GRIMALDI GROUP

Procedure for handling whistleblowing reports

PURSUANT TO LEGISLATIVE DECREE 24/2023

GRIMALDI GROUP S.P.A.

GRIMALDI DEEP SEA S.p.A.

GRIMALDI EUROMED S.p.A.

TABLE OF CONTENTS

1. Introduction

1.1. Objectives of the document

This procedure (the "**Procedure**") regulates the system that the Grimaldi Group Companies**(Grimaldi Group S.p.A, Grimaldi Euromed S.p.A, Grimaldi Deep Sea S.p.A** (hereinafter the Company) have adopted to allow the internal reporting of violations of national or European Union regulations, detrimental to the public interest or to the integrity of the company, of which the *whistleblowers*have become aware in the context of their work (so-called *whistleblowing*).

The Procedure defines in particular:

- those who can activate the internal system for reporting violations;
- conduct, acts or omissions that can be reported;
- the modalities through which alleged violations can be reported and the persons in charge of receiving the reports;
- the process of handling alerts, with an indication of the timing and stages of the procedure and the persons involved in it;
- the ways in which the reporting subject and the reported subject are informed of developments in the proceedings;
- measures to ensure confidentiality and to protect against retaliatory conduct as a result of the report.

Finally, the Procedure provides information on external reporting and public disclosure, the further channels available to whistleblowers. The new rules of the Whistleblowing Decree (as defined *below*), however, provide that the choice of reporting channel is not left to the discretion of the *whistleblower*, since the internal channel is to be used as a matter of priority, and only if the conditions listed therein are met is it possible to use the other reporting channels.

1.2. Approval and revision of the Procedure

This Procedure, for the drafting/revision of which the company structures concerned were involved in order to ensure a clear definition and sharing of objectives, roles and responsibilities, is approved, following the information provided to the company trade union representatives pursuant to Article 51 of Legislative Decree No. 81 of 2015, by resolution of the Board of Directors. The Company also carried out a Prior Impact Assessment of the reporting management platform pursuant to Art. 35 GDPR in accordance with Art. 13, paragraph 6 of Legislative Decree no. 24/2023, which can be consulted upon request to the Data Protection Officer.

The Company, having adopted the organisational, management and control model (the '**MOG**') provided for in Legislative DecreeNo. 58/1998, has decided to adopt the ' **MOG**'. 8 June 2001, no. 231 (the '**Decree 231/01**') refers to this Procedure within the framework of the MOG, pursuant to the provisions of Article 6, paragraph 2 *bis* of Decree 231/01, as amended by Legislative Decree no. 10 March 2023, no. 24.

The Procedure will be reviewed and - if necessary - amended, whenever regulatory update requirements, interventions by the Supervisory Authorities, *business* strategies or changes in the context (significant changes in business processes, significant structural reorganisations, significant changes in the IT platforms used, changes in the scope of application) so require.

The Procedure is communicated and made available by the Company to all personnel as well as to other interested parties by means of appropriate communication channels, as better specified in the following section. 10.

2. Context of reference

2.1. Normative references

This Procedure has been drawn up in accordance with the relevant regulations below:

Community legislation:

- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law;
- Reg. (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.

National legislation:

- Legislative Decree 10 March 2023, No. 24 'Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws' (the ' ***Whistleblowing*** **Decree**');
- Legislative Decree 8 June 2001 no. 231 'Regulations on the administrative liability of legal persons, companies and associations, including those without legal personality', as amended by the *Whistleblowing* Decree;
- Legislative Decree 30 June 2003, no. 196 'Personal Data Protection Code', as amended and supplemented;

2.2. Definitions and terminology

In addition, the following terminology is used in alphabetical order:

Other subjects deserving protection	Other persons connected to the whistleblower who may be subject to retaliation within the work context, such as (i) the facilitator (defined below); (ii) work colleagues who have a habitual or recurrent relationship with the person; (iii) persons in the same work context who are linked to the whistleblower by a stable emotional or family relationship up to the fourth degree; (iv) the entities for which the whistleblower works as well as entities operating in the same work context as the whistleblower.
AOG	Reporting Officers
ANAC	National Anti-Corruption Authority.
Work context	Present or past employment or professional activities carried out in the context of the relationships referred to in par. below. 0through which, irrespective of the nature of such activities, a person acquires information about violations and where he or she may risk retaliation if he or she reports them.
Public Disclosure	The act of making information about infringements public through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people.
Facilitator	The natural person assisting the reporting person, if any, in the reporting process, operating within the same work context and whose assistance must be kept

	confidential.
Corporate Support Functions	The corporate functions supporting the reporting management body in the investigation phase of the report investigation.
Competent Functions	The corporate functions to which reports not falling within the scope of the whistleblowing decree are forwarded by the management body.
Grimaldi Group	The group of companies consisting of the parent company Grimaldi Group S.p.A. (GG) and its direct subsidiaries, Grimaldi Deep Sea SpA (GDS) and Grimaldi Euromed SpA (GEM).
MOG	Organisational, Management and Control Model adopted by the above-mentioned companies, pursuant to Leg. 231/01
Privacy Policy	Regulation (EU) 2016/679 of 27 April 2016*(General Data Protection Regulation* or GDPR), Legislative Decree No. 196 of 30 June 2003, as amended by Legislative Decree No. 101 of 10 August 2018, containing "*Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*" (Privacy Code), the Measures of the Guarantor for the Protection of Personal Data and in general all external legislation on the protection of natural persons with regard to the processing of personal data.
Sectoral regulations	The set of European Union or national acts indicated in the Annex to the *Whistleblowing* Decree or the national acts constituting implementation of the European Union acts indicated in the Annex to Directive (EU) 2019/1937, where applicable[1].
VO	The supervisory body provided for in Article 6(1)(b) of Decree 231/01.
Governing bodies	The set of bodies with strategic supervision, management and control functions (Board of Directors, Chief Executive Officer and Board of Statutory Auditors of the Company).
Decision-making body	Function/body in charge of defining and/or adopting measures in response to Reports (see *below*) received, according to the system of delegations and powers in force at the Company[2].
Reporting Management Body (OGS)	The Committee set up internally by the Company as the body responsible for receiving, examining and assessing reports pursuant to the applicable *whistleblowing* legislation, by resolution of the Board of Directors. The Committee ensures the proper conduct of the Procedure and prepares the report on Material Reports which, following the investigation carried out, appear to be reasonably well-founded. It also keeps a special Register of Reports, and draws up and submits to the Governing Bodies the Report referred to in par. 11.

[1] See Art. 2, para. 1, lett. a) number 3) of the *Whistleblowing*Decree . Reference is made to legislation in the areas of: public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection and security of networks and information systems.

[2] The persons in charge of receiving, examining and evaluating Reports do not participate in the definition of any decision-making measures.

Retaliation	Any conduct, act or omission, even if only attempted or threatened, committed by reason of the Whistleblowing and which causes or may cause the Whistleblower/Whistleblower, directly or indirectly, unjust damage.
ROG	Resource placed by the Board of Directors at the head of the reporting management body, as Head of the OGS structure. The Head may identify, outside the Committee set up by the Board of Directors, one or more staff members of the management body (AOG), with the functions of receiving reports and supporting the performance of management activities related to them.
Signalman	The natural person making the Report.
Reported	The subject, whether natural or legal person, mentioned in the Report, who is attributed, directly or indirectly, responsibility for the fact which is the subject of the Report or otherwise implicated in the reported breach.
Report	Any communication, written or oral and not anonymous, of information acquired by the Whistleblower in the context of his/her work context, including well-founded suspicions, concerning (i) violations committed or which, on the basis of concrete elements, could be committed in the Perimeter Companies, as well as (ii) conduct aimed at concealing such violations.
Anonymous reporting	Notifications lacking information on the sender that can be identified with reasonable certainty (e.g. surname and first name and tax code or date of birth or residence). Therefore, reports in which the sender identifies him/herself by pseudonyms or other generic or fictitious names that do not allow the identity of the reporter to be detected, or that refer to a person who cannot reasonably be unambiguously identified as the sender of the communication, are also to be regarded as anonymous.
External signalling	The written or oral communication of information on violations, submitted through the external reporting channel referred to in para. 12.
Reportable violations	Acts or behaviour, including omissions, that harm the public interest or the integrity of the Company or the Grimaldi Group, carried out in violation: - the Code of Conduct, the OMC and internal regulations/procedures issued by the Company, - laws, regulations or measures of national or European Union authorities, in the fields indicated in the following par. 4, - of the financial interests of the European Union, - the internal market, including violations of EU competition and state aid rules, and, - acts or conduct that frustrate the object or purpose of the provisions of Union acts in 'sensitive' areas.

3. Persons who may activate the internal system for reporting violations

The internal system of reporting violations governed by the Procedure covers Reports of violations made by:

- Shareholders;
- Persons with functions of administration, management, control, supervision or representation, even if these functions are exercised on a de facto basis[3].
- Employees of the Company or the Group, temporary workers, apprentices, trainees and interns, as well as seafarers enlisted on board company ships.
- Self-employed workers, including casual workers, freelancers, consultants, volunteers and trainees (paid and unpaid), who work for Group companies.
- Employees and collaborators who work for suppliers of goods or services, contractors or subcontractors used by the Company.
- Agents and shipping agents used by the Company.

Reports may also be made when the legal relationship with GG has not yet commenced (if breach information was acquired during the selection process or in other pre-contractual stages), during the probationary period and after termination of the legal relationship (if breach information was acquired during the course of the legal relationship).

4. Subject of Reports

The internal system of reporting violations governed by the Procedure covers reports concerning:

• criminal and/or administrative offences and/or accounting offences under national law;

• relevant unlawful conduct within the meaning of Legislative Decree No. 231 of 8 June 2001 (i.e. constituting predicate offences) or violations of the Organisation and Management and Control Model or the Code of Conduct;

• offences committed in breach of the European Union legislation listed in Annex 1 to Legislative Decree No. 24/2023 [4] and of all national provisions implementing it relating to the following areas:

- public procurement;
- financial services, products and markets and the prevention of money laundering and terrorist financing;
- safety and conformity of products;
- transport security [5];

[3] This includes managers and members of the Supervisory Board of the Company.

[4] The reference to Annex 1 of the Decree is to be understood as a dynamic reference as it relates to changing regulations.

[5] The sensitive sectors of primary reference, for the Grimaldi Group Companies, are those relating to "Transport Safety" and "Environmental Protection", in relation to which the Annex to Decree 24/2023 refers to the following acts: Legislative Decree 15 February 2016, No. 32, implementing Directive No. 2013/54/EU on certain flag State responsibilities for compliance with the Maritime Labour Convention, 2006 and its enforcement; Legislative Decree. no. 53 of 24 March 2011, implementing Directive 2009/16/EC concerning international standards for ship safety, pollution prevention and shipboard living and working conditions for ships calling at Community ports and sailing in the waters under the jurisdiction of the Member States; Legislative Decree. 18 August 2015 No 145, implementing Directive 2013/30/EU on the safety of offshore oil and gas operations and amending Directive 2004/35/EC.

- environmental protection;
- radiation protection and nuclear safety;
- food and feed safety and animal health and welfare;
- public health;
- consumer protection;
- privacy and protection of personal data;
- security of networks and information/digital systems;

• acts or omissions affecting the financial interests of the Union or affecting the internal market, including violations of EU competition and state aid rules.

• acts or conduct that frustrate the object or purpose of the provisions of the acts of the European Union.

The information may also concern:

(a) violations not yet committed that the reporter, on the basis of concrete evidence, believes could be committed;

(b) conduct aimed at concealing violations already committed.

The reports that are the subject of this procedure **do not concern** disputes, claims or requests linked to an interest of a personal nature on the part of the reporter that relate exclusively to his or her individual employment relationships, or inherent in his or her employment relationships with hierarchically superior figures.

Thus, reports concerning, for example, labour disputes and pre-litigation phases, discrimination between colleagues, interpersonal conflicts between the reporting person and another worker or with hierarchical superiors, reports concerning data processing carried out in the context of the individual employment relationship, in the absence of injury to the integrity of the entity, are excluded.

Unfounded reports made with malice or gross negligence result in the lapse of the protective measures set out in para. 8 as well as the application of disciplinary sanctions, in accordance with the Company Disciplinary Regulations in force and without prejudice to other forms of liability provided for by the law.

Nor do reports based on mere suspicions or rumours, those unrelated to the work context or relating to information that is already in the public domain fall within the internal system of reporting violations governed by the Procedure.

5. Channels and Means of Transmission of Reports

Since the reporter must be guaranteed a choice between different reporting methods, the channels and/or means of transmission that may be used, at his or her choice, to convey reports to the OGS are as follows:

5.1. Whistleblowing Portal

The Grimaldi Group makes available to whistleblowers a *cloud-based* telematic platform designed to take in reports and manage them, with autonomous and distinct partitions dedicated to each Group Company directly involved (hereinafter, "whistleblowing portal" or simply "portal").

The portal can be reached at https://grimaldigroup.whistleblowings.it/ and accessible from the company

website via a dedicated web page.
The portal allows authorised persons - as defined in section 3 - to make reports through a guided *online*path, guaranteeing the confidentiality of the reporter's identity or, where chosen, anonymity.

The system, in fact, allows you to send reports without having to register or declare your personal details. If the reporter chooses to give his/her personal details, confidentiality is guaranteed.

The portal allows remote and confidential dialogue with the reporter, with no possibility for the receiver or others to trace the origin of the report. In any case, the reporter may also provide his or her personal details at a later stage, also through the messaging system provided by the Portal.

Access to the Whistleblowing Portal is, in fact, subject to the “no-log”policy to prevent the identification of whistleblowers who wish to remain anonymous: this means that the company’s IT systems are not able to identify the portal access point (IP address) even if access is from a computer connected to the company network.

Reports transmitted via the Whistleblowing Portal are received exclusively by OGS members and the association of the identity of the reporter to the report can only be made by that body.

The processing of the data contained in the reports takes place using organisational and processing logics that guarantee the security, integrity and confidentiality of the data in compliance with the organisational, physical and logical measures laid down by the provisions in force.

In particular, the transmission of data provided by the reporter through the use of the platform is managed using a secure network protocol (https) for data transport. Encryption techniques are also applied, thus guaranteeing the confidentiality of the information transmitted.

After accessing the Portal, the reporter is asked to fill in a questionnaire consisting of a progressive series of open and closed questions, some compulsory, others optional, concerning facts, places, temporal context, and further elements characterising the report, with the aim of providing, from the outset, useful elements of investigation to support the preliminary investigation phase.

When the report is sent, the Portal issues the reporter with a unique identification code (ticket). The ticket will be used by the reporter to access, through the Portal, his report in order to: monitor its progress; enter additional information to substantiate the report; provide his personal details at a later stage, with respect to an initially anonymous report; answer any further questions addressed, through the portal, by the OGS.

The Reporting Officer has the possibility, by accessing the Portal after the first one, to check at any time the progress of his Report as well as the outcome of the procedure (including archiving). In any case, the OGS shall, within three months from the date of receipt of the Report or, in the absence of such notice, within three months of the expiry of the seven-day period from the submission of the Report, provide feedback - in writing via the[6] platform - on the outcome of the proceedings or on any further feedback to be expected.

[6] In the case of a Report through a face-to-face meeting, as referred to in § 5.3 below, written feedback is sent to the contact person indicated by the Reporting Party at the interview.

5.2. Voice channel

The Company establishes a 24-hour hotline every day of the year that allows the reporting person to report the content of the Report to a qualified operator by telephone through a multilingual service. The dedicated number is **800778747**.
The transcript of the voice report is made available to the management body in the form of a pdf report via the web portal.
When information on violations is communicated orally by recording a voice message or, at the Reporting Party's request, during a direct meeting with OGS members as described below, the direct meeting with OGS members as described below, the Report - with the consent of the reporter - is documented by OGS either by recording it on a device suitable for storage and listening or in writing by means of a detailed record of the conversation. The consent of the Reporting Party to the documentation of the Report is expressly acknowledged at the beginning of the recording or written report by means of a verbatim transcript. In the case of a transcript, the reporter may verify, rectify and confirm its content by signing it.

5.3. Direct meeting with the OGS

If the reporter prefers to meet the Management Authority in person, he/she may make a request via the voice channel mentioned in the previous section. 5.2 or that of the ordinary mail referred to in par. 5.4.
The face-to-face meeting may take place in simultaneous physical presence, or also by means of remote communication systems, while ensuring the confidentiality criteria imposed by the applicable legislation.
The face-to-face meetings are scheduled, within fifteen working days from the date of receipt of the Whistleblower's request, at the Company's head office, in company premises that guarantee the utmost confidentiality within the meaning of par. 8.1or, if consented to by the applicant, by means of a videoconference link which in turn guarantees the utmost confidentiality of the interview and in which only persons entitled to do so may participate.
At the request of the reporter, any Facilitators may also take part in the meetings.
At the end of the meeting, the management body - after issuing the information notice on the processing of personal data and/or the information needed to find the full text of the information notice - in order to ensure the traceability of the oral report and the same level of protection ensured for written reports, proceeds to upload the contents of the report on the IT portal, taking care to ensure that it is faithful to the statements made by the reporter, and then to record on the portal all the progress of the investigation.

5.4. Forwarding by ordinary mail

If the whistleblower wishes to use a traditional transmission channel, he/she may draft the report in analogue written format, respecting the following modalities:

a) fill in a note containing your identification data and the type of legal relationship with the company (shareholder, manager, employee, consultant, etc.) with a photocopy of your identification document attached and place it in a first sealed envelope;
b) draft the report in writing, taking care to detail as much as possible the description of the fact - with evidence of the circumstances of time and place (e.g. vessel, company head office/office or other

location where the fact occurred) and other elements (including documents) enabling the identification of the person or persons to whom the reported facts are to be attributed - and place it in a second sealed envelope, so as to separate the identification data of the reporting person from the contents of the report;

c) place both envelopes in a third sealed envelope marked "confidential for*the reporting manager*" (e.g. "confidential OGS") on the outside and send the envelope to the Company's registered office.

The report sent by ordinary mail will then be subject to confidential registration, also by means of the autonomous register referred to in the following paragraph. 6.3, by the OGS, which will take care of pouring it into the telematics portal.

5.5. Residual channels

Anyone who receives a Report through a channel other than those described above is obliged to communicate it, in whatever form, to the OGS in order to ensure the proper handling of the Report.

The OGS is responsible for promptly feeding the Reports thus received back into the portal.

5.6. Conflict of interest

In the sole special case where the Report has one of the OGS members as a Reported person, the electronic portal provides for modalities to exclude the Reported person and his or her reporting officers from the list of Report recipients. It is the task of the OGS to ensure the exclusion of any reported member/associate from the subsequent investigative activity, informing the Board of Directors if necessary.

6. Process for handling alerts

The reporting process is divided into the following steps, which are detailed in the following paragraphs:

- reception and preliminary analysis of admissibility of alerts;
- examination and assessment of the merits of the Reports;
- reporting to the decision-making body;
- compilation of the register of alerts.

6.1. Receipt and preliminary analysis of admissibility of reports

Upon receipt of the Report, the Reporting Officer is informed by the OGS - via the Platform or in another traceable way - of the receipt of the Report, within seven working days from the date of receipt of the Report, as well as of the possibility of being contacted again in order to acquire any useful elements for the investigation phase.

During the preliminary analysis of the report, OGS members first assess whether the report has the characteristics to be qualified as a manageable report under the whistleblowing legislation and this Procedure; in particular, OGS assesses whether the report

- either anonymous or named, and in the former case:
    - is relevant to the business/work context, or, in the second case:

- is made by a person who is one of those entitled to make reports under para. 0;

- relates to conduct, acts or omissions that may constitute a breach within the meaning of para. 4also assessing the non-personal nature of the report and its relevance to the purpose of protecting the integrity of the institution.

In the absence of any of the above elements, the report is to be considered as not falling within the scope of the Procedure and must be dismissed for inadmissibility according to the parameters of the law, with the reporting party being informed [7]. However, if the OGS assesses that the reported fact, even though it cannot be dealt with for the purposes of the *whistleblowing* legislation, is nonetheless relevant for other purposes for the Company, the report is forwarded, accompanied by a brief explanatory note, to the competent function - while at the same time informing the Whistleblower - so that it can be dealt with on the basis of other reference legislation. Examples include, but are not limited to:

- complaints that can be classified as a 'complaint' (e.g. from customers or passengers of social ships), according to the 'Complaints Handling Policy' in force (where adopted), are forwarded to the competent complaints structure according to the Policy;

- reports of disciplinary relevance that do not relate to this Procedure are forwarded to the Company's HR or Marine Hr departments, depending on whether they concern administrative or maritime personnel.

If, on the other hand, the Report falls within those that can be handled under the sectoral legislation and this Procedure, the OGS proceeds with the activities set out in the following paragraphs.

6.2. Examination and assessment of the merits of Reports

Having passed the subjective and objective admissibility check in accordance with the preceding paragraph, the OGS assesses, first of all, whether the Report is sufficiently circumstantial to be able to initiate the necessary in-depth investigations; if not, it promptly requests the Reporting Officer to provide the additional information deemed necessary.

If, within 15 working days from the request, such additional information is not provided or is provided in an incomplete and/or insufficient manner for a full assessment of the Report itself, the OGS will proceed to archive the Report, promptly informing the Reporting Officer, within 30 working days from receipt of the Report or from receipt of any additional information.

If, also as a result of the further information received from the Reporting Officer, the Report appears to be not obviously unfounded, the OGS takes charge of the Report and starts the preliminary investigation phase as to its merits.

In particular, the OGS in the investigation phase, in examining the facts narrated by the reporter and in compliance with legal obligations concerning the way the facts are ascertained has the power to:

a) obtain relevant documentation from the reporting person or third parties;

b) obtain information from other employees or from persons indicated by the Whistleblower as having been informed of the facts, or from the Whistleblower himself;

c) summon and request hearings from the Whistleblower or his hierarchical superiors, heads of function, managers, etc.

[7] In this case, the OGS is not obliged to enter the report received via toll-free number, face-to-face meeting, ordinary mail or other means into the Platform.

Where the Report relates to criminal misconduct relevant under Decree 231/01 or to breaches of the OMC, the OGS, in compliance with the confidentiality measures set out in par. 8.1, it promptly informs the Company's Supervisory Body of the Report received and its intention to proceed with the preliminary investigation phase, in order to collect any indications from the Supervisory Body itself, which, from that moment on, cooperates with the OGS in investigating the progress of the case.

If it considers it appropriate, the OGS uses the support of other corporate functions to carry out the necessary checks, including at the relevant corporate structures or persons involved, always in compliance with the confidentiality measures set out in para. 8.1.

The OGS is not obliged to inform the Report(s) of Reports received concerning him/her, but is entitled to do so and, in such a case, may ask the Report(s) whether he/she intends to make statements. In any case, the Reported person(s) must be heard at his/her/their request in this respect, also by means of a paper procedure through the acquisition of written comments and documents, through the computer channel provided for and always in compliance with the confidentiality measures set out in par. 8.11.

Once the preliminary investigation phase has been completed and all the elements relevant to the assessment of the Report have been collected, the OGS, having consulted the Supervisory Board (if the Report concerns breaches of the OMC 231) or the company support function (if the Report concerns breaches outside the OMC 231), draws up a note explaining the analyses carried out and the results that emerged (the so-called report report), highlighting its opinion on the merits or unfoundedness of the Report and the reasons for it.

6.2.1 Judgement of unfoundedness of the report by the OGS

At the end of the preliminary investigation phase, if the Report appears to be unfounded on the merits as a result of the in-depth investigations carried out, the OGS will make a reasoned proposal to dismiss the Report, which will be communicated to the Company's governing body, which has the right to object to the dismissal and to convene the OGS for a further joint assessment of the Report. The Whistleblower is informed of the dismissal or the supplementary investigation following an objection by the Governing Body within the legal deadline (three months from the date of receipt of the report). Where the in-depth investigation ordered at the request of the Governing Body takes longer than three months, the OGS may provide interim feedback to the reporter, postponing final feedback to the outcome of the additional investigation.

By way of example and without limitation, the OGS orders the filing of the report on its merits in the following cases:

(a) manifestly unfounded due to the absence of factual elements referable to the infringements typified by Legislative Decree no. 24/2023 (cf. 4)

(b) generic content of the Report of Offence such that the facts cannot be understood;

c) Reports of wrongdoing accompanied by inappropriate or irrelevant documentation, such that the content of the Report cannot be understood;

(d) production of documentation only in the absence of a report of unlawful conduct;

(e) existence of minor infringements [8].

[8] The term 'minor breaches' refers to all breaches characterised by a 'limited seriousness of the breach and/or the slight significance of the interests involved': it also includes all those reports from which it can be inferred that, owing to the manner of the conduct reported and/or the slightness of the damage or danger, the offence caused to the integrity of the Entity is of particular tenuousness and the conduct is not habitual.

6.2.2 Assessment of the merits of the report by the OGS

If, on the other hand, the Report, following the in-depth investigations carried out, appears to be reasonably well founded - in terms of the likely/probable existence (although not certain nor objectively proven) of the reported unlawful act - the OGS transmits the report, accompanied by its own assessments, to the competent Decision-making Body and informs the Reporting Officer thereof.

6.3. Reporting Register

The OGS keeps a register of all the Reports it receives (including anonymous ones) and their management, ensuring that they and all accompanying documentation are stored in appropriate paper/computer files, in compliance with the confidentiality measures set out in par. 8.1.

The OGS takes care of the archiving of all documentation supporting the Report received. Personal data relating to Reports are retained and kept for the period necessary to complete the verification of the facts set out in the Report, and for 5 years after the date of communication of the final outcome of the reporting procedure, except for any proceedings arising from the handling of the Report (disciplinary, criminal, accounting) against the Reported Person or the Reporting Party (bad faith, false or defamatory statements). In that case, they will be retained for the duration of the proceedings and until the expiry of the time limit for challenging the relevant measure. At the end of this period, the data are either deleted or irreversibly anonymised and stored for statistical purposes only.

7. Adoption of decision-making measures

The tasks of the OGS cease with the official report containing its opinion on the merits or unfoundedness of the report to the decision-making body.

On receipt of the OGS report, the competent decision-making body decides on the appropriate action to be taken on the basis of the current internal and external regulatory framework, unless it deems it necessary to carry out further investigations, in which case it asks the OGS or the Supervisory Board or other support functions to carry them out, depending on the cases referred to in the preceding paragraphs.

Consequently, by way of example but not limited to, the decision-making body is responsible:

- decide whether to order further investigations;

- initiate disciplinary proceedings directly;

- address the competent authorities.

In the event the Report constitutes a prerequisite for the possible initiation of disciplinary proceedings against the reported person, if the charge is based, in whole or in part, on the Report (and not also on the results of separate and additional investigations with respect to the Report, carried out by the Company also following the Report) and knowledge of the identity of the reporter is indispensable for the reported person's defence, the Report will be usable for the purposes of disciplinary proceedings only if the reporter has consented to the disclosure of his/her identity.

In the event that the Whistleblower is jointly responsible for violations, a modulation of the disciplinary measures that may be imposed on him/her is envisaged, taking into account his/her contribution to the discovery or prevention of violations and consistent with the applicable discipline.

The Decision-Making Body informs the OGS of the action taken following the report submitted to it, including notice of any closure of the proceedings.

8. Measures to protect the reporter and the reported person

8.1. Confidentiality

Alerts may not be used beyond what is necessary to adequately follow them up.

Throughout the entire Whistleblowing management process, from the reception phase to the preliminary and conclusive phases, the utmost confidentiality is ensured on the identity of the Whistleblower and of the reported person, as well as on the content of the Whistleblowing and of the related documentation.

The persons receiving, examining and assessing Reports, the OGS, the members of the Supervisory Board and any other person involved in the Procedure have an obligation to ensure that the information received is kept strictly confidential and that the identity of the Whistleblower is not disclosed except under certain conditions, set out in par. 8.2.

The use of the Portal referred to in par. 5.1 allows:

- already upon receipt, to encrypt the elements linked to the Report, as well as the identification data of the Reporting Party;
- to keep all Reports and related documentation in a 'protected environment' accessible only to OGS members;
- to avoid communication or circulation of documents outside this environment, in cases where it is not strictly necessary for the management of the Alert.

Platform authorisations for the management of Reports are defined according to criteria that guarantee access to a number of users limited to those strictly necessary for the effective management of the process. The decryption of the reporter's identity may only take place with the prior authorisation of the ROG, and under the conditions set out in par. 8.2.

The following measures must also be observed:

- any paper or electronic documents containing information that is the subject of a Report are identified by the words "Confidential" and must never be left unattended; they are kept in premises with controlled physical access or in dedicated archives protected by appropriate security systems;
- when the transmission/storage of information subject to reporting is by means of electronic *files* , these must, where possible, be *password-protected*;
- printing or copying documents should only be carried out if strictly necessary and in any case in protected environments, avoiding throwing printouts or leaving copies unattended at printers and photocopiers located in corridors or other unattended places;
- the transfer of paper documents is to be avoided; if necessary, it is tracked by filling in the appropriate form for the transmission of confidential documents in Annex 1;
- anyone who has knowledge that the reported information has come into the possession of persons not involved in the reporting process, shall report this to the OGS.

Breach of the confidentiality obligation is a source of disciplinary liability, in accordance with the current Corporate Disciplinary Regulation or the Disciplinary System set out in the MOG adopted by the Company and without prejudice to other forms of liability provided for by the law.

8.2. Cases in which the identity of the Whistleblower may be disclosed and information to the reported person

Except in the cases expressly provided for by the legislation in force[9], the identity of the Whistleblower and any other information from which this identity may be inferred, directly or indirectly, may not be disclosed without his/her express consent to persons other than those competent to receive or follow up Whistleblowings, who are expressly authorised to process such data in accordance with the Privacy Rules.

In the disciplinary proceedings, in particular, no information is given to the reported person about the Report against him or her, let alone about the identity of the reporting person:

- both in the event that disciplinary proceedings are initiated against the reported person;
- or if the Report is archived.

As mentioned in par. 7, moreover, if the dispute is based, in whole or in part, on the Report (and not also on the findings of investigations separate and additional to the Report, carried out by the Company even following the Report itself), the latter shall be usable only in the presence of the Whistleblower's consent to the disclosure of his identity. In this case, the identity of the reporting person may be disclosed to the reported person if it is indispensable for the latter's defence. In such a case, the OGS informs the reporter in writing of the reasons for disclosing the confidential data.

8.3. Prohibition of Retaliation

Whistleblowers may not suffer any retaliation.

Dismissal, change of job within the meaning of Article 2103 of the Civil Code, as well as any other retaliatory or discriminatory measure against the Whistleblower[10] are null and void if taken for reasons directly or indirectly linked to the Whistleblowing[11]. The submission of a Report does not, in itself, constitute a breach of the obligations arising from the contractual relationship between the Whistleblower and the Company concerned.

It is understood that if the criminal liability of the Whistleblower for the offences of defamation or slander or his civil liability in cases of wilful misconduct or gross negligence is established, even by a judgment of first instance, a disciplinary sanction may be imposed on him.

The above protection measures also apply to Other Persons deserving protection.

Persons who believe they have been retaliated against may take action in the manner and form provided for in Article 19 of the *Whistleblowing*Decree[12].

---

[9] The law provides for the disclosure of the identity of the reporting person when it is absolutely necessary for the defence of the reported person.

[10] Pursuant to Art. 17 para. 4 of the *Whistleblowing*Decree , include, but are not limited to, suspensions, transfers, downgrading or non-promotion, non-renewal or early termination of a fixed-term employment contract, failure to convert a fixed-term employment contract into an open-ended employment contract where the employee had a legitimate expectation of such conversion, cancellation of holidays or leave, negative evaluations or references, early termination or cancellation of a contract for the supply of goods or services.

[11] In the event of a dispute, the onus is on the employer to prove that these measures are based on reasons unrelated to the Report itself.

[12] Article 19 of the Decree *whistleblowing* provides for the possibility of notifying ANAC of any retaliation. In such a case, the ANAC informs the National Labour Inspectorate, for measures within its competence.

8.4. Protection of the Reported

The Whistleblower is protected (i) from negative repercussions arising from the Whistleblowing, if the process of handling the Whistleblowing does not reveal any elements that justify taking measures against him/her, and (ii) from possible negative effects other than those envisaged by any measures taken.

9. Personal data protection provisions

Pursuant to the Privacy Regulations in force[13], the Data Controller of the personal data acquired in the management of the Reports is Grimaldi Euromed S.p.A., jointly with Grimaldi Group S.p.A. and Grimaldi Deep Sea S.p.A. and on the basis of a specific co-ownership agreement between them signed pursuant to Article 26 GDPR. Annex 2 contains the information on the processing of personal data for the purpose of receiving and handling the Report, which is made available, together with the Procedure, in accordance with the following paragraph. 10. When the reporter makes the Report - either through the Platform or by face-to-face meeting - he/she must confirm that he/she hasread the privacy policy.

The persons who, for various reasons, are involved in the process of managing Reports (as, for example, ROG or members of the Supervisory Board) have each been appointed as 'Data Managers' pursuant to Article 29 of the GDPR and Article 2-quaterdecies of the Privacy Code, and process the personal data acquired in the management of Reports under the authority of the Company. In addition to the foregoing, the Company has adopted and implemented its own ' *Data Protection*Organisational Model', which provides that all persons who, in the performance of their respective job functions, might process personal data (including personal data relevant to this Procedure) have each received a specific appointment as a 'person authorised to process personal data', in accordance with the aforementioned regulatory provisions. In relation to the processing of the aforesaid data and in addition to (i) the provisions of the personal data protection procedures in force in the Grimaldi Group and (ii) the "Organisational *Data Protection*Model", it is hereby specified that any person authorised to process personal data for the purpose of managing the Reports shall process such data solely for the purpose of carrying out the operations strictly necessary for the proper performance of the activities envisaged by the Procedure itself.

Individuals in various capacities involved in the Reports may exercise their rights under the Privacy Rule (Articles 15 to 22 of the GDPR) within the limits of Article 2-undecies of the Privacy Code. In particular, the right of access referred to in Article 15 of the GDPR cannot be exercised with a request to the Company, in relation to the personal data processed in the context of the Whistleblowing and for all stages of the procedure, if the exercise of this right could result in actual and concrete prejudice to the confidentiality of the identity of the Whistleblower. In this case, the reported person must be informed of the limitation of his/her right of access in order to protect the confidentiality of the reported person, as well as of the possibility of exercising this right through the Data Protection Supervisor, pursuant to Article 2-undecies of the Privacy Code. On the other hand, the right of access of the reported person to the identity of the reporting person should be granted when the reporting person has consented to it or when the knowledge is indispensable for the defence of the reporting person and the reporting person has consented to it, e.g. to protect the reputation of the reporting person following a bad faith report.

In order to ensure the reconstruction of the different phases of the reporting process, and as already indicated in the previous section. 6.3, it is the responsibility of the recipients of Reports to ensure that, for a period of five years from the date of closure of the investigation into the Report: (i) the traceability of the Reports and the related investigative activities; (ii) the preservation of the Reports and the documentation relating to them

[13] See Art. 4, para. 1, point 7 of the GDPR.

and the related verification activities, in special archives (paper/informatics) protected by adequate security measures pursuant to the Privacy Law.

Personal data that are not relevant to the handling of the Report are not collected or, if accidentally collected, are immediately deleted.

10. Dissemination and publication of the document

In order to encourage the use of the internal reporting system and to foster the dissemination of a culture of legality among all addressees, this Procedure:

- is published by the Company in one or more dedicated sections[14] of the website;
- is made available to all staff members in the form of a circular to be circulated through the appropriate internal communication channels by the competent offices.

11. Reporting

The Company's Governing Bodies receive an annual report from the ROG on the proper functioning of the internal reporting system (the '**Report**'), containing aggregated and anonymised information on the results of the activity carried out as a result of the Reports received.

If Reports are received relating to unlawful conduct relevant under Decree 231/01 or to breaches of the OMC, the company's Supervisory Board is informed by the OGS, in compliance with the confidentiality measures set out in par. 8.1.

12. External Reporting and Public Disclosure

The Complainant may submit an External Report to the ANAC if, at the time of submission, one of the following conditions is met:

- in the work context, there is no provision for activating the internal channel as mandatory or, if provided for, it has not been activated or, even if activated, it does not comply with the provisions of Article 4 of the *Whistleblowing* Decree;
- has already made an internal report under this Procedure and the report has not been followed up;
- has reasonable grounds to believe that, if it were to make an internal Report, it would not be effectively followed up or that it might lead to a risk of retaliation;
- has well-founded reasons to believe that the infringement may constitute an imminent or obvious danger to the public interest.

Such external reports may be made through the channels set up pursuant to Article 7 of the *Whistleblowing* Decree, in accordance with the modalities indicated on the ANAC website[15] or of the competent authorities of the reporting party's country of nationality.

Competent authorities and external reporting channels are governed by the relevant local legislation. The external reporting channels active and known at the date of issue of this procedure are listed *below*, in Appendix 3.

A *whistleblower* who makes a public disclosure benefits from the protection provided by the *Whistleblowing* Decree if, at the time of the disclosure, one of the following conditions is met:

[14] Easily accessible and whose name contains the term '*whistleblowing*'.

[15] *https://www.anticorruzione.it/-/whistleblowing*

- has previously made an internal and external Report or has made an external Report directly and not been replied to in time;
- has well-founded reasons to believe that the infringement may constitute an imminent or obvious danger to the public interest;
- has well-founded reasons to believe that the external Report may entail the risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed, or where there is a well-founded fear that the recipient of the Report may be colluding with or involved in the infringer.

[end of document]

Annex 1 - Form for the transmission of confidential documents

Confidential Document

Company	
Document title	
Date of last update	

Sender

Name	
Surname	
E-mail address	
Function/Corporate Role	
Company affiliation	

Sender's signature

_____

Recipient

Name	
Surname	
E-mail address	
Function/Corporate Role	
Company affiliation	

Recipient's signature for receipt of confidential documents

_____

Annex 2 - **Information provided pursuant to Articles 13 and 14 of Reg. EU 2016/679 on the Processing of Personal Data Derived from the Handling of Reports**

REGULATORY AND PROCEDURAL REFERENCES

- Art. 13 Regulation (EU) 2016/679 of 27/04/2016 - General Data Protection Regulation ("**GDPR**").
- Legislative Decree 24/2023 - Implementation of Directive (EU) 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws ("**Whistleblowing Decree**").
- Procedure adopted by Grimaldi Group S.p.A. to comply with the provisions of the Whistleblowing Decree (the "**Whistleblowing Procedure**").

CO-PROCESSORS

The following companies are co-processors of personal data: GrimaldiGroup S.p.A., Grimaldi Euromed S.p.A. and Grimaldi Deep Sea S.p.A., each with registered office in Palermo, Via Emerico Amari, 8 (the "**Joint Owners**"), e-mail privacy@grimaldi.napoli.it.

The co-owners have signed a special co-ownership agreement to regulate their responsibilities and tasks regarding the processing of personal data, as required by Article 26 of the GDPR, the contents of which are available to interested parties upon request.

The joint owners have appointed a *data protection officer* (DPO) who can be contacted at the following e-mail address: DPO@grimaldi.napoli.it.

PURPOSE AND LEGAL BASIS OF PROCESSING

The personal data you provide will be processed exclusively for the following purposes:

a) receipt, processing and management of reports sent to the Contact Persons through the reporting channels made available to them in accordance with the Whistleblowing Decree;

b) fulfilment of the obligations laid down in the Whistleblowing Decree, in further applicable regulatory provisions and in provisions issued by supervisory and control authorities and bodies, in accordance with the Whistleblowing Procedure.

The processing of personal data for the above-mentioned purposes does not require the express consent of the data subjects; the legal basis for the processing is in fact the obligation of the Data Controller to fulfil specific legal obligations (Art. 6.1.c of the GDPR).

COMPULSORY OR OPTIONAL NATURE OF PROVIDING DATA AND CONSEQUENCES OF A REFUSAL TO PROVIDE DATA

Reporting may be anonymous. In this case, however, it may not be possible for the co-owners to proceed further with the alert or the related investigative activity.

Otherwise, if the reporting party provides its identification and contact data in the report, these data will be used by the Reporting Parties, or parties authorised by them, for the further handling of the report and only for the purposes specified above.

The Co-owners shall also process the personal data of the persons reported, i.e. any additional persons mentioned in the report, facilitators and/or other persons involved in the handling of the report.

MODALITIES OF DATA PROCESSING

Your personal data will be processed, for the purposes set out above, on both paper and computer media, by means of electronic or automated tools, in compliance with current legislation in particular on confidentiality

and security, and in accordance with the principles of fairness, lawfulness and transparency laid down in the GDPR and reinforced, in this case, by the Whistleblowing Decree.

COMMUNICATION AND DISSEMINATION

The personal data of the persons concerned may be communicated, within the limits strictly pertinent to the obligations, tasks and purposes as set out above and in compliance with the relevant legislation in force, to the following categories of subjects

1. subjects to whom such communication must be made in order to fulfil or require the fulfilment of specific obligations laid down by laws, regulations and/or EU legislation;
2. natural and/or legal persons providing services instrumental to the activities of the Joint Holders for the purposes specified above (e.g. consultants, supervisory body, board of auditors, auditing companies, lawyers, forensic consultants, etc.).
3. police forces, competent authorities (e.g. the National Anti-Corruption Authority) and other public administrations, acting as autonomous data controllers.

Personal data will not be disseminated in any way.

DATA RETENTION PERIOD

Personal data will be retained for the entire duration of the handling of the report and for a maximum of 5 years from the closing date of the report. After this period, the data will be deleted or anonymised.

DATA TRANSFER

Personal data are stored on servers located within the European Union. It is in any case understood that the Joint Holders, if necessary, will be entitled to move servers or data also outside the European Union. In this case, it is hereby assured that the transfer of data outside the EU will take place in accordance with the applicable legal provisions**.**

RIGHTS OF THE DATA SUBJECT

Data subjects may exercise their rights under Article 15 of the GDPR:

1. obtain confirmation of the existence or otherwise of personal data concerning them, even if not yet recorded, and its communication in intelligible form;
2. obtain information on: **a)** the origin of the personal data; **b)** the purposes and methods of processing; **c)** the logic applied in the event of processing carried out with the aid of electronic instruments; **d)** the identification details of the data controller and data processors; **e)** the subjects or categories of subjects to whom the personal data may be communicated or who may become aware of it in their capacity as designated representative in the territory of the State, data processors or persons in charge of processing;
3. obtain: **a)** the updating, rectification or, where interested therein, the integration of the data; **b)** the cancellation, transformation into anonymous form or blocking of data processed in breach of the law, including those the conservation of which is not necessary in relation to the purposes for which the data were collected or subsequently processed **c)** certification to the effect that the operations as per letters a) and b) have been notified, as also related to their contents, to the entities to whom or which the data were communicated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected;
4. object, in whole or in part, on legitimate grounds, to the processing of personal data concerning them, even if relevant to the purpose of collection.

Where applicable, data subjects may also exercise their rights under Articles 16-21 of the GDPR (Right to rectification, Right to be forgotten, Right to restriction of processing, Right to data portability, Right to object), as well as the right to complain to the Garante Privacy (https://www.garanteprivacy.it/)).

Pursuant to the provisions of subparagraphs 1(e) and (f) of Article*2-undecies* of Legislative Decree no. 196/2003 ("**Privacy Code**"), data subjects are informed that their rights identified in Articles 15 to 22 of the GDPR and, in particular the right of access, may not be exercised by request to the Data Controllers, or by complaint to the Garante for the protection of personal data pursuant to Article 77 GDPR, where the exercise of such rights may result in actual and concrete prejudice to the confidentiality of the data subjects making a report, and/or to the conduct of investigations or the exercise of a right in court. Pursuant to Section*2-undecies* , paragraph 3, of the Privacy Code, the exercise of these rights may also be delayed, limited or excluded for as long as this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the data subjects, in order to safeguard the defence interests of the Data Subjects and the confidentiality of the data subjects.

In such cases:

(i) the persons concerned shall be informed by reasoned notice given without delay, unless such notice would jeopardise the purpose of the limitation of the exercise of rights;

(ii) data subjects will be able to exercise their rights through the Garante for the protection of personal data, in the manner set out in Article 160 of the Privacy Code. In such a case, the Data Protection Supervisor shall inform the persons concerned that it has carried out all the necessary checks or has conducted a review**.**

The right of the persons concerned to appeal to the courts remains unaffected.

For the exercise of the rights specified above or for questions or information regarding the processing of data and the security measures adopted, data subjects may in any case send a request to the Joint Data Controllers at the above e-mail address.

Annex 3 External Reporting Channels within the EU

For each EU Member State, the following table shows the Competent Authority for handling external alerts and the link to:

- the external reporting channel (where available),
- the transposing law (if the authority or its site or channel cannot be found).

Nation	Reference Authority	External signalling channel
Austria	Federal Office for Preventing and Combating Corruption	https://www.bak.gv.at/601/
Belgium	– Competent authorities designated by the King, by decree passed in the Council of Ministers – the Federal Ombudsmen	According to national law available at http://www.ejustice.just.fgov.be/eli/loi/2022/11/28/2022042980/justel#LNK0012
Bulgaria	Data Protection Commission	https://www.cpdp.bg/?p=rubric&aid=67
Cyprus	Competent authorities	According to national law available at https://www.dataguidance.com/sites/default/files/2022_1_006.pdf
Croatia	Ombudsman	https://www.ombudsman.hr/en/ whistleblowers-key-information
Denmark	1. the Danish Data Protection Authority 2. the Danish Financial Supervisory Authority 3. the Danish Enterprise Authority 4. the Norwegian Working Environment Authority 5. the Environmental Protection Agency 6. the Ministry of Justice (at the Police Information Service) 7. the Ministry of Defence (at the Defence Intelligence Service)	Respectively: 8. https://whistleblower.dk/english 9. https://www.finanstilsynet.dk/whistleblower 10. https://erhvervsstyrelsen.dk/whistleblowerordning 11. https://offshore.at.dk/whistleblower/ 12. https://mst.dk/service/kontakt/whistleblowerordning/ 13. https://www.justitsministeriet.dk/ministeriet/whistleblowerordning/pet/ 14. https://www.fmn.dk/da/om-os/fe-whistleblowerordning/
Estonia	/	At the date of adoption of this procedure, the Directive has not yet been transposed
Finland	Office of the Chancellor of Justice	https://oikeuskansleri.fi/ilmoittajansuojelu
France	– Competent Authority among those designated by decree of the Council of State – to the Rights Defender, who refers it to the competent authority or authorities	According to national law available at https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045388745 The Defender of Rights can be contacted at https://formulaire.defenseurdesdroits.fr/code/afficher.php?ETAPE=accueil_2016

Germany	Federal Office of Justice (BfJ)	https://www.bundesjustizamt.de/DE/Home/Home_node.html
Greece	National Transparency Authority	https://aead.gr/
Ireland	Office of the Commissioner for Protected Disclosures	https://www.ombudsman.ie/index.xml?&Language=ga
Italy	National Anticorruption Authority (ANAC)	https://www.anticorruzione.it/-/whistleblowing;
Latvia	– State administration – State Chancellery	– https://latvija.gov.lv – https://www.trauksmescelejs.lv/
Lithuania	Office of the Prosecutor of the Republic of Lithuania	https://prokuraturos.lt/lt/aktualu-pranesejams/5954
Luxembourg	Competent authorities	According to Chapter 4 of the national law available at https://legilux.public.lu/eli/etat/leg/loi/2023/05/16/a232/jo#chapter_3
Malta	Reporting Office of the Competent Authorities	According to national law available at https://legislation.mt/eli/cap/527/eng/pdf
The Netherlands	Competent authorities	As indicated in Chapter 1a. of the national law available at https://www.wetbeschermingklokkenluiders.nl/wetstraject/wetstekst
Poland	/	At the date of adoption of this procedure, the Directive has not yet been transposed
Portugal	Competent authorities	As indicated in Article 12 of the national law available at https://dre.pt/dre/detalhe/lei/93-2021-176147929
Czech Republic	Ministry of Justice	https://oznamovatel.justice.cz/chci-podat-oznameni/
Romania	– the authorities responsible for receiving and handling violations of the law – the National Integrity Agency – other authorities to which the Agency sends alerts	According to the national law available at https://legislatie.just.ro/Public/DetaliiDocument/262872 The National Integrity Agency channel is available at https://avertizori.integritate.eu/
Slovakia	Office for the Protection of Whistleblowers	According to the national law available at https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/54/
Slovenia	Competent authorities	As indicated in Article 14 of the law available at https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2023-01-0301/zakon-o-zasciti-prijaviteljev-zzpri
Spain	Independent Whistleblower Protection Authority	According to the national law available at https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513
Sweden	Competent authorities appointed by the government	The list of competent authorities is available at the link:

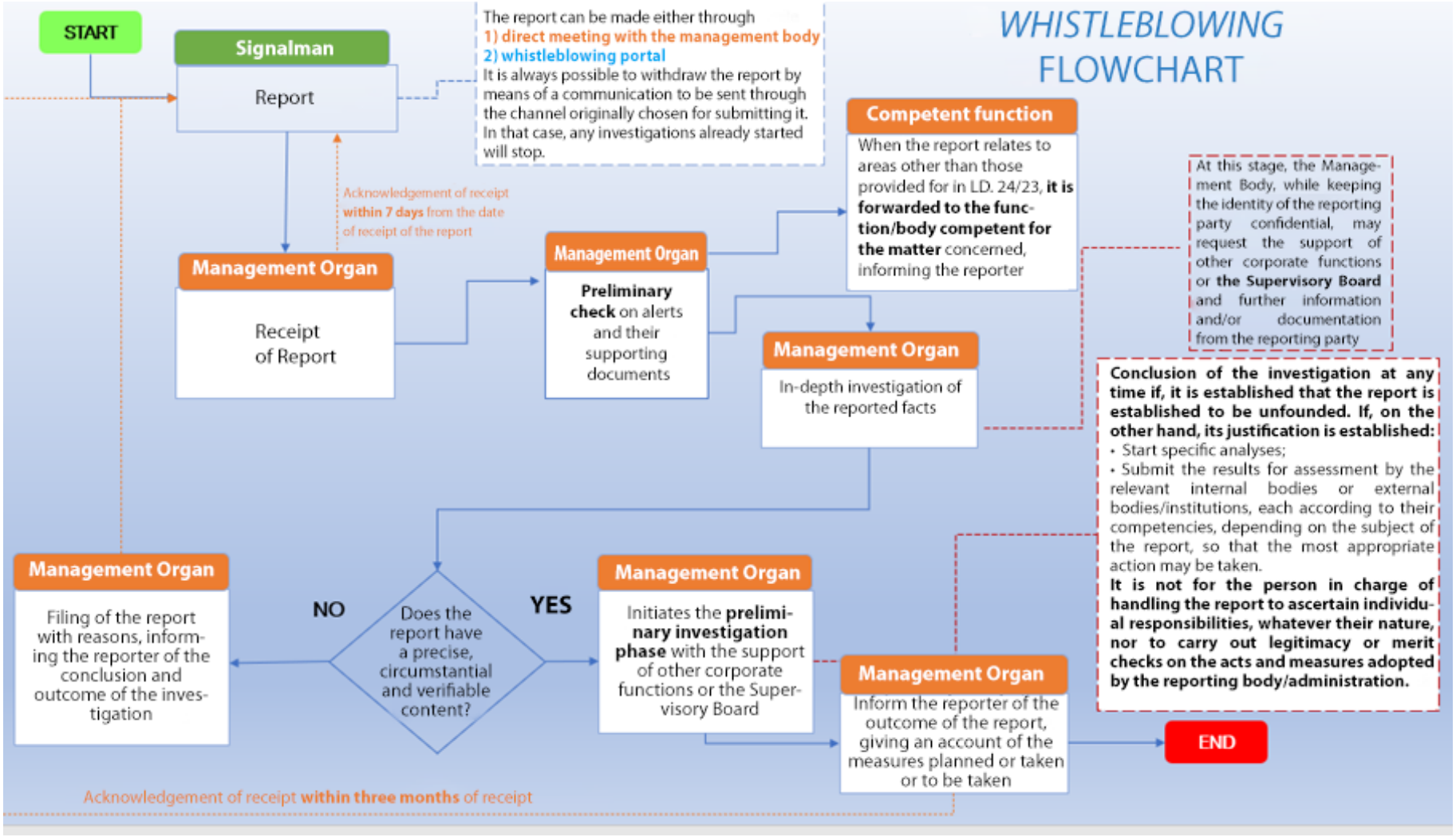
		https://www.av.se/om-oss/visselblasarlagen/extern-rapporteringskanal/lista-over-myndigheter-med-ansvar-enligt-ansvarsomrade-enligt-forordning-2021949/
Hungary	Competent authorities	According to national law available at https://magyarkozlony.hu/dokumentumok/6bbe329db1ee2d1c621b47a3e099084503a9e560/megtekintes

Legislation national laws transposing the so-called Whistleblowing Directive

Nation	Transposition of the Whistleblowing Directive
Austria	https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2023_I_6/BGBLA_2023_I_6.pdfsig
Belgium	http://www.ejustice.just.fgov.be/eli/loi/2022/11/28/2022042980/justel#LNK0012
Bulgaria	https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=6784
Cyprus	https://www.dataguidance.com/sites/default/files/2022_1_006.pdf
Croatia	https://narodne-novine.nn.hr/clanci/sluzbeni/2022_04_46_572.html
Denmark	https://www.folketingstidende.dk/samling/20201/lovforslag/L213/20201_L213_som_vedtaget.pdf
Estonia	At the date of adoption of this procedure, the Directive has not yet been transposed
Finland	https://www.finlex.fi/fi/laki/alkup/2022/20221171
France	https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045388745
Germany	https://www.gesetze-im-internet.de/hinschg/BJNR08C0B0023.html
Greece	https://www.lawspot.gr/nomikes-plirofories/nomothesia/nomos-4990-2022
Ireland	https://www.irishstatutebook.ie/eli/2022/act/27/enacted/en/index.html
Italy	https://www.gazzettaufficiale.it/eli/id/2023/03/15/23G00032/sg
Latvia	https://likumi.lv/ta/id/329680-trauksmes-celsanas-likums
Lithuania	https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/bb9a85607be711eb9fc9c3970976dfa1?jfwid=-a3k5cky91
Luxembourg	https://legilux.public.lu/eli/etat/leg/loi/2023/05/16/a232/jo#intituleAct
Malta	https://legislation.mt/eli/cap/527/eng/pdf
The Netherlands	https://www.wetbeschermingklokkenluiders.nl/wetstraject/wetstekst
Poland	At the date of adoption of this procedure, the Directive has not yet been transposed

Portugal	https://dre.pt/dre/detalhe/lei/93-2021-176147929
Czech Republic	https://www.psp.cz/sqw/text/orig2.sqw?idd=227907
Romania	https://legislatie.just.ro/Public/DetaliiDocument/262872
Slovakia	https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/54/
Slovenia	https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2023-01-0301/zakon-o-zasciti-prijaviteljev-zzpri
Spain	https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513
Sweden	https://data.riksdagen.se/fil/579EB8AD-7901-4202-BE2E-9F33ECB10347
Hungary	https://magyarkozlony.hu/dokumentumok/6bbe329db1ee2d1c621b47a3e099084503a9e560/megtekintes

Annex 4 Whistleblowing flowchart


WHISTLEBLOWING
FLOWCHART
START
Signalman
Report
The report can be made either through
1) direct meeting with the management body
2) whistleblowing portal
It is always possible to withdraw the report by means of a communication to be sent through the channel originally chosen for submitting it. In that case, any investigations already started will stop.
Acknowledgement of receipt within 7 days from the date of receipt of the report
Management Organ
Receipt of Report
Management Organ
Preliminary check on alerts and their supporting documents
Competent function
When the report relates to areas other than those provided for in LD. 24/23, it is forwarded to the function/body competent for the matter concerned, informing the reporter
At this stage, the Management Body, while keeping the identity of the reporting party confidential, may request the support of other corporate functions or the Supervisory Board and further information and/or documentation from the reporting party
Management Organ
In-depth investigation of the reported facts
Conclusion of the investigation at any time if, it is established that the report is established to be unfounded. If, on the other hand, its justification is established:
• Start specific analyses;
• Submit the results for assessment by the relevant internal bodies or external bodies/institutions, each according to their competencies, depending on the subject of the report, so that the most appropriate action may be taken.
It is not for the person in charge of handling the report to ascertain individual responsibilities, whatever their nature, nor to carry out legitimacy or merit checks on the acts and measures adopted by the reporting body/administration.
Management Organ
Filing of the report with reasons, informing the reporter of the conclusion and outcome of the investigation
NO
Does the report have a precise, circumstantial and verifiable content?
YES
Management Organ
Initiates the preliminary investigation phase with the support of other corporate functions or the Supervisory Board
Management Organ
Inform the reporter of the outcome of the report, giving an account of the measures planned or taken or to be taken
END
Acknowledgement of receipt within three months of receipt