ETHICS CHANNEL OPERATING POLICY

APPROVED BY THE GOVERNING BODY:

Cristóbal Valderas Alvarado (Sole Administrator)

on behalf of:
ACS SERVICIOS Y CONCESIONES S.L.

June 2023

AMENDMENT CONTROL

VERSION – SECTIONS	REMARKS – DATE
V.0. Initial document	Prepared, supervised and approved by the CB in the Minutes of 24th March and by the Governing Body in 03/2022
V.1. Amendment of point 3.4. Suppression of *electronic mail as a whistle-blowing channel, and the distinction between ordinary and alternative channels.*	Prepared, supervised and approved by the CB in the Minutes of 3rd November and by the Governing Body in 11/2022
V2 – Review and adaptation to Act 2/2023, of 20th February, which regulates protection of persons who report on regulatory infringements and combating corruption. Reorganisation of the index, inclusion of a new point (3.3. On general principles) and suppression of the former point 3.8 What happens when a report is submitted through the other channels? to merge it into a single section.	Prepared, supervised and approved by the CB in the Minutes of 29th June and by the Governing Body in 06/2023

INDEX

1. PURPOSE AND OBJECT

The Governing Body of ZENIT LOGISTICS, S.A. (hereinafter ZENIT or the Organisation), has shown its determination by making the necessary decisions for effective implementation of a Compliance System in which its Ethics Channel is configured as the main axis within the Internal Information System on infringements.

The objective of the Ethics Channel is to receive and effectively process notifications regarding behaviour that, essentially, breaches the principles considered in its Code of Ethics and other documents that comprise its Integral Compliance Management System.

To that end, this Ethics Channel Operating Policy records the matters related to management and processing correspondence received, including a flexible, agile model pursuant to the legal regulations in force, best national and international standards and practices, through the channels potential whistle-blowers may use, without fear of reprisals or suffering harmful behaviour, to report events that imply infringement of the Compliance System.

This Policy, along with its internal development regulations, has the purpose of guaranteeing professional, confidential, impartial management, with maximum protection during the whole process, thus generating a feeling of confidence among the parties concerned.

In addition to the foregoing, this Policy contributes to strengthening the information culture within the Organisation, by encouraging use of adequate communication mechanisms to prevent and detect threats to the public interest.

Lastly, the Internal Information System has a System Manager (IISM), who is in charge of its management and diligently processing correspondence received, as set forth in this Policy and its internal development regulations.

2. SCOPE

This Policy is applicable to all the activities and compliance is mandatory for all members of ZENIT, regardless of the office or post they hold within the organisation, the juridical nature of their relationship and their geographic location.

On the other hand, the Policy shall be extended to third parties, business partners, foreign subsidiaries, non-controlled owned companies and, in general, any person who aims to report or provide information on the existence of any infringement related to ZENIT pursuant to the regulations in force.

3. OPERATING RULES

3.1. What may be reported?

Information on severe or very severe criminal or administrative infringements, in the ample sense, that is, reasonable suspicion, real or potential infringements, which have taken place or may probably take place, either by action or omission.

Pursuant to the regulations in force, one must report:

a) Any actions or omissions that may constitute breaches of European Union Law, pursuant to the terms set forth in the material scope of application of Act 2/2023, of 20th February, that regulates protection of people reporting regulatory infringements and combating corruption (hereinafter Whistle-blower Protection Act).

b) Actions or omissions that may constitute a severe or very severe criminal or administrative infringement.

c) Any other information on irregularities that may be determined pursuant to the terms established in this Policy.

For illustration, the following is a description of some possible matters to be reported:

- Bribery and corruption;
- Conduct against health and safety in the workplace;
- Conflicts of interest in any action related to personal performance;
- Discrimination, as well as sexual and labour harassment;
- Internal fraud;
- Cases of unfair competition;
- Breaches in matters of defence of competition;
- Undue use of the company's assets;
- Conduct that endangers the health and safety of our users;
- Irregularities in tax or accounting matters, or that compromise the integrity of the business and financial records.

- Disclosure of information when such disclosure may affect the interests of ZENIT or legitimate rights of third parties;
- Cyber-attacks;
- Acts that harm the environment or breach the regulations on town planning and territorial organisation matters;
- Actions against human rights;
- Among others.

3.2. What channels are available?

ZENIT provides the following **internal channels** to be able to submit the reports this Policy covers:

- Our means to receive them are the telematic ones (*), accessible through the web, as well as the 24 hour, 7 day a week telephone channel, that are recorded on the web page of the application EthicsPoint, by the external provider Navex Global Inc. **https://compromiso.ethicspoint.com**
- Direct superior or a member of the company management.
- Member of the Compliance Body.
- By postal mail to the attention of:

  Canal Ético (Ethics Channel)

  Parque Empresarial Vía Norte

  C/ Quintanavides, 19, Edificio 4- Plta. 2ª

  C.P. 28050 – MADRID

(*) Use of the telematic channels shall be encouraged as, due to matters of security, confidentiality and integrity of the content of the communication, these are more recommendable.

Any severe or very severe infringement report received by any other additional channel at ZENIT shall be managed according to the internal regulations.

In addition to the internal channels, any possible whistle-blower has an **external channel** available, provided by an Independent Whistle-blower Protection Body, or channels of the regional bodies, or even those of the European Union that are

constituted for that purpose. Information may be submitted to such an Independent Authority or relevant body on any actions committed or omissions included within the scope of the law mentioned, either directly, or by notification through the internal channels described above.

On the other hand, it has **external channels** managed by other authorities, which may be resorted to according to the nature of the infringement to be notified, such as, among others:

- In matters of defence of competence - Authority: *CNMC* (*Spanish Competition Authorities*)
- In Stock Exchange related matters – Authority: CNMV (*Spanish National Stock Exchange Commission*)
- In money laundering matters – Authority: SEPBLAC (*Money Laundering Authorities*)
- In tax infringement matters – Authority: AEAT (*National Tax Authorities*)

3.3. On what general principles is the Ethics Channel based?

- **Principle of confidentiality**:

Processing both the identity of the parties acting, as well as related information provided, shall be governed by this principle.

All persons legitimated to participate in the proceedings, including their investigation, must maintain confidentiality of the information received or made known to them. Thus, they may not disclose information known in exercise of their functions to third parties, especially that related to personal data.

The exception to the preceding paragraph is related to the need to share information with persons involved in the case, respecting the need to know principle in cases in which this is strictly necessary and legitimate.

- **Principle of objectiveness and impartiality**

The absence of conflict of interest shall be assured during the course of the

proceedings.

- **Principle of presumption of innocence**

Any *party reported* is entitled to be treated as if they were innocent, until, if appropriate, it is proven that an *Infringement* has been committed and it is appropriate to impose a penalty.

- **Principle of proportionality**

This principle is due to the need for any action carried out by during the procedure not to be performed in a random or disproportionate manner.

3.4. When must it be reported?

It must be reported when the whistle-blower has reasonable cause to believe that the information being provided is true and liable to be considered an infringement or non-compliance. The report must always be submitted in good faith.

3.5. What happens in urgent cases?

Processing reports considered through the different channels ZENIT has available requires performance of an initial classification, according to the severity and critical nature of the content, so their processing may be prioritised.

It is recommendable in urgent cases, and as long as the context allows, to make sure to inform one's hierarchical superior, the IISM and/or the Regulatory Compliance Management at ZENIT as soon as it is possible, in order to deal with the matter in the most efficient way possible in keeping with what is provided in the management procedure.

3.6. What information must I provide when reporting?

ZENIT appreciates the information received being the most complete, detailed, and true as possible. And due to this it asks that, in the event of reporting, you share all the information known to the whistle-blower, or available in relation to the possible infringements. The text or message must be clear, being able to provide any proof or document to back the report. This allows ZENIT to be able to carry out case management in the quickest, most effective way possible.

3.7. Do I have to identify myself when reporting?

It is not necessary. The Ethics Channel at ZENIT allows reports to be submitted anonymously.

Notwithstanding this, in the event of submitting a report in which your identification, post or relationship and contact data are provided, the personnel in charge of processing may contact the whistle-blower for follow-up if necessary. In that sense, ZENIT does not allow reprisals to be taken when reports are made in good faith.

3.8. What happens when a report is submitted?

In the case of using telematic channels, ZENIT uses a safe server to support administration of such channels, in keeping with what is required by the applicable regulations. Reports through the channels are saved directly on the server, which is extremely secure.

The server allows the whistle-blower:

- To specify the place, date, company affected, as well as the persons related to the report.
- To opt for anonymous communication.
- To be able to attach supporting documentation to the report or notification to justify its content.

On submitting the report through such *telematic channels*, the server shall provide the person reporting a case number, as well as an exclusive personal password. The case number and password allow the whistle-blower to be able to initiate a session on the whistle-blowing website to be able to obtain comments and/or updates on their report. The system will allow the whistle-blower to provide additional information to amend or complement their report.

It is important to emphasise that the server only transfers the reports to specific persons within ZENIT who are authorised to manage them. Likewise, the internal team that handles the documents produced receives training on how to manage the documents and reports effectively, as well as the way to assure their confidentiality.

ZENIT shall acknowledge receipt within a term of seven days, from when it has a record of effective receipt of the notification, and as long as it is possible to provide such acknowledgement of receipt.

Once the acknowledgement of receipt has been given, and if the whistle-blower has provided identification, ZENIT may contact the person reporting directly to

provide them comments and updates.

Processing the report shall be settled within a reasonable period, not exceeding three months from acknowledgement of receipt, a term that may be extended to six months in cases of special relevance or complexity.

The principle of action is that, when there are sufficient signs regarding a possible infringement that arises from, or may lead to severe or very severe infringements, either criminal or administrative, an investigation shall be initiated pursuant to the internal procedure established for the purpose.

ZENIT shall provide the whistle-blower information on the report and, as far as possible, the result of evaluation of the matter. One must bear in mind that, in some cases, for security reasons or the integrity of the investigation, there may be limitations regarding updates on the report that may be provided, according to the progress of its internal procedure.

Protection of the parties involved may involve adopting reasonable accompaniment and support measures to avoid harm being caused and to guarantee the principles arising from this Policy, as long as they have acted in good faith.

3.9. What is the prohibition on reprisals?

ZENIT does not tolerate any kind of reprisal. This includes threats, or any other means to make the person reporting events this Policy involves in good faith afraid.

Protection against reprisals also includes persons who, in good faith, report possible infringements externally to the competent authorities. The prohibition on reprisal in this Policy covers the following persons:

1. Any third party related to the whistle-blower (such as colleagues and relatives) who may suffer reprisals in the labour context.

2. Any person who has helped the whistle-blower in the reporting process.

3. Any legal entity that the whistle-blower is the owner of, where they may work, or that is in any other way related in a labour or professional context.

The prohibition of reprisals covers any act or omission, direct or indirect, that may harm a whistle-blower due to reporting possible infringements in good faith. For example, ZENIT shall not take any of the following measures against whistle-blowers due to presenting a report in good faith:

1. Suspension, dismissal, demotion or equivalent measures.
2. A negative performance evaluation.
3. Refusal of promotion.
4. Unjustified changes of place of work, salary reduction, change in working hours.
5. Coercion, threats, harassment or ostracism.
6. Discrimination, disadvantaged or unfair treatment.
7. Not renewing, or early termination of a temporary labour contract.
8. Damage, even to the person's reputation, in particular in the social media, or financial losses, including loss of business or loss of income.
9. Early termination of a goods or service contract.
10. Cancellation of a permit.
11. Among other measures that may be considered reprisals.

In the event of any person at ZENIT directly or indirectly taking reprisals against this Policy, ZENIT itself shall take the necessary measures to ensure the reprisals cease as soon as possible and, when appropriate, shall take disciplinary measures against those responsible for these.

3.10. What must we understand as good faith by the company and the person reporting?

From the point of view of the whistle-blower, good faith requires the report to be made with at least reasonable causes to believe the information provided on possible infringements was true at the moment of reporting.

From the point of view of the company, this involves not adopting any reprisal due to the fact of a report being presented, as well as it is protecting the confidentiality and personal identity of the whistle-blower in all cases and with the sole exception of the Law, in its different modes, requiring this to be notified to a judicial or administrative authority.

3.11. Is my personal data protected?

Yes, it is protected.

ZENIT undertakes to maintain strict protection of privacy, security and data conservation, as detailed in our policy created for the purpose and published on our website.

These rules are also applied regarding all the personal data related to reports made pursuant to this Policy.

3.12. Who are the receivers of my personal data if I submit a report?

The data collected in the context of a report submitted may be processed or notified to the following parties when necessary:

- Navex Global, Inc., the independent third party that manages the telematic whistle-blowing channels as data processor.
- The Internal Information System Manager, as well as the Compliance Body of ZENIT.
- Authorised representatives of ZENIT who intervene in the investigation, if the nature or scope of the facts reported requires their participation.
- Investigator, advisor, or external consultant hired to support ZENIT in evaluation of the notification, the investigation of the matter, or to advise ZENIT regarding the matter.
- Public Prosecutor, Judicial Authority, the police and/or other legal regulatory or enforcement bodies.

3.13. What is the legal basis for processing my personal data?

Processing personal data within the framework of the whistle-blowing channel has the legal basis of compliance with a legal obligation of the Company, pursuant to Act *2/2023, of 20th February, that regulates protection of persons who report regulatory infringements and combating corruption,* to have an internal information system on irregularities.

Thus, processing the personal data on the person reporting, or the persons reported

to, is that strictly necessary to manage the report and comply with the aforementioned legal ends and obligations. Under no circumstance shall ZENIT perform automated decisions based on the data submitted.

3.14. What data is collected, how is it kept and for what purpose is it processed?

Purpose for which ZENIT processes the personal data

At all times, only the strictly necessary personal data shall be processed in order to manage, process and investigate reports on commission of irregularities or acts contrary to ethics, legality or the corporate regulations of ZENIT and to carry out the necessary actions to investigate the facts reported, including, where appropriate, adoption of the relevant disciplinary or legal measures. The personal data shall not be used for a purpose other than that stated.

Personal data collected by ZENIT

In processing the reports made pursuant to this Policy, ZENIT collects the following personal data and information provided when submitting a report and throughout its investigation:

- Name and contact data (unless reported anonymously) and if a ZENIT employee.

- Name and other personal data of the persons mentioned in the report, if that information is provided (that is, description of the functions and contact data).

- Any data or information included in the report that may identify a specific person.

Conservation of personal data

ZENIT shall keep a register of all the reports received. These records and the personal data they contain shall be kept confidentially.

The records shall be conserved for all the time necessary to comply with any legal requisite that is applicable from time to time and, under no circumstance, for a term exceeding ten (10) years.

In particular, ZENIT shall conserve the personal data of the whistle-blower for the essential time to decide on whether it is appropriate to commence an investigation of the facts or conduct reported and, once this is decided, it shall be deleted from the Ethics Channel, and may be processed outside the system to investigate the events for the necessary time until conclusion thereof. Once the investigation of the notification is completed and, if appropriate, the necessary actions are taken, the data from reports that have been processed shall be kept blocked to comply with the appropriate legal obligations in each case.

In all cases, the personal data shall be deleted from the Ethics Channel within the maximum term of three (3) months from being input, except if conserved for an additional term due to being necessary to fulfil the legal and corporate obligations, and may not continue to be processed outside the Ethics Channel in the case of not having concluded investigation of the report, for the necessary time until its conclusion.

If it is decided not to proceed with a report submitted, the information may be kept in anonymised format.

3.15. What are the rights of the person reporting in data protection matters?

As whistle-blower, the person reporting may exercise access to their personal data attorney time and under the terms set forth in the applicable regulations.

Should that person believe the data is not correct or is incomplete, they may request correction thereof pursuant to the applicable legislation. They may apply for deletion of data that is no longer necessary, except in the event of there being a legal obligation to conserve such.

Moreover, they may request that processing of their personal data be limited, oppose such, or request portability of their data and they shall be entitled to withdraw their consent.

To that end, they must submit a written application to **rgpd-zenitlogistics@zenitlogistics.es** with prior due proof of their identity by a legally valid means, stating "Exercise of Rights" in the subject and specifying the right they wish to exercise.

In the event of not having achieved satisfactory exercise of their rights, they may submit a complaint to the Spanish Data Protection Agency.

More information is available in the Privacy Policy available in the Ethics Channel section of the corporate web site.

4. ENFORCEMENT, TERM NOTIFICATION AND REVIEW

This Policy shall come into force right on the date of approval, amendment, or update of this document.

It shall be published and distributed for adequate knowledge, being made available for consultation through the corporate website.

In ordinary circumstances, ZENIT shall review its content with the frequency established in its documented information system and, under extraordinary noes, when significant circumstances of a legal, organisational nature arise, or any other that may require its immediate adaptation and/or updating.