered necessary in response of a report, where fact-finding determines no further investigation is warranted, where the report is referred to another process to be dealt with, or at the end of any investigation (whether or not wrongdoing is found).

Concluding a case can involve acting in response to any recommendation (e.g., policy review, disciplinary actions) to identifying lessons learnt (e.g., additional controls to improve policy, procedures, or practices).

Where wrongdoing is found, TMI will:

- Take the appropriate measures to resolve the wrongdoing and to continuously monitor the effectiveness of those measures, in accordance with the appropriate corporate policies.
- Administer appropriate sanctions.
- Refer matters to the relevant authorities where appropriate and monitor the results or decisions made.

The actions planned and taken, and any findings will be communicated in a timely manner to the whistleblower and relevant interested parties. This includes any independent avenues available to review the handling of the case.

Where there are legal restrictions on what can be communicated about the actions and findings (e.g., when the wrongdoing constitutes a criminal offence), the whistleblower should be notified of the reasons, where possible, for the limited communication.

The possibility that it may be necessary to reopen a case cannot be excluded. If either one of the parties feels that the resolution process failed to meet the requirements established in this Policy (i.e., impartiality, confidentiality, timelines, investigation, and assessment process), or if they wish to contest the specifics of the proposed corrective actions, the party can submit an appeal to the Case Manager.

The appeal shall be reviewed and assessed with impartially by a third party who has not previously been involved in the case. It may be decided that an independent competent and qualified individual, group of individuals or organisation maybe assigned with the task to review the appeal.
Decision and recommendation made following such appeal review process are final and the complaint or grievance shall be closed unless the appeal assessor concludes that the complaint or grievance has not been adequately dealt with and shall be re-opened.

The Parties maintain their right to escalate the complaint or grievance and follow relevant legal proceeding at any time during this process.

The specific procedure in place to conclude whistleblowing cases is described in the TMI's Procedure on Investigation of Reported Wrongdoing.

5.2.5 Addressing detrimental conduct: prohibition of retaliation.

TMI considers that it is advisable to go beyond the simple prohibition of retaliation and that protection and practical support shall be afforded to the whistleblower. TMI presumes that whistleblowers act responsibly and in good faith unless otherwise demonstrated.

From the whistleblower's perspective, good faith means only reporting concerns when there are reasonable grounds to support the belief that the information being reported about a potential wrongdoing is accurate at the time of the report. At the same time, responsibly because TMI wishes to make it clear that the reporting of any wrongdoing knowing it to be false constitutes a serious misconduct that will be severely sanctioned.

This Policy makes clear that seeking to identify the whistleblower or detrimental conduct in connection with a whistleblower report is not tolerated and can potentially carry a disciplinary sanction appropriate to the high severity of the facts.

Top Management of TMI is accountable for ensuring support and protection. The Whistleblowing Management Function is responsible for ensuring that support and protection measures are implemented throughout all TMI organizations.

Detrimental conduct is defined[11] as: "*threatened, proposed or actual, direct or indirect act or omission that can result in harm to a whistleblower or other relevant interested party, related to whistleblowing*". Harm includes any adverse consequence, whether work-related or personal, including, but not limited to, dismissal, suspension, demotion, transfer, change in duties, alteration of working conditions, adverse performance ratings, disciplinary proceedings, reduced opportunities for advancement, denial of services, blacklisting, boycotting, damage of reputation, disclosing the whistleblower's identity, financial loss, prosecution or legal action, harassment, isolation, imposition of any form of physical or psychological harm.

Detrimental conduct includes retaliation, reprisal, retribution, deliberate actions, or omissions done knowingly or recklessly to cause harm to a whistleblower or other relevant parties.
Detrimental conduct also includes the failure to prevent or to minimize harm by fulfilling a reasonable standard of care at any step of the whistleblowing process.

Action to deal with whistleblower's own wrongdoing, performance, or management, unrelated to their role in whistleblowing, is not detrimental conduct.

If any person from TMI infringes this Policy by performing some direct or indirect act detrimental conduct, the company must take responsibility for implementing the measures necessary to ensure that the detrimental conduct is ended as soon as possible, and when appropriate, it must apply disciplinary measures against those responsible.

[11] *ISO 37002:2021Whistleblowing Management Systems – Guidelines.*

Whistleblowers can report detrimental conduct via the channels already in place, both ordinary and alternative, as well as to the Whistleblowing Management Function personnel responsible for supporting and protecting them. To the greatest extent possible, the whistleblower should be restored to a situation that would have been theirs had they not suffered detriment.

6. Data protection and storage

6.1 Identity of the data controller.

The personal data of the whistleblower and other subject(s) of the report will be processed by the company that receives the report and which provides the whistleblowing management services to TMI.[12]

TMI is committed to strict protection of privacy and security and proper storage of that data, as detailed in their policies and procedures on the subject. These same standards must also be applied with respect to all other personal data associated with the report taking place in accordance with this Policy.

6.2 Storage of personal data.

The service provider maintains a register to record all the reports it receives. These records, and the personal data they contain, are maintained in a strictly confidential manner. In all cases, these records are stored for the entire time required to comply with the legal requirements applicable at any given time, but never for a time period longer than necessary.
Once the investigation has been completed for the report received, and any appropriate actions have been taken, the data taken from any report that has been investigated will be stored to comply with the legal obligations applicable to each case, but with access to that information appropriately blocked.

In all cases, personal data will be deleted from the CEC within a maximum time period of three (3) months after being entered, unless storage for an additional time period is necessary in order to comply with any legal obligations or with the company's need to maintain evidence regarding potential criminal offenses. If investigation of the report has not been completed within said time period, the data can be processed outside of the Ethical Channel for the period of time required to allow that investigation to be finalized.

In cases where a decision is made not to further investigate the report received, the information can be stored after being made anonymous.

6.3 What personal data does TMI collect?

[12] *Find detailed information in the TMI Procedure on Investigation of Reported Wrongdoing.*

When processing the report made in accordance with this Policy, the Whistleblowing Management Function collects the following types of personal data and information, both at the time when report occurs and during the subsequent investigation:

- The whistleblowers' name and contact information (unless the report is anonymous), and whether that person is an employee.
- The names and other personal data of the persons mentioned in the report (persons committing alleged wrongdoing, possible witnesses, and other subjects), if information about them is provided (i.e., a description of their positions and contact information, and the nature of their role or participation in the events being reported).
- Description of the alleged wrongdoing, as well as the circumstances surrounding the incident(s).

6.4 Why does TMI process personal data?

At all times, the only personal data processed is the data strictly necessary for purposes of managing, processing, and investigating the reporting received in relation to commission of irregularities or acts that are unethical, unlawful, or contrary to Tri Marine's corporate rules; for performing any acts necessary to investigate the facts and events reported; and for applying any appropriate disciplinary or legal measures.

No personal data will be used for any purpose other than those described.

6.5 What is the legal basis of the processing?

Relevant legal basis of processing personal data in the context of a whistleblowing management system are, among others:

- Article 6.1(e) of the European Union's General Data Protection Regulation (GDPR): processing for purposes of detecting and preventing claims and therefore any resulting harm and liability risks for the companies.
- U.S. DOJ[13]: "Prosecutors should assess whether the company's complaint-handling process includes pro-active measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers."

Processing personal data can also be based on compliance with a legal obligation or on satisfaction of the company's legitimate interest.

Therefore, processing the whistleblowers' personal data is strictly necessary in order to manage the report and comply with the purposes and legal obligations described above. In no case will TMI perform automated decision-making based on the data submitted.

[13] *U.S. Department of Justice. Evaluation of Corporate Compliance Programs – Guidance Document. Updated: April 2019.*

6.6 Who are the recipients of the personal data?

Personal data collected in the context of report taking place through the alternative reporting channels can be processed by, or disclosed to, the following parties when necessary:

- The service provision entity for the platform, which is responsible for day-to-day management of the alternative reporting channels.
- Members of TMI Whistleblowing Management Function.
- Authorized representatives of TMI, if the nature or scope of the reported events or concerns makes their participation necessary.
- External investigators, advisers, or consultants contracted to assist TMI in evaluating the report, investigating the matter, or advising TMI in relation to the matter.
- The police or any other regulatory or law enforcement authorities.

6.7 What data protection rights do whistleblowers have?

Whistleblowers can exercise their right to access their own personal data at any time, under the terms established in the applicable legislation. If the whistleblower believes that their data is inaccurate or incomplete, they can submit a request for rectification in accordance with the applicable legislation. They can also request erasure of their data if it is no longer necessary, except in cases where there is a legal obligation to store it. They can also request restriction of processing of their personal data or object to such a process, and they can request data portability. They also have the right to withdraw their consent to processing. At the time when they submit their report, they will be informed about how they can exercise all those rights.
If they believe it is appropriate, they can also submit a claim to the competent data protection authority.

7. Non-Compliance with this Policy

Any breach of this Policy by an officer, employee or contractor of Tri Marine will be taken seriously and may be the subject of a separate investigation and/or disciplinary action.

A breach of this Policy may amount to a civil or criminal contravention under the applicable whistleblower laws (any local applicable jurisdiction), giving rise to prosecution, fines, or other actions.

Tri Marine encourages all employees and other interested parties to raise any concerns about non-compliance with this Policy with a member of the Whistleblowing Management Team in the first instance. You may also raise any concerns through the channels described in this Policy or any official whistleblowing channel available.