

OW Polska sp. z o.o. Complaint Management Policy

Document Code : **POGEN-OW-GEN-LEG-POL-00001**

Date: 16/09/2026

Prepared by:	Reviewed by:	Approved by:
Name: Berenika Sepczyńska	Name: Joao Paulo Mateus	Name: Dan Finch
Title: OW Polska Ethics and Compliance Partner	Title: Chief Ethics and Compliance Officer	Title: Country Manager
Date: 25-03-2025	Date: 20-05-2025	Date: 01-10-2025
	Name: Jose Miguel Mesa	Name: OW Management Committee
	Title: BPE & Communications Director	Date: 25-11-2025
	Date: 20-05-2025	Name: Company Board of Directors
		Date: 05-12-2025

DISTRIBUTION & CONFIDENTIALITY (please mark with X)

Personal	General	Confidential	Strictly Confidential
	X		



VERSION CONTROL

REVISION	DATE	PURPOSE OF THE REVISION	UPDATES
01	16/09/2026	Approved for Use	Compliance with the Polish Act of 14 June 2024 on the protection of whistleblowers



INDEX

- 1. DEFINITIONS, ACRONYMS AND ABBREVIATIONS..... 5**
- 2. PURPOSE 5**
- 3. POLICY 6**
- 4. GUIDING PRINCIPLES 7**
- 5. SCOPE OF THE POLICY..... 10**
 - 5.1. SUBJECTIVE SCOPE OF APPLICATION 10
 - 5.2. OBJECTIVE SCOPE OF APPLICATION 10
- 6. CONTROLLER OF THE COMPLAINTS MANAGEMENT SYSTEM..... 11**
- 7. COMPANY SPEAK UP CHANNEL 11**
- 8. GENERAL DESCRIPTION OF THE COMPLAINT MANAGEMENT PROCEDURE 11**
 - 8.1. TYPES OF REPORTS 11
 - 8.2. PRIOR CONTACT WITH THE REPORTING PERSON AND NOTIFICATION OF RECEIPT OF REPORT..... 12
 - 8.3. PRELIMINARY SCREENING/EXAMINATION PROCESS 13
 - 8.4. INVESTIGATION 13
 - 8.5. CLASSIFICATION OF THE REPORT, PROCEDURE CONCLUSION AND DECISION..... 14
- 9. SUPERVISION AND COMMUNICATION..... 14**
- 10. FINAL PROVISIONS..... 15**
- 11. DISTRIBUTION 15**
- 12. REFERENCES..... 15**
- 13. ANNEX I – EXTERNAL CHANNELS OF THE COMPETENT AUTHORITIES..... 16**



1. Definitions, acronyms and abbreviations

For purely interpretative purposes of this Policy, the terms and definitions used therein will have the meaning described below.

Breach or Breaches: any breach of current laws or regulations as indicated in section 5 of the Policy.

Investigation: process to collect, examine and investigate the facts rigorously, independently and objectively to accurately establish the credibility of the Report and the surrounding circumstances; to identify the parties involved; to assess whether or not the issue constitutes Breach or some type of irregularity and the root causes and potential impacts/consequences arising thereof.

Investigation Team (IT): group of people that ensure the Reports made are examined and investigated.

Retaliation: any act or omission (including threats or attempts) which occurs directly or indirectly in a work-related context, prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified property damage or pain and suffering to the Reporting Person, including the unfounded initiation of proceedings against the Reporting Person; in particular, actions that bear signs of discrimination or unfair treatment.

Report: communication in good faith of an actual Breach or a reasonable suspicion of a potential Breach to the Company using one of the reporting methods indicated in the Policy.

Registry: the register of Reports.

Person Concerned: a natural or legal person who is mentioned in the Report as party and/or co-perpetrator to the alleged Breach or Breaches.

Person Reported: the person who under this Policy is attributed by the Reporting Person with having allegedly committed the Breach or Breaches.

Policy: Complaint Management Policy for OW Polska sp. z o.o.

Reporting Person: the person who submits a Report through the means of communication put in place for this purpose.

Stakeholder: a person or organization that may affect, be affected by or believe itself to be affected by a decision or activity (e.g., in Company shareholders, employees, customers, suppliers, communities; etc.).

Company: OW Polska sp. z o.o.

Act: Act of 14 June 2024 on the protection of whistleblowers.

2. Purpose

This Policy lays down the rules that apply to the procedure to receive, process, settle and register communications received by Company, about alleged unethical conduct that breaks the law or regulations.

In addition, external communications channels managed by independent public authorities are also made available for this purpose (see Annex I).

3. Policy

For some time now OW Offshore S.L. (shareholder of OW Polska sp. z o.o.) (hereinafter the “**OW**”) has had a trust and transparency policy in place that deals with how it does business and engages with all of its Stakeholder and also applies to OW Group companies, including but not limited to OW Polska sp. z o.o. Clear guidelines have been laid down regarding these matters, both by means of its Code of Ethics approved in 2021, as well as through its Anti-Corruption Policy, not to mention other very important documents that define company principles and commitments in these matters. This trust and transparency policy naturally contains channels to report allegedly ethically questionable conduct that all Stakeholders can use when they consider that company ethical principles and integrity may be compromised.

Increasing developments in these matters, such as the proliferation of different standards — albeit sharing the common aim of regulating issues heretofore subject to ethical and moral appraisal — attest to that fact that OW hit the mark with its early and resolute commitment to self-regulation regarding these issues.

Given the growing concern by lawmakers, both nationally and at EU level, to regulate issues that previously depended on the commitments undertaken by each company, OW has made the necessary amendments to these to ensure full compliance with this legislation.

A case in point is Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 on the protection of persons who report breaches of Union law (hereinafter the “**European whistleblower protection directive**” or the “**Directive**”) as well as the Polish Act of 14 June 2024 on the protection of whistleblowers (hereinafter the “**Polish whistleblower act**”) that lays down the legal obligation for all legal entities employing fifty or more workers, or that carry out certain activities as provided for in the legislation, to define and put in place a whistleblowing channel. In addition to implementing the established provisions and with a view to fostering even greater confidence for OW Stakeholders regarding these matters, OW has reviewed and updated its complaint management process, the procedures thereof and the technical support for its already existing whistleblowing channel (the “**Speak Up Channel**”).

This updating of the complaint management process clearly attests to the decisive importance OW gives to meeting its compliance obligations, particularly with respect to its intervention in investigating and resolving matters that are now grounded in specific, targeted legislation.

Accordingly, this Policy seeks to establish the rules that apply to the procedure to receive, process, settle and register communications and reports made over the Speak Up Channel to ensure to all whistleblowers full compliance with the law regarding strict, ethical business conduct, while also making sure that all well-founded reports of a breach that are submitted in good faith will be presented securely and effectively, without fear of Retaliation.

As Company is part of a OW Group (the group of companies in which OW Offshore S.L. has, directly or indirectly, the majority or the management control group of companies), the OW Complaint Management Policy were used as the basis for creating this policy for Company and was adapted to Polish law and local regulations.

Due to the fact that the Speak Up Channel through which reports are made is a dedicated channel for the entire OW Group and the categories of potential breaches are very broad, only the reporting of Breaches listed in this Policy will be covered by the protection described in the Act.

Furthermore, the confidentiality required in these matters is assured for all those who make reports on the Speak Up Channel. A corporate speak up culture can only be effective if it is

based on maximum discretion, offering whistleblowers, reported and interested parties a procedure that meets the highest ethical and behavioral standards, thereby fostering trust and the effective reporting of situations that are in breach of ethical principles and commitments.

This Policy has been approved by: Country Manager on 01 October 2025, OW Management Committee on 25 November 2025, Company Board of Directors on 5 December 2025.

4. Guiding Principles

This procedure to receive, process, settle and register Reports received by Company under this Policy will be governed by the following guiding principles:

- a) **Anonymity:** Reporting Persons can, if they so wish, request that they remain anonymous by choosing the option in the Speak Up Channel form. Notwithstanding this option, anonymity does not prevent two-way communication between (i) the person in charge of selecting, analyzing and managing the processing process and (ii) the Reporting Person, thereby leaving open the possibility of attaching supporting documentation on the reported acts by means of the field created for this purpose on the channel support platform.
- b) **Confidentiality:** Under the terms defined in this Policy, Reports will be treated as confidential information by all those who receive information on the reported events. Knowledge of its existence and the findings of the examination will be restricted to the report management team and to those who require such information to receive and monitor the Reports submitted over the Speak Up Channel. The identity of the Reporting Person together with any other information from which their identity may be directly or indirectly deduced will be kept confidential and protected and can only be disclosed with the consent of that person or where this is necessary in the context of an investigation only by a dedicated national authority or in the context of judicial proceedings. In such situations, the Reporting Person will receive a written communication indicating the reasons for the disclosure of the confidential data in question, unless any disclosure of this information might compromise ongoing investigations or related court proceedings. The Company will ensure that the individual's identity of the Person Reported and the Person Concerned is kept confidential and protected for at least so long as investigations triggered by the Report are ongoing and will ensure that the individual is treated fairly and has a right to be heard.
- c) **Data protection:** The Report reception, registration and processing procedures under this Policy are compliant with current data protection rules and information security standards. Any processing of personal data, including the exchange or transfer of personal data under this Policy, will be conducted in accordance with the EU (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) and national law (Act of 10 May 2018 on the Protection of Personal Data). Personal data that is not pertinent to handling a specific Report will not be collected or, if accidentally collected, will be deleted without undue delay.
- d) **Good faith:** All Reports must be submitted in good faith and duly substantiated. Good faith means the sincere belief of the Reporting Person that the content of the Report is true and has been prepared in the interest of the Company, without considering personal benefits and not based on personal biases; it is not necessary for a Report made in good faith to prove to

be true. Any unjustified use of the Speak Up Channel may be considered a disciplinary or legal breach.

- e) **Independence and autonomy:** Any person who has or is suspected of having a conflict of interest or direct or indirect involvement in the reported situation, will be excluded from the investigation and decision process to ensure that the receipt, screening, examination and filing of the Reports is done independently and impartially, while also ensuring the absence of any real or potential conflict of interest in the performance of those functions.
- f) **Legal protection:** As long as the Reports are made in good faith, Reporting Persons will be specifically protected and supported by the assurance of legal protection and access to tribunals to defend their rights.
- g) **Misuse:** misuse and bad faith in the use of the Speak Up Channel may leave the Reporting Person or other people involved open to disciplinary or legal proceedings.
- h) **Prohibition of Retaliation:** The Company indicates that protection against Retaliatory actions will be in line with the applicable law; examples of actions against which the Reporting Person is protected are indicated below.

The Company appreciates that the decision to file a Report can be a difficult one to make, especially when there may be a fear of reprisal from those who may be involved the Breach (e.g. from those who may have committed the Breach, etc). The Company will not tolerate retaliation against any Reporting Person where they have reasonable grounds to believe that the information in the Report is true at the time of reporting, even if it transpires that there is no basis for concluding that any Breach has occurred or is likely to occur.

The Company will take appropriate steps to protect all impacted individuals, including taking necessary action, which may include but is not limited to disciplinary action or dismissal, against anyone who is found to be pursuing any form of retaliation or discrimination, or has threatened to do so. The Company does not tolerate any form of Retaliatory actions taken by any person against the Reporting Person or any people involved in an investigation of a Report. Examples of Retaliatory actions may include, but are not limited to:

- a) refusal to establish an employment relationship;
- b) reduction in the amount of remuneration for work;
- c) overlooking the award of work-related benefits other than remuneration or reducing the amount of such benefits;
- d) suspension, lay-off, dismissal or equivalent measures;
- e) demotion or withholding of promotion;
- f) transfer of duties, change of location of place of work, reduction in wages, change in working hours;
- g) withholding of training;
- h) a negative performance assessment or employment reference;
- i) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
- j) coercion, intimidation, harassment or ostracism;
- k) discrimination, disadvantageous or unfair treatment;
- l) failure to convert a temporary employment contract into a permanent one, or probationary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;

- m) failure to renew, or early termination of, a temporary employment contract or probationary employment contract;
- n) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- o) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- p) unjustified psychiatric or medical referrals.

The above applies accordingly to the Reporting Person, engaged by the Company on a basis other than an employment contract. In particular, Retaliatory actions include the termination of a contract to which the Reporting Person is a party, withdrawal from such a contract, or its termination without notice.

This prohibition of Retaliation extends in all its forms to any person that helps the Reporting Person in the reporting process and whose help must be kept confidential, including trade union representatives or employee representatives, or any third party related to the Reporting Person that may be subjected to Retaliation in a professional context and those legal persons or similar entities owned or controlled by the Reporting Person, or for which the Reporting Person works or is professionally related.

- i) **Protection of Person Concerned data:** Generally accepted rights and guarantees protected by due process of law will be ensured for those persons concerned by the Report or public disclosure. In other words, they shall enjoy benefit of the doubt, criminal process defence guarantees and confidentiality regarding their identity.
- j) **Record keeping:** All information related to the different report processing phases are registered on the Speak Up Channel tool in accordance with Privacy Policy principles (the Registry). The Registry contains, at a minimum, information on:
 - 1) Report case number;
 - 2) description of the subject of the Breach;
 - 3) the personal data of the Reporting Person and the person concerned by the Report necessary to identify them;
 - 4) Contact address of the Reporting Person;
 - 5) date the Report was made;
 - 6) date of conclusion of the case.
 - 7) Follow-up actions carried out, including:
 - a) the outcome of the verification of the Report;
 - b) the investigation carried out and its outcome, if any;
 - c) follow-up actions carried out, if any.

According to the Polish whistleblower act records are deleted from the Registry three years after the end of the calendar year in which the follow-up actions have been completed or the proceedings initiated by these actions have been completed.

If the report was made anonymously, the register will not contain the data in points 3) and 4).

Access to the Registry is granted only to authorized individuals.

- k) **Voluntary:** This Policy is based on a voluntary reporting scheme.

5. Scope of the Policy

5.1. Subjective scope of application

This Policy applies to the Company.

All individuals employed by the Company, regardless of their basis of hire, and any individual or legal person who has had, has, or may have a professional relationship with the Company are encouraged to use the Speak Up Channel as a formal reporting mechanism regardless of any other means of communication made available to them.

This policy applies to the following individual providing information about the Breach or Breaches in a work-related context:

- a) an employee,
- b) a temporary employee,
- c) a person providing work on a basis other than employment, including under a civil law contract,
- d) entrepreneur,
- e) proxy,
- f) shareholder or partner,
- g) a member of a body of a legal person or an organisational unit without legal personality,
- h) a person performing work under the supervision and direction of a contractor, subcontractor or supplier,
- i) an intern,
- j) volunteer,
- k) trainee.

The above Policy applies to the above-mentioned individuals if the information about the Breach or Breaches obtained in a work-related context is communicated prior to the commencement of the employment relationship or any other legal relationship giving rise to the provision of work or services or the exercise of functions in or for the Company, and after its termination.

5.2. Objective scope of application

The Speak Up Channel can be used to Report an actual or suspected Breach, including but not limited to breaches involving the following areas:

- 1) corruption;
- 2) public procurement;
- 3) financial services, products and markets;
- 4) prevention of money laundering;
- 5) prevention of terrorist financing;
- 6) product safety and compliance;
- 7) transport safety;
- 8) protection of the environment;
- 9) radiation protection and nuclear safety;
- 10) food and feed safety;
- 11) animal health and welfare;
- 12) public health;
- 13) consumer protection;
- 14) protection of privacy and personal data;
- 15) security of network and information systems;

- 16) the financial interests of the State Treasury of the Republic of Poland, of local government units and of the European Union;
- 17) European Union's internal market, including public competition law and state aid rules and corporate taxation;
- 18) Constitutional freedoms and rights of the human being and citizen – occurring in the relations of the individual with the public authorities and not related to the points 1-17 above.

This Policy does not cover matters related to labour law, in particular disciplinary issues, mobbing (moral harassment), sexual harassment or those concerning the termination of employment contracts and internal policies and, therefore, the notification of the above subjects does not ensure the protection provided by the Act.

Any communication, as long as it falls under the scope of this Policy, will be covered by the protection and assurance measures established by the Company and by the applicable regulations.

6. Controller of the Complaints Management System

OW Offshore S.L. (shareholder of Company) Board of Directors has designated the Ethics and Compliance Coordination Body (hereinafter “**ECCB**” or the “**Coordination Body**”) as the Controller of the Complaints Management System (hereinafter the “**Channel Controller**”), while the Chief Ethics and Compliance Officer in OW Offshore S.L. (hereinafter “**CECO**” or “**Compliance Officer**”) has been designated as the individual to manage the Complaints Management System for the purposes of notifications and liaising with the competent public authorities in these matters.

OW Polska Board of Directors appoints the Polish Compliance Partner as local representative to assist and support the CECO regarding the scope of this Policy.

7. Company Speak Up Channel

Company Speak Up channel is available on OW website as well as on the Company’s website (<https://www.bc-wind.pl>), which can be used by Stakeholders from Company and any of its subsidiaries. This channel receives Reports on any Breach as per this Policy.

8. General description of the complaint management procedure

8.1. Types of Reports

The Reporting Person can Report through internal and external whistleblowing channels

8.1.1 Internal reporting

Internal Reports must be made through the internal channel put in place by Company as follows:

- a) Accessing through the Whistleblowing Channel available at **OW website and Company's website**;
- b) Selecting the subject matter of the Report to be made;
- c) Completing the respective form with information identifying the Reporting Person, email and contact details (unless the anonymous option is selected); the subject matter of the Report; identification of the company involved (if applicable); and a description of the facts.

8.1.1.1 Particularities of oral Report

Oral reporting can be done via the Speak Up Channel tool, allowing for anonymous Report if chosen by the Reporting Person.

The oral reporting done via the Speak Up Channel is documented with the consent of the Reporting Person in the form of a recording or a complete and accurate transcript of the conversation.

Additionally, at the request of the Reporting Person and where provided for in the local applicable regulation, oral reporting can be done at a physical meeting to be held no later than fourteen (14) days as of the request. Video conferences shall be understood for these purposes as constituting physical meetings.

If the Reporting Person opts to make the Report at a physical meeting or via videoconference, the CECO, Polish Compliance Partner or Investigation Team (IT), as appropriate, must document this by recording it on video (if so authorized by the Reporting Person) or by a complete and accurate transcription of the conversation. At this meeting:

- Reporting Person can be accompanied by a lawyer or workers' representative if the Reporting Person chooses to
- To ensure due investigation confidentiality, those who attend this meeting will be informed by the CECO, the Polish Compliance Partner or the IT (as appropriate) in writing of their duty to secrecy and confidentiality, as well as all legal information regarding Data Protection matters.
- The transcription must be signed by those present at the meeting. If for some reason the Reporting Person or any of those present does not want to sign the minutes, this will be duly recorded, and the Investigation will continue its course.
- The CECO, Polish Compliance Partner or the IT (as appropriate) will attach the recording or transcription of the conversation to the Speak Up Channel tool and will continue with the Investigation as described in this Policy.

8.1.2. External reporting

Although Stakeholders make a Report over the Company Speak Up Channel, they can also do so externally via the competent authorities.

The Reporting Person may make a Report to a competent external authority, without any prior internal Report, in accordance with this Policy (see Annex I).

8.2. Prior contact with the Reporting Person and notification of receipt of Report

The Reporting Person will be notified of receipt of the Report (acknowledgment of receipt) no later than seven (7) days after it has been made, unless this may compromise its confidentiality.

Whenever necessary, the Reporting Person may be contacted to ask for further information considered relevant for the preliminary examination.

8.3. Preliminary screening/examination process

After the Report has been received, the CECO together with the Polish Compliance Partner will screen it to assess initially whether the reported situation is a Report lacking serious grounds and deliberately and clearly unfounded or not, by considering: the content of the reported Breach, the grounds on which it is based and, any possible evidence provided by the Reporting Person. Any Report that is not seriously substantiated and is deliberately and clearly unfounded will entail the provisional shelving of the Report, duly notifying the Reporting Person.

If the Report involves a conflict of interest for the CECO or the Polish Compliance Partner, the Report will be redirected to the President of the Ethics and Compliance Coordination Body.

8.4. Investigation

If the Report is considered to be well founded, the Investigation phase will begin. This process involves collecting, examining and investigating the facts rigorously, independently and objectively to: (i) accurately establish the credibility of the Report and the surrounding circumstances; (ii) identify the parties involved; (iii) assess whether or not the issue constitutes a Breach; and (iv) assess the root causes and potential repercussions/consequences arising thereof.

In some instances, it might be necessary to refer the matter to an external authority or an external expert for further investigation or assistance in the investigation.

8.4.1 Term

The internal Investigation phase must not take any longer than three (3) months as of receipt of the Report.

In case the Reporting Person is not notified of receipt of the Report within 7 days from the date of the internal notification, the internal Investigation must not take any longer than 3 months after the expiry of 7 days from the date of the internal notification, unless the Reporting Person has not provided a contact address to which feedback should be provided.

8.4.2 Contact with the Reporting Person

Throughout the process, the IT may request additional information and/or support documentation from the Reporting Person over the Speak Up Channel to better assess the reported facts, even if the Reporting Person decides to remain anonymous. All Stakeholders are required to cooperate with the Company's investigation by providing truthful explanations and relevant documents in a timely manner in response to interviews, questions and requests for information. Destruction of documents or other evidence related to the investigation is prohibited. Any Stakeholder, who fails to cooperate or otherwise obstructs, prevents or improperly influences an Investigation, or attempts to do so, will be subject to disciplinary action and even termination of their cooperation, in accordance with applicable Company's applicable policies.

8.4.3 Contact with the Persons Concerned

During the process the Persons Concerned will be notified of the Report and of the acts reported therein. Under no circumstance whatsoever will the identity of the Reporting Persona and/or those being investigated be revealed. They will also be informed of the processing of their personal data. This notification will be given at an advanced stage of the Investigation if it is considered that doing so early on may hinder the investigation process.

8.4.4 Urgent measures and immediate action

Without prejudice to the final decision taken regarding the Report made, in clearly urgent and serious situations, appropriate measures must be adopted to protect Company and/or Stakeholders' interests against the detected irregularities.

8.4.5 Information record

All Investigations and Reports received over the Speak Up Channel will be registered and kept in an internal record, strictly observing at all times confidentiality and protection of personal data requirements.

8.4.6 Legality and process compliance

All Investigations will guarantee full compliance with the applicable legal framework and OW policies and procedures, as well as any other internal rules that apply.

8.5. Classification of the Report, Procedure Conclusion and Decision

Based on the examination and Investigation of each Report of alleged Breach, the CECO together with the assistance of the Polish Compliance Partner will send a decision proposal to the Channel Controller, which will issue the respective decision.

This decision can find the Report:

- a) **Warranted:** A Breach has been confirmed. A Report classified as "warranted" can lead to the presentation of recommendations to adopt the appropriate response measures.
- b) **Unwarranted:** The Investigation fails to confirm the existence of a Breach.
- c) **Inconclusive:** There is not enough evidence to confirm the existence of a Breach.

Where the findings of the Report classify it as warranted, the Channel Controller can adopt measures it deems appropriate considering the reported situation.

Information will also be provided on the measures planned, or that have already been taken within the legally provided terms for this purpose.

The procedure is concluded by registering the closing of the Report on the Speak Up Channel support tool, with the Reporting Person being duly informed.

9. Supervision and Communication

The Compliance Officer will regularly inform the Channel Controller about their activity related to the Reports considered.

Likewise, the Polish Compliance Partner will regularly inform the Boards of Directors of the Company of its whistleblowing related activity.

10. Final Provisions

The Polish Compliance Partner is in charge of reviewing this Policy whenever pertinent changes are made to the applicable legal framework or arise in the context of the activities conducted by Company, as well as when new factors arise that attest to their inadequacy. All proposed changes must be communicated to the CECO and submitted for approval to the Channel Controller and the Board of Directors of the Company.

The right to raise concerns under this Policy may not be waived or limited by any contract, policy, form or condition of hire, and the Company will never require such waiver or limitation of rights by any Stakeholder.

This Policy was established after internal consultations, in accordance with the process indicated in the Act.

This Policy enters into force within 7 days of its publication.

11. Distribution

This Policy is posted on OW website and on the following Company's website: **<https://www.bc-wind.pl>** and has been made available to persons working for the Company for their information.

12. References

COCOXX-OW-GEN-CMP-COD-00003	<u>OW Code of Ethics</u>
COCOXX-OW-GEN-CMP-POL-00005	<u>OW Complaint Management Policy</u>
COCOXX-OW-GEN-CMP-PRO-00005	<u>OW Complaint Management Procedure</u>

13. Annex I – External Channels of the Competent Authorities

- European Union
 - the European Anti-Fraud Office (OLAF),
 - the European Maritime Safety Agency (EMSA),
 - the European Aviation Safety Agency (EASA),
 - the European Securities and Markets Authority (ESMA) and the European Medicines Agency (EMA).
- Poland
 - Contact options dedicated to external reporting, provided by Ombudsman (RPO) or public authority

