Internal Information System Policy and Whistleblower Channel Management Procedure

Internal Audit, Risk and Compliance Department

May 2023

PROFAND
FISHING HOLDING

Table

–

1. Internal Information System Policy

The purpose of this Internal Information System policy and management procedure (hereinafter and jointly, the "**Policy**"), in compliance with the provisions of Law 2/2023, of 20 February, regulating the protection of individuals who report regulatory violations and the fight against corruption (hereinafter, "**Law 2/2023**"), is to encourage a culture of information and scrupulous compliance with regulations through the establishment of an internal channel that regulates the reception, processing and investigation of possible reports, as well as the protection of the informant.

This Policy shall apply to Profand Fishing Holding, S.L.U. (hereinafter "**PFH**") and all its subsidiaries under the terms of Article 42 of the Code of Commerce (hereinafter the "**Group**"), including the Spanish subsidiaries ("**Spanish Subsidiaries**") and foreign subsidiaries ("**Foreign Subsidiaries**").

The purpose of the Group's internal information channel ("**Internal Information Channel**") is to strengthen the information culture, understood as a mechanism to prevent and detect threats to the public interest, as well as to guarantee the protection of individuals who, in a work or professional context, report:

a) Acts or omissions that may constitute violations of European Union law, as provided for in Article 2 of Law 2/2023.

b) Actions or omissions that may constitute a serious or very serious criminal or administrative infringement of Spanish law. In any case, all serious or very serious criminal or administrative offenses that imply economic losses for the Tax Administration and for the Social Security will be understood to be included.

The Group has also established a Compliance Program, comprised of the Code of Ethics and Conduct, the Supplier Code, the Anti-Corruption and Money Laundering Policy, the Human Rights Policy, and the Criminal Risk Prevention Model. Any non-compliance with the provisions of the Compliance Program may also be reported through the Internal Information Channel.

In circumstances where there is any doubt as to whether this Policy applies to Foreign Subsidiaries, or whether there is a conflict with the applicable local laws, the compliance officers or managers of these Foreign Subsidiaries should seek guidance from corporate legal or internal audit teams before taking measures.

1.1. General provisions

The Group's internal reporting system ("**Internal Reporting System**") is the channel for reporting any action or omission provided for in sections i) and ii) above (hereinafter the "**Violation**" or "**Violations**") in a labor or professional context, without prejudice to the fact that it may also be used to report actions, facts, or circumstances that involve a breach of the provisions of the Compliance Program.

On the other hand, the Internal Information System is managed in a secure manner, so it guarantees: i) the confidentiality of the identity of the informant of the Violation (hereinafter the "**Informant**" or "**Whistleblower**") and of any third party mentioned in the communication, ii) the actions carried out in the management and processing thereof, iii) data protection, thus preventing access by unauthorized personnel, and iv) adequate protection against any retaliation that may be directed at the Informant(s).

In compliance with the provisions of Law 2/2023, it is mandatory that all communications be made through a single channel for the entire Group, the Internal Information Channel, which shall be governed by the provisions of this Policy.

1.2. General aspects that apply to the Internal Information Channel

1.2.1. Who can file a report through the Internal Information Channel?

The Internal Information Channel is aimed at Informants who, in a work or professional context, have evidence of, are aware of, or detect any Violation, including in any case:

a) Individuals who are employees or workers.

b) The self-employed.

c) Shareholders/partners, participants and individuals belonging to the administrative, management or supervisory bodies of any of the Group's companies, including non-executive members.

d) Any person working for or under the supervision and direction of contractors, subcontractors, or suppliers.

e) Persons whose employment or statutory relationship with the Group has ended, as well as volunteers, interns, trainees and employees undergoing training, regardless of whether or not they receive remuneration. This includes those whose employment relationship has not yet begun, in cases where information on violations has been obtained during the hiring or pre-contractual negotiation process.

1.2.2. What can be reported through the Internal Information Channel?

Any of the Violations described in i) and ii) of section 1 above. These include, but are not limited to, various types of violations, including serious and very serious criminal and administrative offenses, occupational health and safety offenses, tax matters, and matters relating to European Union law.

In addition, any non-compliance with the provisions of the Compliance Program may also be reported through the Internal Information Channel.

Excluded from this Policy are communications of a commercial nature or those that are intended to disclose:

a) Information contained in communications that have been rejected by any internal information channel or for any of the reasons set forth in article 18.2.a) of Law 2/2023.

b) Information related to claims about interpersonal conflicts or that affect only the Informant and the persons to whom the communication or report refers.

c) Information that is already fully available to the public or that constitutes just rumors.

d) Information concerning actions or omissions not covered by Article 2 of Law 2/2023.

1.2.3. What is the governance system for the Internal Information System?

The PFH Governing Body i) is ultimately responsible for the approval and implementation of the Internal Information System, and ii) has the authority to appoint the person in charge of the Internal Information System.

Responsibility for the Group's Internal Information System falls to a collegiate body called the Supervisory Body, comprised of 3 members.

In compliance with the provisions of Law 2/2023, the Supervisory Body shall delegate the powers to manage the Information System and to process the investigation files to one of its members (the "Manager").

In this respect, the Manager carries out their functions independently and autonomously from the rest of the PFH bodies, receives no instructions of any kind for performing them, and has all the human and material means necessary to carry them out.

1.2.4. Protection of personal data, preservation of the identity of the Informant and the persons concerned and prohibition of retaliation.

In the management of the Internal Information Channel, the legal regulations on personal data protection applicable to the different companies of the Group shall be complied with.

In particular, the following aspects will be taken into account:

- All companies must implement the personal data security measures that are applicable according to the risk level established for the Internal Information Channel or, as the case may be, the measures that are mandatory as per the applicable legal regulations and the internal Group regulations related to this aspect. The level of security shall be at least equivalent to that provided in the data protection compliance system for sensitive or special-category data, in accordance with the applicable data protection regulations.

- Proper compliance with the processing of personal data must be guaranteed, in particular with respect to the rights of the owners of such data to be informed about the processing thereof. All of this in accordance with the applicable legislation in each country.

- PFH guarantees to respect the absolute confidentiality of the Whistleblower's data and to ensure that there will be no retaliation. Any individual who must be informed of an incident or irregular conduct in order to properly deal with the matter in question will also be subject to a confidentiality agreement.

- Without prejudice to the foregoing, a Whistleblower’s information may be provided to the administrative or judicial authorities if so requested, always in compliance with personal data protection legislation.

1.2.4.1. Legal framework for the processing of personal data

The processing of personal data that stems from the communication of an Violation shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, that of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights, that of Organic Law 7/2021, of 26 May, on the protection of personal data processed for the purposes of the prevention, detection, investigation, and prosecution of criminal offenses and enforcement of criminal penalties, and that of heading VI of Law 2/2023.

In this regard, personal data will not be collected if it is not patently necessary for the processing of specific information. If it is collected by accident, it will be deleted without undue delay.

1.2.4.2. Information on personal data protection

Whistleblowers will be expressly informed that their identity will in all cases be kept confidential and that it will not be communicated to the persons to whom the report refers or to third parties.

1.2.4.3. Processing of personal data in the Internal Information System

Access to the personal data contained in the Internal Information System shall be limited, within the scope of their competencies and functions, exclusively to:

a) The Manager and whoever directly supervises them.

b) The person in charge of Human Resources or the duly designated competent body, only when disciplinary measures may be taken against an employee.

c) The person in charge of PFH's Legal Department, should legal action need to be taken in relation to the facts/events described in the communication.

d) The persons in charge of the processing that eventually may be appointed.

e) The data protection officer.

1.2.4.4. Preservation of the identity of the Informant and of the persons affected

The Informant may decide whether to make the communication anonymously or non-anonymously; in the latter case, the Informant's identity will be kept confidential, it will not be

disclosed to third parties. Consequently, the Internal Information System will not obtain data that allows for the identification of the Informant and has adequate technical and organizational measures in place to preserve and guarantee the identity and confidentiality of the data corresponding to the persons concerned and any third party mentioned in the information provided.

Notwithstanding the foregoing, the identity of the Informant may solely be communicated to the legal authorities, the Public Prosecutor's Office, or the competent administrative authority in the context of a criminal, disciplinary, or sanctioning investigation.

1.2.4.5. Prohibition of retaliation

In compliance with the provisions of Law 2/2023, any acts constituting retaliation, including threats of retaliation and attempted retaliation against Informants, are expressly prohibited.

Retaliation means any acts or omissions that are prohibited by law, or that, directly or indirectly, involve unfavorable treatment that places the person(s) receiving them at a particular disadvantage with respect to others in the work or professional context, solely due to their status as Informants or because they have released a public disclosure.

Retaliation includes, but is not limited to, the following: i) suspension of the employment contract, dismissal or termination of the employment or statutory relationship, including non-renewal or early termination of a temporary employment contract, ii) a negative evaluation or references regarding work or professional performance, iii) denial of training, and iv) discrimination, or unfavorable or unfair treatment.

The whistleblower protection measures provided for in Law 2/2023 shall also apply, where appropriate, to:

a) The legal representatives of the workers in the exercise of their functions of advising and supporting the Informant.

b) The natural persons who, within the framework of the organization in which the Informant provides services, assist the Informant in the process.

c) Natural persons who are associated with the Informant and who may suffer retaliation, such as coworkers or relatives of the Informant.

d) Legal entities, for which they work or with which they maintain any other type of relationship in an employment context or in which they have a significant shareholding.

2. Communications management procedure

2.1. Recepción de las comunicaciones

The Internal Information Channel allows communications to be carried out as follows:

a) Anonymously; in any case, the identity of the Informant will be safeguarded.

b) They may be made i) in writing, by mail or by any electronic means provided for this purpose, or ii) verbally, by telephone, or by voice messaging system.

Communications in writing may be addressed to:

- Web: https://grupoprofand.com/en/compliance-en/

- Address:

  C/ García Barbón, 62, Bloque 1
  36201, Vigo

  The communication should expressly state Attn: The Manager of the Internal Information System

Verbal communications may be made:

- By telephone or through voice messaging system to the telephone number: +34 986 44 73 84.

- At the informant's request, it may also be presented by means of a face-to-face meeting, which shall be held within a maximum period of seven (7) days of the request.

2.2. Procedure for managing communications, follow-up and presentation of the resolution

The procedure for the communication and how it is to be conducted until its resolution will be as follows:

Step 1: **Notification**

Using any of the means provided for above, the following must be reported: i) any Violation, or ii) in case there is evidence or suspicion of any non-compliance related to irregularities of a financial and/or accounting nature, facts or conduct contrary to the Law, the Code of Conduct and Suppliers, the Anti-Corruption and Money Laundering Policy and the PFH Criminal Risk Assessment program, and/or the Group's internal corporate regulations or procedures.

Step 2: **Minimum requirements for presenting a communication**

The communication shall contain, at minimum, the following information:

- The identity of the Informant, unless the communication is made anonymously.
- The Informant may indicate an address, e-mail or safe place to receive notifications.
- Description of the fact/event that is the object of the Violation, detailing, as far as possible, all the facts or circumstances that have given rise to said Violation.
- If possible, documents or evidence of the facts and/or events constituting the Violation shall be provided.
- In the event that the communication is made verbally, it must be documented in one of the following ways, with the Informant's consent:

    a) By a recording of the conversation in a secure, long-lasting, and accessible format.

    b) With a complete and exact transcription of the conversation, made by the staff responsible for handling it.

Without prejudice to the Informant's rights under data protection regulations, the Informant will be given the opportunity to verify, correct, and agree to the transcription of the conversation with their signature.

Step 3: **Registration and admission for processing**

The communication will be entered into a record book called the register of information (the "**Register**") and an identification code will be assigned to it. In the Register, the communications received and the internal investigations which they have yielded shall be recorded, guaranteeing confidentiality in all cases. This register shall not be public and only at the reasoned request of the competent legal authority, by means of an order, and within the framework of a judicial proceeding and under the guardianship of said authority, may total or partial access be granted to the contents of this Register.

Once the communication is received, the Informant shall be sent an acknowledgment of receipt of the communication within seven (7) calendar days of it being received, unless this could jeopardize the confidentiality of the communication.

The communication may be inadmissible if it is considered that:

a) The facts/events lack any credibility.

b) The facts/events reported do not constitute an infraction.

In cases where the communication is considered inadmissible, the Informant will receive notification of such inadmissibility within a maximum period of three (3) months.

Step 4: **Investigation activities**

The Manager will have all the human and material resources needed to carry out the investigation, guaranteeing at all times the protection of the Informant and the confidentiality obligations as provided for in Law 2/2023.

Step 5: **Classification of communication**.

The communication will be classified in order to establish priorities, as per the criteria of categorization, into minor, serious, very serious, or inadequate, in those cases in which the minimum requirements for processing specified in Step 2 are not met.

In the event that the Manager considers that the events/facts may be indicative of a crime, they shall immediately forward the information to the Public Prosecutor's Office. If the events/facts

affect the financial interests of the European Union, it will be referred to the European Public Prosecutor's Office.

Step 6: **Execution of the investigation of the communication**

Within the framework of the investigation, the Manager may establish communication with the Informant and, if deemed necessary, request additional information from them.

The persons affected by the communications have the right to be informed of the actions or omissions attributed to them, and to be heard at any time. Such communication shall take place at the time and in the manner deemed appropriate to ensure the proper conduct of the investigation. Likewise, in no case will the identity of the Informant be communicated to the affected subjects.

At all times, the presumption of innocence and respect for the honor of all persons concerned shall be guaranteed.

The maximum term to respond to the investigation proceedings may not exceed three (3) months from the receipt of the communication or, if no acknowledgment of receipt was sent to the Informant, three (3) months from the expiration of the seven (7) day term after the communication was made, except in cases of special complexity that require an extension of the term, in which case, this may be extended up to a maximum of three (3) additional months.

Step 7: **Resolution of the claim**

Once the investigation proceedings have been completed, the Manager shall issue a report containing at minimum:

a) A statement of the facts or events, reported together with the identification code of the communication and the date of registration.

b) The classification of the communication for the purpose of knowing its level of priority or lack thereof in its processing.

c) The actions carried out in order to verify the truthfulness of the facts.

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

External information channels

The Informant's right to choose the channel they consider most appropriate is recognized. They shall be able to resort to both the Internal Information Channel and the external information channels before the competent authorities, meaning the Informant may also resort to the Autoridad Independiente de Protección del Informante [Independent Authority for Whistleblower Protection] (the "A.A.I."), to the corresponding regional authorities or bodies or to the institutions, bodies, or agencies of the European Union, to report the commission of any Violation, either directly or following communication through the Internal Information Channel.

3. Supervision program

PFH's Supervisory Body will review this Policy annually to verify that it is updated and conforms to the legislation in force at any given time.

PROFAND
FISHING HOLDING