THEON INTERNATIONAL
Advanced Optronics

Whistleblowing Policy

Date of entry into force	19.01.2024
Edition	1st

TABLE OF CONTENTS **Error! Bookmark not defined.**

1. Introduction

Fundamental commitment of Theon International PLC ("the Company") and the subsidiaries of the Theon International Plc group (collectively called “Theon Group”) is to maintain the highest level of ethics and professional conduct, by discouraging acts or omissions that may affect its reputation and credibility. Basic condition for the fulfillment of this commitment is the cultivation of open communication between the employees and the Company.

Given the above, the Company has developed a Whistleblowing Policy ("the Policy") which is in full compliance with the provisions of the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 (“the Directive”), on the protection of persons who report breaches of Union law.

The Company encourages and urges all employees of Theon Group to report violations, confidentially or anonymously as soon as they come to their attention and to express any concerns regarding any issue of violation as defined in the Directive.

All submitted reports will be taken into consideration and will be investigated with objectivity and strict confidentiality, according to the provisions of the Policy. The Company guarantees the protection of the reporting persons, whose reports fall within the Policy’s scope, prohibits any threat, attempt or act of retaliation and ensures the confidentiality of the reporting person’s identity as well as any third parties named in the reports.

2. Definitions

- **Breaches**: Illegal acts and omissions, as described in Paragraph 4 of the Policy.
- **Information on breaches**: Information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the Company.
- **Report**: The oral or written communication of information on breaches.
- **Reporting person**: A natural person who reports or discloses information on breaches, acquired in a lawful manner in the context of his or her work-related activities.
- **Person concerned**: A natural or legal person who is referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated.
- **Good faith**: The reasonable belief of the reporting person that the information they provide is valid and true.
- **Retaliation**: Any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person
- **Follow-up**: Any action taken by the recipient of a report or any competent authority, to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure
- **Feedback**: The provision to the reporting person of information on the action envisaged or taken as follow up and on the grounds for such follow-up

3. Purpose & Personal Scope

The purpose of the Policy is to ensure that the Company and Theon Group fully complies with the provisions of the Directive, regarding the protection of persons reporting breaches of Union law.

More specifically, the Policy's objectives are:

- The establishment of internal reporting channels.
- The establishment of appropriate internal reporting and monitoring procedures.
- Encouraging and promoting the disclosure of any breach within the Company.
- The establishment of a confidentiality and protection framework for the reporting persons.

The Policy applies to the Theon Group staff, regardless of their employment status and in compliance to the relevant laws applicable to each jurisdiction. It also extends to third party advisors, contractors and all levels of management within the organization.

4. Definition of Whistleblower

A whistleblower is defined as an employee, officer, consultant, intern, secondee or agent of Theon Group who reports or publicly discloses information on breaches acquired in the context of his or her work - related activities. Further, they perceive a need to avail themselves of protection against retaliation for having made the report. A whistleblower may choose to remain anonymous, but the Company encourages the whistleblower to report on a named, confidential basis.

5. What to Report

According to the provisions of the Directive, breaches of Union Law that are to be reported include the following, when they fall within the scope of the Company's activity:

- public procurement,
- financial services, products and markets, and prevention of money laundering and terrorist financing,
- product safety and compliance,
- transport safety,
- protection of the environment,
- radiation protection and nuclear safety,
- food and feed safety, animal health and welfare,
- public health,
- consumer protection,
- protection of privacy and personal data, and security of network and information systems,
- breaches affecting the financial interests of the Union and those relating to the internal market (as per article 2 of the Directive).

The material scope of the Directive (and perhaps the applicable national law, from case to case, transposing the Directive) do not cover:

- Disagreements regarding policies and decisions made by the Company's Management as far as they are compliant with national and Union legislation.
- Personal grievances
- Rumors
- Reports of breaches of the procurement rules involving defense or security aspects of the nation unless they are covered by the relevant acts of the Union.

- Reports of breaches of specific rules on the compulsory reporting of breaches of sector specific Union acts, such as in the sector of financial services, products and markets, and prevention of money laundering and terrorist financing.

Furthermore, false and malicious reports submitted in bad faith will not be investigated further.

6. Reporting

When a report is being filed (in person, in writing, online or by phone) please provide as much detailed information as you can to enable the Company to assess and investigate the concern. Information that can be included are the following:

- The background, history and the reason for the concern.
- Names, dates, places and other relevant information.
- Any documents that may support the report.

A report can be followed if it contains sufficient information or if there is a reasonable possibility of obtaining further information through an investigation.

All reporting is done confidentially. This means that information will only be shared with a limited number of people on a strict need to know basis. Information will be disclosed only if this is required by law or if a public interest is at stake. The reporting person's identity and any information from which the identity might be possible to be recognized will only be shared with people that are authorized to receive the information with the person's explicit consent.

6.1 Reporting Channels

The Company provides channels that enable named or anonymous reporting, in writing and orally, or in both ways. More specifically, the Company prompts reporting via:

- P.O. Box 5, Agios Antonios str. Muskita Building 2, 1st floor, Office/Apart. 102, 2002, Nicosia, Cyprus to the attention of the Compliance Officer, marked as "Confidential"
- Electronical email at Whistleblower@theon.com
- Orally, if requested by the reporting person, by holding a meeting with the appointed persons for receiving reports or by telephone or other voice messaging systems.

The Company encourages the submission of named reports, without excluding, of course, the option of anonymous reports. Anonymous reports, however, may be extremely difficult to be evaluated for their credibility and investigated thoroughly and efficiently.

6.2 Investigation process

The Compliance officer is the exclusive recipient of reports submitted through the established reporting channels and plays a central role in the investigating process. However, if the suspected irregularities pertain to the conduct of the Compliance Officer, the submitted report should be directed to the Chairman of the Audit Committee. The investigative process can be summarized as follows:

- Receiving and register keeping of reports.
- Confirmation of receipt of reports within seven days following their submission, in case the reports have been submitted on an eponymous basis.
- Evaluation of whether the reported breaches fall within the scope of the Policy.
- Evaluation of the credibility of the reports.
- Decision of whether a case needs to close or requires further investigation, either exclusively by the Compliance Officer, or by requesting the assistance of third parties, either from within the Company or externally.

- Provide feedback, in writing, to the reporting persons, regarding the progress of the investigation, within a reasonable time frame, which may not exceed (a) three months from the notification of receipt of the respective reports, or (b) if no receipt confirmation has been delivered to the reporting person, three months from the lapse of the prescribed seven day period for the delivery of the receipt confirmation, provided that the reports have been submitted on an eponymous basis.
- Decision of whether disciplinary measures need to be imposed, based on the result of the investigation process, and accordingly the competent Departments of the Company.
- Cooperation with the competent Authorities (Cypriot Police, the Attorney General of the Republic and the Independent Authority against Corruption, or any other competent authority as per the Theon Group entity jurisdiction), when required. In the case that the offense pertains to personal data then the Competent Authority might be the Commissioner for Personal Data Protection of the Republic of Cyprus (or any other competent authority depending on the Theon Group entity jurisdiction).
- Record keeping of the reports.

7. Confidentiality

The Company undertakes to take all appropriate measures, in order to protect the identity of the reporting persons and not to disclose it to anyone other than the staff members who are authorized to receive reports and investigate the reported cases, without their consent. The same applies to any other information from which the identity of the reporting persons can be directly or indirectly deduced.

However, the identity of the reporting persons, as well as any other information related to the reports, may be disclosed only when it is imposed by national law in relation to investigations by national authorities, judicial proceedings or safeguarding the right of defense of the persons concerned in the reports.

Disclosures made under the aforementioned derogation are subject to appropriate safeguards, according to the EU and national law. Reporting persons are informed before their identity is revealed, unless such information would jeopardize the related investigations or judicial proceedings. In that case, the Company shall provide an explanation for sharing the confidential data concerned.

7.1 Personal data protection

Company is dedicated to safeguarding personal data and privacy in accordance with the EU General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679**)** throughout the whistleblowing process:

- Personal data shall be kept confidential, used only for necessary purposes and access will be restricted to authorized individuals.
- Company shall maintain data security and demonstrate accountability in data processing.
- Personal data shall be retained as long as necessary and securely deleted when no longer needed.
- Individuals have rights over their data, such as access, rectification, and erasure, in compliance with GDPR.
- Third parties involved shall adhere to GDPR standards though data processing agreements.
- Whistleblower consent shall be sought before sharing data, and transparency in data processing will be maintained.
- GDPR requirements shall be followed in case of a data breach, including notifying supervisory authorities and affected individuals.
- Employees and involved parties shall be regularly trained in GDPR principles.

8. Protection measures

8.1 Prohibition of retaliation

Threats, attempts or acts of retaliation, in the context of this Policy, include the form of:

- suspension, lay-off, dismissal or equivalent measures
- demotion or withholding of promotion
- transfer of duties, change of location of place of work, reduction in wages, change in working hours
- a negative performance assessment or employment reference
- imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty
- coercion, intimidation, harassment or ostracism
- discrimination, disadvantageous or unfair treatment
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment
- failure to renew, or early termination of, a temporary employment contract
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income
- 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
- early termination or cancellation of a contract for goods or services
- Cancellation of a license or permit
- Deprivation of training
- Psychiatric or medical referrals
- Unilateral harmful change in working conditions

8.2 Measures for protection against retaliation

Theon Group is committed to preserving an environment of trust, transparency and open communication, where every person the Policy is addressed to, can express their concerns freely and without fear. Therefore, the reporting persons, even if they turn out to be mistaken, provided that the reports are submitted in good faith and not maliciously, are protected.

No act of retaliation is under any circumstances acceptable or tolerated and any relevant incident should be reported immediately to the Compliance Officer for investigation and resolution, along with any substantiating information. Theon Group takes all appropriate measures to restore the working environment and conditions of any employee who is found to have been subject to acts of retaliation. Additionally, any confirmed act of retaliation entails disciplinary measures.

It shall be noted that a Reporting person who reported or publicly disclosed information on breaches anonymously, but who are subsequently identified and suffer retaliation, shall nonetheless qualify for the protection provided herein.

The protection framework applies even if the reported breaches cannot be confirmed after the investigation process, unless the relevant reports are found to be submitted maliciously. Finally, the reporting persons remain accountable for any violations and omissions they are involved in, unrelated to the relevant submitted reports, according to the Company's policies and the applicable EU and national law.

8.3 Protection of the reported persons

The Company acknowledges the presumption of innocence of the persons concerned in the reports and is committed to provide for their protection, as it does for the reporting persons, throughout the investigation process.

8.4. Employees' training

Theon Group is committed to providing ongoing training to all its employees, focusing on compliance with the Whistleblowing Policy and fostering integrity and transparency values.

- Training sessions shall cover whistleblowing procedures, legal and ethical considerations, reporting mechanisms, and protection of whistleblowers.
- The Board shall oversee the training programme implementation, collaborating with relevant departments (e.g., Human Resources) to ensure access to meaningful training.
- Training content shall include policy procedures, legal obligations, and practical examples.
- The Board shall continuously monitor and adapt training programmes to stay relevant and effective.
- Periodic reports on training progress and effectiveness shall be shared with stakeholders to uphold transparency.

8.5 Review and Update of the Policy

The Audit Committee shall be responsible for keeping this Policy updated and in effect. The Policy shall be reviewed at least annually, aligned with regulatory changes, and consider feedback from stakeholders. An internal assessment and external expertise may be used when needed. Any necessary updates will be communicated to employees, and records of the review process shall be maintained.