

Whistleblowing Procedure

1. PURPOSE

This Procedure sets out the rules of conduct in the event of a report of a violation of the law by:

- identifying areas subject to reporting;
- establishing rules for receiving, recording and investigating reports;
- ensuring protection for persons making reports;
- establishing corrective and preventive measures;
- ensuring compliance with applicable laws.

2. SCOPE

The procedure applies to all employees, persons performing work on a basis other than an employment relationship (e.g. civil law contracts), as well as to contractors, suppliers and other persons in a business or economic relationship with VENTUM. The provisions of this Procedure apply to the extent that they are not contrary to or incompatible with the national law in force in the country where VENTUM is registered.

3. DEFINITIONS

- **Compliance Officer** - a person appointed by the Chief Executive Officer (CEO) responsible for receiving reports, verifying them and supervising follow-up actions;
- **Internal Report** - oral or written communication to VENTUM of information about a violation of the law;
- **External report** - oral or written communication to the competent public authorities, supervisory institutions or other authorised entities in any country where the organisation operates, of information about an actual or potential violation of the law;
- **Information about a violation of the law** - this should be understood as information, including a reasonable suspicion of an actual or potential violation of the law that has occurred or is likely to occur in a legal entity in which the whistleblower participated in the recruitment process or other negotiations preceding the conclusion of a contract, works or has worked, or in another legal entity with which the whistleblower maintains or has maintained contact in a work-related context, or information concerning an attempt to conceal such a violation of the law;
- **Work-related context** - past, present or future activities related to the performance of work under an employment relationship or other legal relationship constituting the basis for the provision of work or services or the performance of functions in or for a legal entity, or the performance of service in a legal entity, in the course of which information about a breach of law was obtained and there is a possibility of experiencing retaliatory measures;

- **Follow-up action** - action taken by a legal entity or public authority to assess the veracity of the information contained in the report and to counteract the violation of law that is the subject of the report, in particular by conducting an investigation, initiating an inspection or administrative proceedings, bringing charges, action taken to recover funds, or closing a procedure carried out as part of an internal procedure for reporting violations of the law and taking follow-up action, or a procedure for receiving external reports and taking follow-up action;

- **Retaliatory action** - direct or indirect action or omission in a work-related context that is caused by the report or public disclosure and that infringes or may infringe the rights of the whistleblower or causes or may cause unjustified harm to the whistleblower, including the unjustified initiation of proceedings against the whistleblower;

- **Feedback** - information provided to the whistleblower on planned or taken follow-up actions and the reasons for such actions

- **Conflict of interest** – circumstances that may lead to a conflict of interest between or involving a member of the company's statutory body, a customer, a supplier or an entity affiliated with the company;

- **Corruption** - prohibited, unethical or unlawful acts or omissions or promises of action, to obtain an undue advantage, both material and personal (non-material), directly or indirectly;

- **Whistleblower** - a natural person who reports or publicly discloses information about a violation of the law obtained in a work-related context, including: an employee and former employee, temporary employee, a person performing work on a basis other than an employment relationship, including on the basis of a civil law contract, an entrepreneur, a proxy, a shareholder or partner, a member of a legal person or an organisational unit without legal personality, a person working under the supervision and management of a contractor, an intern, a volunteer, an apprentice, persons whose employment relationship with the company is yet to be established, where information about violations was obtained during the recruitment process or other negotiations preceding the conclusion of the contract;

- **The person concerned by the report** - a natural person, legal person or organisational unit without legal personality indicated in the report or public disclosure as a person who has violated the law, or as a person with whom the person who has violated the law is associated;

- **Person assisting in making the report** - a natural person assisting the whistleblower in making a report or public disclosure in a work-related context and whose assistance should not be disclosed;

- **Person associated with the whistleblower** - a natural person who may experience retaliatory measures, including a colleague or a person close to the whistleblower;

- **Anonymous report** - a report that does not contain data allowing the identity of the person making the

report (whistleblower) to be established or that makes it impossible to contact that person;

- Public authority – a national, regional or local public administration body, government agency, local government unit or other entity performing public functions under the law of a given country, competent to take follow-up action in areas covered by the definition of a breach;

- Public disclosure – making information about a breach of law available to the public.

4. RESPONSIBILITY

- The CEO is responsible for implementing, supervising and ensuring the effective functioning of the breach reporting system. He promotes a culture of ethics, transparency and openness within the organisation, supporting the building of trust in the breach reporting mechanism.

- The Compliance Officer is responsible for the ongoing process of receiving, recording and verifying reports, ensuring the confidentiality of whistleblowers' data, conducting investigations and reporting the results to the Management Board.

- Department managers cooperate with the Compliance Officer in investigating reports, implementing corrective measures and preventing retaliation against whistleblowers.

- All employees, associates and business partners are required to:

- a) report known or suspected violations;
- b) cooperating in their investigation;
- c) maintaining confidentiality and refraining from retaliatory actions.

5. DESCRIPTION

5.1. SCOPE OF REPORTED VIOLATIONS

- Persons who become aware of violations of the law may report both actual events and reliable assumptions about irregularities that they have obtained in the context of their work or cooperation with VENTUM. Reports may cover the following areas in particular:

- corruption;
- anti-money laundering and counter-terrorist financing;
- public procurement;
- improper financial practices, accounting irregularities or economic fraud;
- product safety, services and their compliance with requirements;
- environmental protection;
- protection of privacy and personal data;
- security of networks and information technology systems;
- freedom and human rights and professional ethics, including unequal treatment, mobbing, discrimination or abuse of official position;
- financial interests of states, public sector entities and international organisations, including the European Union;
- the principles of internal and international markets, including regulations on competition, state aid, corporate taxation and other regulated areas of economic activity.

5.2. MAKING INTERNAL REPORTS

- Violations of the law can be reported verbally, in writing or electronically (by e-mail or online form).

- VENTUM provides three secure channels for reporting violations:

- personal contact with the Compliance Officer – during a face-to-face meeting, arranged in advance at a time convenient for the whistleblower;
- a dedicated e-mail address for reporting violations: whistleblowing@ventum-offshore.com;
- an electronic reporting form, available on the VENTUM website.

- Verbal reports of violations during a face-to-face meeting should be recorded by the Compliance Officer. The whistleblower may check, correct and approve the report by signing it.

- For the report to be effectively considered, it should, if possible, contain the following information:

- date and place of the incident;
- description of the nature of the violation;
- persons involved (e.g. perpetrator, witnesses, victims);
- evidence or documents confirming the incident (e.g. emails, reports, photographs);
- contact details for feedback.

- The identity of the whistleblower and any information disclosed in the report are protected and confidential.

- Reports may only be made in good faith, i.e. when the whistleblower has a reasonable belief that the information provided is true and relevant to the public interest or the organisation. Knowingly making false reports is a violation of ethical principles and may result in disciplinary or legal liability in accordance with applicable laws in the country concerned.

- A person who makes a report in bad faith does not enjoy the protection provided for whistleblowers.

5.3. ANONYMOUS REPORTS

- VENTUM allows for the possibility of making anonymous reports of violations of the law.

- If the whistleblower has not provided a contact address or if it is not possible to determine this address based on the available data, VENTUM:

- will not send confirmation of receipt of the report;
- will not provide feedback on the actions taken as a result of the report;

- The information contained in an anonymous report is subject to preliminary analysis to assess its credibility and relevance to VENTUM's activities. If the report contains sufficient data, appropriate follow-up actions are taken, including an investigation. If the data does not allow for due diligence analysis, the report will not be considered.

- In the event of disclosure of the identity of a person who has previously made an anonymous report and if retaliatory measures are taken against them, that person is protected in accordance with section 5.6 of this procedure.

5.4. REGISTRATION OF REPORTS

- Each report is sent directly to the Compliance Officer and recorded in the Report Register.
- The Register of Reports is kept in electronic form, in accordance with the principles of confidentiality and personal data protection.
- The Register contains at least: the report number; the subject of the violation of law; the personal data of the whistleblower and the person concerned by the report, necessary to identify these persons; the whistleblower's contact address; the date of the report; information on the follow-up actions taken and the date of closure of the case.
- Personal data and documents related to the report are stored for a period of 3 years from the end of the calendar year in which the follow-up actions were completed or after the completion of the proceedings initiated by these actions.

5.5. ANALYSIS OF REPORTS AND INVESTIGATION

- Within 7 days of receiving the report, the Compliance Officer confirms receipt of the report to the whistleblower (if the report is not anonymous).
- The Compliance Officer analyses the information and documentation collected and carries out the necessary explanatory and investigative activities.
- A report may not be investigated if:
 - the report does not concern a violation of the law and falls outside the scope of this procedure;
 - the report concerns a matter that has already been reported, without any new information;
 - the report is an abuse of the law (knowingly false information);
 - an anonymous report makes it impossible to contact or verify the reporter;
 - there is insufficient data to assess the report;
- Depending on the nature of the case, the Compliance Officer may involve the following persons in the proceedings:
 - persons with relevant substantive, technical or legal expertise, or
 - with the written authorisation of the company – an external specialist entity (e.g. a law firm or auditor).
- Persons whose actions or omissions are the subject of the report, or the whistleblower themselves, may not be involved in the investigation.
- In the event of a conflict of interest or suspicion of bias, the Company's Management Board shall appoint another impartial person or team responsible for conducting the investigation and any corrective measures.
- After completing the investigation, the Compliance Officer prepares a final report in accordance with the investigation procedure adopted at VENTUM. The report is submitted to the CEO for approval.
- The deadline for providing feedback to the whistleblower shall not exceed 3 months from the date of confirmation of receipt of the internal report or, if no confirmation of receipt has been provided, no later than 3 months from the expiry of 7 days from the date of the internal report.

5.5. ANALYSIS OF REPORTS AND INVESTIGATION

- Any person who reports a violation or risk of a violation in good faith is protected from any retaliatory measures, as well as from attempts or threats of retaliation by other persons.
- This protection also applies to:
 - persons assisting the whistleblower in making the report,
 - third parties associated with the whistleblower who may suffer retaliatory measures in a work-related context (e.g. colleagues, family members),
 - legal entities owned by the whistleblower, for which they work or with which they are professionally associated.
- Whistleblowers may not be punished, discriminated against or treated unfavourably for making a report in good faith, regardless of the outcome of the investigation.
- Any actions or omissions that may be considered a form of retaliation against the whistleblower are prohibited. In particular, the following are unacceptable:
 - refusal to establish an employment relationship;
 - termination or dismissal without notice;
 - failure to conclude a fixed-term employment contract or an indefinite employment contract after termination of a probationary employment contract, failure to conclude another fixed-term employment contract or failure to conclude an indefinite employment contract after termination of a fixed-term employment contract where the whistleblower had a reasonable expectation that such a contract would be concluded with him or her;
 - reduction in remuneration for work;
 - suspension of promotion or omission from promotion;
 - omission in the award of work-related benefits other than remuneration or reduction of the amount of such benefits;
 - transfer to a lower position;
 - suspension from performing employee or official duties;
 - transfer of the whistleblower's current duties to another employee;
 - an unfavourable change in the place of work or working hours;
 - negative assessment of work performance or negative opinion about work;
 - imposition or application of a disciplinary measure, including a financial penalty, or a measure of a similar nature;
 - coercion, intimidation or exclusion;
 - mobbing;
 - discrimination;
 - unfavourable or unfair treatment;
 - suspension of participation or omission from selection for participation in training courses to improve professional qualifications;
 - unjustified referral for medical examinations, including psychiatric examinations, unless separate regulations provide for the possibility of referring an employee for such examinations;
 - actions aimed at making it difficult to find future employment in a given sector or in a given industry based on an informal or formal sectoral or industry agreement;
 - causing financial loss, including economic loss, or loss of income;

- causing other non-material damage, including violation of personal rights, in particular the good name of the whistleblower.

• Causing non-material damage, including violation of the personal rights or dignity of the whistleblower. If the work or services were, are or are to be performed based on a legal relationship other than an employment relationship constituting the basis for the performance of work or services or the performance of functions or service, the reporting or public disclosure may not constitute grounds for retaliatory measures or attempts or threats of retaliatory measures, including in particular:

- termination of a contract to which the whistleblower is a party, in particular concerning the sale or delivery of goods or the provision of services, withdrawal from such a contract or termination without notice;
- imposing an obligation or refusing to grant, restricting or withdrawing a right, in particular a licence, permit or concession.

• VENTUM ensures full confidentiality of the whistleblower's identity and any information that could lead to their identification.

• Access to the data is restricted to the Compliance Officer and persons authorised to follow up on the matter.

• The identity of the whistleblower may only be disclosed if required by law or at the request of law enforcement authorities. If disclosure of data is necessary, VENTUM shall notify the whistleblower in advance, provided that this does not prejudice the interests of the proceedings.

• The person concerned by the report is informed of the fact that it has been made and of the proceedings being conducted, while maintaining the confidentiality of the whistleblower's data.

• All information related to the investigation is strictly confidential. The whistleblower, Compliance Officer and persons involved in the proceedings are obliged not to disclose information to third parties, except in cases required by law.

• If the report concerns an action or omission by the whistleblower, the fact of making the report does not exempt them from possible disciplinary, civil, criminal or administrative liability, but this circumstance may be considered a mitigating factor in the assessment of their conduct.

• Persons who obstruct or attempt to obstruct the reporting of violations, take retaliatory action against whistleblowers, or violate the obligation to maintain the confidentiality of whistleblowers' identities or information related to the report, are acting unlawfully and contrary to the organisation's ethical principles. Such actions may result in disciplinary, civil or criminal liability in accordance with the applicable laws of the country concerned.

5.7. EXTERNAL REPORTING AND PUBLIC DISCLOSURE

• This procedure regulates the rules for making internal reports at VENTUM.

• Whistleblowers have the right to make external reports to the competent public authority in their country.

• In Poland, the central authority receiving reports is the Ombudsman or another public authority competent in the matter, in accordance with the Act of 14 June 2024 on the

protection of whistleblowers (Journal of Laws 2024, item 928, as amended).

• In cases provided for in the Act, the whistleblower may also make a public disclosure, i.e. disclose information about the violation of the law to the public, while retaining the right to protection provided for in the provisions of the Act.

5.8. PERSONAL DATA

• The controller of personal data is VENTUM Sp. z o.o. with its registered office in Gdańsk (80-171) at ul. Franciszka Schuberta 1A/2.

• VENTUM processes personal data contained in reports, follow-up actions and in report registers to the extent necessary to fulfil the obligations arising from this procedure.

• The processing of personal data for the purpose of accepting a report, taking follow-up action and ensuring the protection of the whistleblower is carried out without the need to obtain the consent of the data subject.

• Personal data shall be processed for the period necessary to achieve these purposes, not longer than 3 years from the end of the calendar year in which the follow-up activities were completed.

• The data subject has the right to request access to their personal data, rectification, restriction of processing, erasure or transfer, as well as the right to object to processing. That person also has the right to complain to the competent supervisory authority for personal data protection in the country where they reside or where the data processing took place.

• The above rules also apply to the person assisting in making the report, the person associated with the whistleblower and the person concerned by the report.

6. RELATED DOCUMENTS

- VENTUM.3.06FR Register of reports
- VENTUM.5.07PR Investigation of an incident or accident

7. TABLE OF CHANGES

See next page.

REVISION	DATE	DESCRIPTION OF CHANGE	PREPARED BY	REVIEWED	APPROVED
1.0	28/11/2025	Introduction of the procedure	KM	AM, SL, DK	MW