



PURPOSE: This policy addresses the safe reporting of concerns about actual or suspected misconduct within the EXMAR Group, with a view to promoting a climate of accountability with respect to EXMAR's resources and encouraging disclosure of irregularities before they can disrupt the business or operations or lead to serious damages. We encourage you to immediately notify if you discover, become aware of, or have reasonable grounds to suspect (potential) misconduct within the EXMAR Group, in accordance with the procedure and principles set out herein.

I. DEFINITION

Whistleblowing means the confidential or anonymous reporting of illegal, dishonest or wrongful conduct within the EXMAR Group's operations, while being protected from retaliation.

The "Whistleblower" means the person reporting the suspected misconduct. Misconduct can be reported under this policy by:

- all the EXMAR Group's employees (being all individuals working at all levels and grades within the EXMAR Group entities listed in Annex 1, including senior managers, officers, directors, permanent, fixed term or temporary employees, trainees, seconded staff, and consultants);
- all crew members serving on board of vessels owned or chartered by the EXMAR Group and/or technically managed by EXMAR Ship Management, if the misconduct is not covered by the Grievance Procedure (CREW1010), part of the Crewing Manual;
- third parties who are professionally related to the business of the EXMAR Group such as suppliers, customers, business partners, former employees, potential candidate employees, shareholders, agents, brokers, joint venture partners, consultants (with no EXMAR e-mail account)

There are two main conditions for receiving protection as a Whistleblower:

- First, the Whistleblower needs to have a reason to believe that the reported information on infringements was correct at the time of reporting; and
- Second, the Whistleblower must follow the present procedure for internal or external reporting.

II. PROTECTION OF THE WHISTLEBLOWER

EXMAR intends to create a safe environment for a Whistleblower to feel comfortable when reporting any suspected misconduct within the organisation through the following measures:

1. CONFIDENTIALITY OF THE WHISTLEBLOWER'S IDENTITY

In each report under this policy the identity of the Whistleblower shall remain strictly confidential and shall not be disclosed to anyone outside the parties involved in the investigation:

- Reports are managed by case handlers and files kept within a dedicated and secured location, which is only accessible to authorized individuals of the investigation team.
- All internal / external parties involved in the investigation and follow-up actions are subject to strict confidentiality.
- Unauthorised disclosure of information related to the investigation, the report or the identity of a Whistleblower will not be tolerated and will result in disciplinary action. Depending on the circumstances such unauthorized conduct may lead to other actions, including civil or criminal lawsuits.



The Whistleblower's identity can only be disclosed in the following limited circumstances:

- If the Whistleblower explicitly consents to such disclosure; or
- If disclosure is required by law. Depending on the type of reported Misconduct, it may be legally required to involve the public authorities to initiate an official investigation. In such cases, the case handlers may be required to report the name of the Whistleblower to the public authorities. The Whistleblower will be informed before their identity is disclosed, except where such prior notification would jeopardize the investigations or judicial proceedings.

2. ANONYMITY

A Whistleblower can remain anonymous when submitting a report and during the subsequent investigations. Following measures are in place to guarantee the anonymity:

- The Whistleblower will at no time be requested to reveal their identity
- The ESM Reporting Channel and the Group Reporting Channel guarantee that the identity of the Whistleblower remains protected and cannot be uncovered
- The Whistleblower can, throughout the follow-up process, refuse to answer questions which they feel could identify themselves

The Company will undertake all reasonable efforts to investigate an anonymous report. However, if the Whistleblower chooses anonymity, there are limitations of what can be achieved.

3. NO RETALIATION

Any type of retaliation, threat, penalty or discrimination against the Whistleblower, third persons connected with the Whistleblower (e.g. colleagues or relatives) or anyone who assisted the Whistleblower to submit a report or participated in the investigation, will not be tolerated.

The Company will take appropriate actions against anyone who retaliates or threatens to retaliate.

In case a Whistleblower, third persons connected with the Whistleblower or anyone who assisted the Whistleblower is worried about facing retaliation or feels they have been retaliated against, they should immediately escalate their concerns to the Chief Legal Officer/CLO (see Annex 1).

The CLO will investigate the matter in all neutrality and make sure the appropriate actions are taken to prevent or remedy the retaliatory actions.

III. REPORTING MISCONDUCT

A report under the Whistleblowing Policy must be made in the general interest of the EXMAR Group. A Whistleblower may report misconduct such as (but not limited to):

- A crime or misdemeanour
- Infringement of governing laws, regulations and/or international treaties
- Infringement of the EXMAR Group's contractual commitments
- Infringement of the EXMAR Group's Compliance Manual and/or other policies and procedures
- Any other type of unethical or dishonest behaviour (the "Misconduct")

A Whistleblower must always act in good faith, and the report must be based on reasonable grounds. A Whistleblower is not responsible to gather proof, perform the investigation or determine corrective measures.



Reporting personal grievances and complaints on unacceptable behaviour at work or excessive workload will not be considered as reporting under the Whistleblowing Policy. If such grievances and complaints are reported the internal follow-up process may deviate.

The Company can take appropriate disciplinary and/or legal measures if a report deliberately contains false information or is made for the sole purpose of defaming or causing damage to others.

1. REPORTING CHANNELS

As an EXMAR employee, before reporting misconduct under the Whistleblowing Policy, consider the normal reporting channels (i.e. your direct line manager or supervisor, or your local HR manager). If for any reason, you feel uncomfortable or reluctant to report through the normal reporting channels, or if you are not an EXMAR employee, EXMAR Group's internal whistleblowing channels provide you with an alternative channel through which you can report the Misconduct.

1.1 Internal Whistleblowing channels

EXMAR has set up a two internal whistleblowing channels (the "Reporting Channels") through which a Whistleblower can report Misconduct:

- a Whistleblower employed by or third parties who are professionally related to the business of EXMAR Shipmanagement NV shall report to the HR Director (the "ESM Reporting Channel"),
- and a Whistleblower employed by or third parties who are professionally related to the business of any other entity of the EXMAR Group shall report to the CLO ("Group Reporting Channel").

The Reporting Channels are secure and confidential channels of reporting. They are available anywhere in the world and 24/7. Reporting can be done in writing or orally.

The contact details of the Reporting Channels can be found in Annex 1.

1.2 External reporting channels (European Union only)

Within the European Union only, a Whistleblower can report Misconduct to a local competent authority responsible for receiving and investigating whistleblowing reports (external reporting).

- For Belgium: <https://federaalinstituutmensenrechten.be/en/whistleblowers/where-to-report>
- For the Netherlands: <https://www.huisvoorklokkenuiders.nl>
- For France: <https://www.defenseurdesdroits.fr/orienter-et-protger-les-lanceurs-dalerte-180>

It is strongly recommended to report misconduct through the normal reporting channels. Internal reporting remains the most efficient route to thoroughly investigate the matter and adopt appropriate measures.

2. INFORMATION IN A WHISTLEBLOWING REPORT

A report must be sufficiently detailed and documented, including the following details (provided the relevant information is known):



- Detailed description of the events forming the suspected Misconduct and how it came to the Whistleblower's attention;
- Date and place of the suspected Misconduct;
- Names and job positions of the persons involved, or information that enables their identification;
- Names of other persons, if any, who can attest to the reported facts;
- The Whistleblower's name (this will not be requested when an anonymous report is made);
- Any other information or elements that could help the investigation team to verify the facts.

A Whistleblower is strongly invited to submit a report including their name. This may facilitate the internal investigation process for further information or questions.

3. INTERNAL FOLLOW-UP



3.1 Acknowledgement of receipt

Within seven calendar days of receipt of the whistleblowing report, the applicable Reporting Channel shall acknowledge receipt to the Whistleblower in writing.

3.2 Investigation

The report will be promptly, thoroughly and diligently investigated in observance of the principles of confidentiality, impartiality and fairness towards all individuals involved.

The Reporting Channel may

- Obtain more information and/or evidence about the Misconduct from the Whistleblower.
- Involve external parties (e.g. external counsel, investigative firms, accounting firms) where needed for conducting a thorough and confidential investigation.

3.2.1 ESM Reporting Channel

When the report was submitted through the ESM Reporting Channel the investigation is undertaken by the HR Director. The Compliance Officer and/or CLO can be involved if the misconduct reveals a more structural problem or involves multiple group companies. This is subject to the confidential treatment of the identity of the Whistleblower which can only be revealed to the Compliance Officer or CLO with the explicit written consent of the Whistleblower.

The ESM Reporting Channel informs immediately the Compliance Officer and CLO on the existence of the case and discloses certain aspects of the report for reporting purposes (internal audit), without violating the confidentiality of the details of the report, the Whistleblower and the persons involved (unless with consent of the Whistleblower).



3.2.2 Group Reporting Channel

When the report was submitted through the Group Reporting Channel the investigation is undertaken by the CLO. The Compliance Officer can be involved if the misconduct reveals a more structural problem or involves multiple group companies. This is subject to the confidential treatment of the identity of the Whistleblower which can only be revealed to the Compliance Officer with the explicit written consent of the Whistleblower.

The Group Reporting Channel informs immediately the Compliance Officer on the existence of the case and discloses certain aspects of the report for reporting purposes (internal audit), without violating the confidentiality of the details of the report, the Whistleblower and the persons involved (unless with consent of the Whistleblower).

3.2.3 ESM Reporting Channel and Group Reporting Channel

When the report was submitted through both Reporting Channels, the latter must consult each other and decide who should take the lead on the investigation taking into account the type of Misconduct and the individuals involved.

3.2.4 Conflicts of Interest

Individuals involved in the Misconduct reported by the Whistleblower will be excluded from the investigation team and will also not be allowed to participate in the consideration of the report or the determination of what action, if any, needs to be taken regarding the report. If such involvement excludes the majority of the investigation team from participating in the process, the task to consider the report and determine appropriate action will be assigned by the chairman of the Audit and Risk Committee of EXMAR to an investigating officer who is not subject to such conflict of interest.

3.3 Feedback

Not later than three months after acknowledgement of receipt, the Whistleblower will receive feedback through the relevant Reporting Channel about the (ongoing or concluded) investigation.

3.4 Report

Upon conclusion of the investigation, the applicable Reporting Channel will prepare a report describing the carried out investigative measures. A redacted non-confidential and anonymized version can be shared with local or Group executive management, on a need-to-know basis only, to come to a decision.

3.5 Decision

The relevant Reporting Channel together with ESM or Group executive management (as appropriate) makes a final decision as to whether the Misconduct is proven and will define the relevant actions needed to terminate the Misconduct and to protect the Company.

The relevant Reporting Channel will document the final decision:



- If the investigation concludes **sufficient evidence** to prove the misconduct, the report is considered **accepted** as accurate and relevant actions to terminate the Misconduct and protect the Company will be taken; or
- If the investigation concludes **insufficient** or no evidence for the misconduct, the report is considered **unfounded**, and the file will be closed.

The Whistleblower is informed through the relevant Reporting Channel about the conclusion of the report and the decision taken.

3.6 Record keeping

Each report including any evidence provided, other documents and information gathered throughout the investigation shall be kept in by the relevant Reporting Channel respecting the strict confidential treatment of the report.

Any record with personal data will be kept no longer than what is necessary and proportionate and will be deleted 3 years after the investigation has been closed. Aggregated and anonymised data for reporting purposes can be kept longer in function of the reporting requirements.

The investigation must be considered closed when

- (i) it was decided not to take any further action, or
- (ii) (ii) all action items defined in the final decision were implemented or completed.

In the event the report results in legal actions or proceedings, the investigation must be considered closed upon expiry of all time limits for legal remedies or upon exhaustion of those remedies.

4. DATA PROTECTION

Personal data of the Whistleblower, a reported person or another third party mentioned in a whistleblowing report is processed by the Company in accordance with the EXMAR Group's privacy policies (see Employee Privacy Policy and Privacy Policy (External)). This section summarizes how your personal data will be processed for the purposes of this Whistleblowing Policy.

4.1 Data controller

Personal data is processed by us as data controller, when necessary to process a report, as described in the Employee privacy policy and Privacy Policy (External).

4.2 What type of personal data do we process?

When you are either the Whistleblower, the reported person or another third party mentioned in the whistleblowing report, we process the information reported to us. This could include name, title, relation to us, information about misconduct or suspicion thereof, and information about sanctions. Even though there is no intention to process such information for whistleblowing purposes, the reported information may also include special categories of personal data such as information on race and ethnic origin, information on political beliefs, information on religious or philosophical beliefs,



information on trade union affiliation, health information and information on sexual relations or orientation. Where the Whistleblower has chosen to submit the report anonymously, the report contains no information that we can link to the Whistleblower.

4.3 Why do we process your data?

We will only process the above-mentioned types of personal data to the extent such personal data is provided to us. Personal data is processed for handling, investigating and following up on submitted whistleblowing reports, including the investigation of allegations mentioned.


An overview of the legal grounds for processing personal data depending on the processing purposes:

Purposes	Legal basis
Receipt, handling, investigation and follow-up on submitted whistleblowing reports	<ul style="list-style-type: none">Processing personal data based on our legal obligation for a whistleblowing system¹;For reports falling outside the scope of our legal obligation, the Company processes personal data based on <u>legitimate interest</u> creating a safe and pleasant working environment and keeping business operations safe and secure². If the report contains breaches of EU law, it is our legal obligation to process the above-mentioned personal data. If the report contains breaches of specific labour laws designed to ensure wellbeing at work, we may be legally obliged to process such personal data.If the report mentions special categories of personal data, we rely, depending on the content of the report, on the necessity of processing the data for an overriding public interest, or on the necessity of processing the data for occupational health purposes³.
Handing over the case including potentially personal data, to the police or judicial authorities as evidence if there are justified suspicions of an unlawful act or crime committed	Processing personal data to comply with a legal obligation ¹ or to comply with any reasonable request from competent law enforcement agents or representatives, judicial authorities, governmental agencies or bodies, including competent data protection authorities.
For establishing or exercising legal claims or organising our defence.	Processing personal data based on our legitimate interest to defend ourselves in the context of legal proceedings.
Reporting on whistleblowing cases.	Processing personal data to comply with legal and statutory internal and external audit and reporting requirements.

¹ i.e. implementation of the Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (art. 6.1.c) GDPR

² art. 6.1.f - GDPR

³ art. 9.2.g and h - GDPR

	EXMAR GROUP WHISTLEBLOWING POLICY	POL 008
		SEPT 2025
		Page: 8 / 9

4.4 With whom do we share your personal data?

We will not share personal data with anyone but the relevant Reporting Channel, and with external service providers if assistance is needed (e.g. a legal advisor/attorney, a forensic auditor). Anyone who has access to personal data will always be bound by strict legal or contractual obligations to keep personal data safe and confidential.

4.5 How long do we keep your personal data?

Personal data will only be processed as long as necessary to achieve the purposes described above, including any consequences thereof and in line with legal and internal retention periods

Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

4.6 What do we do to keep your personal data safe?

The Company applies appropriate technical, physical and organizational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and against other unlawful forms of processing. These measures include processing only the personal data required for achieving the purposes we have communicated to you, restriction of access to personal data to authorized recipients on a need-to know basis, and deleting or anonymising of personal data, which are no longer relevant for the processing purposes.

4.7 What are your rights?

For details concerning personal data owner's rights see the Employee Privacy Policy and Privacy Policy (External).



EXMAR GROUP
WHISTLEBLOWING POLICY

POL 008
SEPT 2025
Page: 9 / 9

ANNEX 1: LIST OF EXMAR GROUP ENTITIES SUBJECT TO THIS WHISTLEBLOWING POLICY AND REPORTING CHANNELS

Country	Legal Entity	Reporting Channel	Contact Details
Belgium	Exmar NV	CLO	gregory.fossion@exmar.be +32 3247 4126
	Exmar Shipmanagement BV	HR Director	florence.motttrie@exmar.be +32 3247 5636
	Exmar Marine NV	CLO	gregory.fossion@exmar.be +32 3247 4126
	Exmar Offshore BV	CLO	gregory.fossion@exmar.be +32 3247 4126
	Travel Plus BV	CLO	gregory.fossion@exmar.be +32 3247 4126
Netherlands	Exmar Netherlands	CLO	gregory.fossion@exmar.be +32 3247 4126
France	Exmar LPG France	CLO	gregory.fossion@exmar.be +32 3247 4126
	DVO	CLO	gregory.fossion@exmar.be +32 3247 4126
United States	Exmar Offshore Company	CLO	gregory.fossion@exmar.be +32 3247 4126
India	Exmar Shipmanagement India pvt.	CLO	gregory.fossion@exmar.be +32 3247 4126
	Seavie	CLO	gregory.fossion@exmar.be +32 3247 4126
Singapore	Exmar Singapore	CLO	gregory.fossion@exmar.be +32 3247 4126
Hong Kong	Exmar Hong Kong	CLO	gregory.fossion@exmar.be +32 3247 4126
Jamaica	Seavie Carribean	CLO	gregory.fossion@exmar.be +32 3247 4126