



Whistleblowing Policy

Aksia Information Technology P.C.

Effective August 2024

Pursuant to the EU Whistleblowing Directive 2019/1937 regarding the protection of persons reporting violations of Union law as incorporated in Greece by Law 4990/2022, Aksia Information Technology P.C. (“Aksia IT”) has adopted the following “Whistleblower Policy” to establish procedures for reporting concerns, violations or suspected violations (“Report” or “Reports”) within Aksia of Law 4990/2022 or any other provision of law, rule, order, standard or prohibition prescribed by the Greek Law or any Greek authority. While Aksia does not encourage frivolous complaints, Aksia does expect all Employees to immediately report any potential violations of applicable law and inappropriate conduct, including the policies described in this Manual, as well as the Code of Ethics.

It is Aksia’s policy that its Employees may submit Reports of such information on a confidential and anonymous basis without fear of dismissal or retaliation of any kind. In addition, nothing in this Manual shall prohibit you from (i) providing truthful and complete information in response to a subpoena, in testifying in any action or proceeding or in connection with any regulatory inquiry, or (ii) communicating with any governmental agency, commission or self-regulatory organization, or otherwise participating in any investigation or proceeding that may be conducted by any governmental agency, commission or self-regulatory organization without notice to Aksia IT.

This policy provides a means whereby individuals can safely raise, at a high level, serious concerns and disclose information that an individual believes in good faith relates to violations of the Manual, Code of Ethics, or applicable law.

A. Reporting Persons Protected

This policy and its related procedures offer protection from retaliation against Employees who submit any Report with respect to perceived violations (referred to herein as a “Reporting Person”), provided the Report is made in good faith. “Good faith” means that the Reporting Person has a reasonably held belief that the Report made is true and has not been made either for personal gain or for any ulterior motive.

Aksia IT will not discharge, demote, suspend, threaten, harass, or in any manner discriminate or otherwise retaliate against any Reporting Person in the terms or conditions of his employment with Aksia IT upon such Reporting Person’s submitting in good faith any complaint regarding a violation of the Manual, Code of Ethics, or applicable law. Any acts of retaliation against a Reporting Person will be treated by Aksia IT as a serious violation of this policy and could result in dismissal.

B. Scope of Reports

Aksia encourages Employees and officers (“**Inside Reporting Persons**”) as well as non- Employees such as agents, consultants, vendors, service providers but also third parties who have relevant information about any unlawful acts concerning Aksia IT (“**Outside Reporting Persons**”) to report suspected wrongdoings.

C. Categories of Violations

The Report should be submitted for the sake of the public interest and fall within the scope of the Law, specifically in one of the following areas:

- a) Public procurement,
- b) Financial services, products, and markets, as well as the prevention of money laundering and terrorism financing,
- c) Product safety and compliance,
- d) Transportation safety,
- e) Environmental protection,
- f) Protection from radiation and nuclear safety,
- g) Food and feed safety, as well as animal health and welfare,
- h) Public health,
- i) Consumer protection,
- j) Protection of privacy and personal data, as well as the security of network and information systems,
- k) Violations affecting the financial interests of the Union (Article 325 of the Treaty on the Functioning of the European Union (TFEU)),

- l) Violations related to the internal market (Article 26(2) of the TFEU), competition rules, state aid, or ensuring tax advantages,
- m) Violations of all internal Aksia IT Policies as well as of policies that will be adopted by Aksia IT in the future,
- n) Violations of the Manual and Code of Ethics

Personal data not related to the conduct described in the report should not be included in the Report.

D. Safeguarding Anonymity

Aksia IT has established internal communication channels to enable Reporting Persons submit their Report either openly or anonymously. However, Aksia IT encourages Reporting Persons to openly submit reports, as this enhances the credibility of the Report's content and the Reporting Person's intentions, while also creating a communication channel both for further clarifications and to inform the Reporting Person on the Report's progress.

Aksia IT urges any Reporting Person that is considering making an anonymous complaint to strongly consider that anonymous complaints are, by their nature, susceptible to abuse, less reliable, and more difficult to resolve. In addition, Reporting Persons considering making an anonymous complaint should be aware that there are significant rights and protections available to them if they identify themselves when making a complaint, and that these rights and protections may be lost if they make the Report on an anonymous basis.

In responding to anonymous Reports, the below will be taken into account:

- a) The fairness to any individual named in the anonymous Report;
- b) The seriousness of the issue raised;
- c) The credibility of the information or allegations in the Report, with allegations that are conclusory or that do not have a specific factual basis being likely to receive less credence; and
- d) The ability to ascertain the validity of the complaint and appropriately resolve the Report without the assistance and cooperation of the person making the Report.

Reporting Persons, who initially reported anonymously, but were later identified, are protected from retaliatory measures, provided they meet the conditions specified in Article E of this Policy. Persons who report or publicly disclose information on breaches anonymously, but who are subsequently identified and suffer retaliation, shall nonetheless qualify for the protection provided.

E. Reporting Person's Protection

Aksia IT ensures that the Reporting Person is properly protected against possible negative consequences, such as threats or attempts of retaliation, or discrimination or any other form of unfair treatment. Furthermore, the Reporting Persons are fully protected against potential negative impact, in such cases where the assessment of the report does not reveal a Policy breach. Even when the investigation decides upon a justified violation and measures have been taken against the Reporting Persons, their protection is ensured against involuntary negative effects, irrespective of potential sanctions imposed by the competent bodies.

Revealing the identity of the Reporting Person may be required by a judicial or other legal procedure in the context of investigating the corresponding case. In particular, the Reporting Person shall be informed before their identity is disclosed, unless such information would jeopardize the related investigations or judicial proceedings. When informing the Reporting Person, Aksia IT shall provide an explanation for sharing the confidential data concerned.

Reporters are entitled to protection under the conditions that:

- a) They had reasonable grounds to believe that the information reported was true at the time of the Report,
- b) The reported information falls within the scope of the Law,
- c) They followed one of the alternative solutions provided by law to report the potential violation (i.e., internal or external Reporting, or public disclosure).

Any Report submitted with intent or purpose to cause harm will be treated as a serious matter that may lead to disciplinary actions, following the relevant Aksia IT internal policies and regulations and the

applicable provisions of labor law.

F. Confidentiality

The Whistleblowing Officer will exercise reasonable care to keep the identity of any Inside Reporting Person confidential and privileged under all circumstances to the fullest extent allowed by law, unless the Inside Reporting Person has authorized disclosure of his or her identity.

The Whistleblowing Officer will exercise reasonable care to keep the identity of any Outside Reporting Person confidential until it launches a formal investigation. Thereafter, the identity of the Outside Reporting Person may be kept confidential, unless confidentiality is incompatible with a fair investigation, there is an overriding reason for identifying or otherwise disclosing the identity of such person, or disclosure is required by law, such as where a governmental entity initiates an investigation of allegations contained in the Report. In such cases, Reporters are informed before the disclosure of their identity, unless such information would jeopardize the relevant investigations or legal proceedings. Furthermore, the identity of an Outside Reporting Person may be disclosed if it is reasonably determined that a Report was made maliciously or recklessly.

Personal data and any information directly or indirectly leading to the identification of the Whistleblower are not disclosed to anyone other than authorized individuals involved in receiving or monitoring Reports unless the Whistleblower provides explicit consent.

G. Procedure for Submitting Reports

Each Report should include: the main reason for submitting the Report (acts that may cause or have caused an incident worth reporting), with specific information (e.g. names, dates, location) and substantiation using relevant documents or other records. Evidence need not be included but any relevant information to facilitate the evaluation of the report will be considered.

In order to facilitate the proper examination and evaluation of submitted Reports, Aksia IT establishes an internal channel for the submission of Reports and has appointed Ms Domi Christodouloupoulou, Senior Compliance Associate, as the Whistleblowing Officer, responsible for receiving and monitoring the Reports.

The Whistleblowing Officer is responsible for receiving the various Reports and informing the Chief Compliance Officer of Aksia LLC on the Reports to be reviewed, in accordance with the provisions set out below. Where a Report has not been received through the whistleblowing platform, it will be recorded by the Whistleblowing Officer.

Reports may be submitted as follows:

- a) Through the compliance platform www.compliance.aksia.com or
- b) by mail to the Aksia IT address, namely Aksia Information Technology, Kapodistriou Avenue, 56, 14235, Athens, Greece, to the attention of the Whistleblowing Officer, marked "Confidential".
- c) in writing or orally directly to the Whistleblowing Officer.
- d) through External Reports as described in article 10 of this Policy

A meeting with the Whistleblowing Officer could also be scheduled in person, upon the request of the Reporting Person and within a reasonable timeframe (The meeting with the Whistleblowing Officer is mandated by Law if this is the Reporting Person's request).

H. Investigation of Reports

Upon receipt of a Report, the Whistleblowing Officer conducts an initial impartial assessment to determine the scope of the investigation and whether the violation falls within the scope of the Law (Article C of this Policy). The Whistleblowing Officer may close the reported case when the Report does not constitute a reportable behavior according to the terms of the Law and this Policy, or when there are no serious indications of the alleged violation, or when the Report was false, malicious, or submitted abusively.

Investigations will be conducted as quickly as practicable, taking into account the nature and complexity of the complaint and the issues raised therein. All Reports will be treated with objectivity, integrity, and confidentiality, according to the process outlined in this Policy. Aksia IT ensures that access to received Reports is restricted to authorized individuals handling Whistleblowing Reports.

In case the report has been submitted on an eponymous basis, the Whistleblowing Officer acknowledges receipt of the report within seven (7) days following its submission.

The Whistleblowing Officer is responsible for investigating and monitoring the Report, requesting further information as needed, and keeping the Reporting Person informed of the progress of the Report. The feedback to the Reporting Person shall be provided no later than three (3) months from the acknowledgement of receipt of the report or, if no acknowledgement was sent, three (3) months from the expiry of the seven-day period after the report was submitted.

If the submitted Report formulates objections against the Whistleblowing Officer, the Whistleblowing Officer registers the Report in the relative file and immediately forwards it to the National Transparency Authority (NTA) (Article K) as an external reporting channel, informing the Reporting Person.

The Whistleblowing Officer provides all available information to the Reporting Persons regarding the submission of Reports through the external channel, in accordance with Article K of this Policy. A Reporter who believes that their Report was not effectively addressed internally may resubmit the Report through the external channel.

The results of each investigation will be documented by the Whistleblowing Officer, which may then apprise other senior officers, and prompt and appropriate remedial action will be taken as warranted.

I. Personal Data and Retention of Reports

Any processing of personal data within the context of submitting and investigating a Report complies with the General Data Protection Regulation (GDPR) (EU) 2016/679, Law 4624/2019 supplementing the GDPR in the Greek legal framework, and Aksia IT applicable Privacy Policy.

The processing of personal data carried out in the context of investigating a Report takes place on the legal basis of fulfilling Aksia IT lawful obligation to establish and operate internal reporting channels and to take the necessary measures to monitor Reports, solely for the purposes of such processing.

Personal data not relevant to handling a specific Report will not be collected, and if collected, must be promptly deleted without undue delay.

Data Subjects have all the rights provided for by applicable legislation, as outlined in the current Aksia IT Privacy Policy. However, as far as the third parties named in a Report or resulting from monitoring measures are concerned, these rights may not be satisfied for as long as it is deemed necessary to prevent and counter attempts to obstruct the investigation of the Report, delay follow-up measures, or obstruct efforts to locate the Reporting Person, as well as the protection against retaliation. In case the Whistleblowing Officer denies the satisfaction of the rights of these subjects without informing them of the reason for the denial, they have the right to file a complaint with the Hellenic Data Protection Authority (HDPa) through its website, www.dpa.gr.

The Whistleblowing Officer will maintain all complaints received, tracking their receipt, investigation, and resolution. All complaints and reports will be maintained for a reasonable and necessary period and in accordance with Aksia's confidentiality and document retention policies.

Aksia IT will not disclose Reports submitted under this Policy to any third party. However, it may forward information received in Reports to the competent supervisory and investigative authorities, which may be used as evidence in administrative, civil, and criminal investigations and proceedings.

The Whistleblowing Officer will maintain all complaints received, tracking their receipt, investigation, and resolution. All complaints and reports will be maintained in accordance with Aksia's IT confidentiality and document retention policies.

J. Unsubstantiated Allegations

If a Reporting Person submits a Report in good faith pursuant to this Policy and any facts alleged therein are not confirmed by a subsequent investigation, no action will be taken against the Reporting Person. In submitting Reports, Reporting Persons should exercise due care to ensure the accuracy of the information reported. If, after an investigation, it is determined that a complaint is without substance or was made for malicious or frivolous reasons or otherwise submitted in bad faith, the Reporting Person could be subject to disciplinary action. Where alleged facts reported pursuant to this Policy are found to be without merit or unsubstantiated: (i) the conclusions of the investigation will be made known to both the Reporting Person, unless the complaint was submitted on an anonymous basis, and, if appropriate, to the persons against whom any allegation was made in the complaint; and (ii) the allegations will be dismissed.

K. External Reports

In certain cases, it may be more effective for the Whistleblower to report their concerns to an external entity. The official external entity is the National Transparency Authority (NTA), and the Report can be submitted:

- Through the electronic platform of the external channel of the National Transparency Authority: <https://extwhistle.aead.gr/#/>,
- Via email at: external.whistle@aead.gr
- In a sealed envelope marked "N. 4990/2022" or "Whistleblowing," either in person or by mail to the central offices of the NTA (Lenorman 195 & Amphiaraou 10442, Athens)
- Through a personal meeting, arranged at the request of the Whistleblower, at 213-2129870 or the email address external.whistle@aead.gr

L. Final Provisions – Adoption, Review and Update

This Policy has been approved and updated by the Chief Compliance Officer of Aksia LLC. The Whistleblowing Officer is responsible for communicating the Policy to the Aksia IT executives, staff and third parties, as necessary. For any questions or doubts regarding compliance with this Policy, you may consult the Whistleblowing Officer.