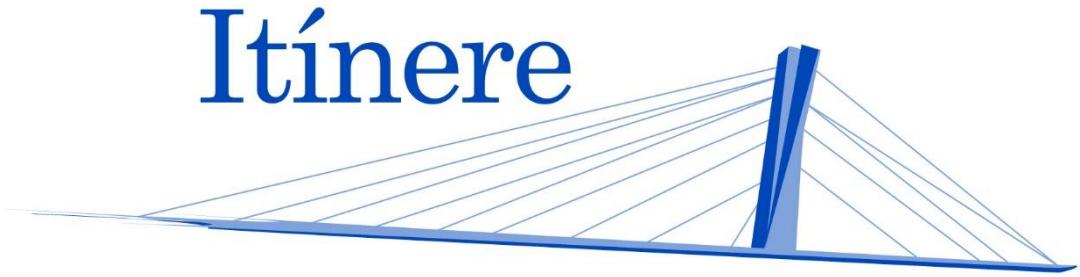


# ITINERE GROUP'S INTERNAL WHISTLEBLOWER PROTECTION AND REPORTING SYSTEM

| V. | Made by | Reviewed by | Approved by | Date | Status |
|---|---|---|---|---|---|
| 1.0 | CCO | Compliance Unit | Board of Directors | 10/12/2025 | Active |

**ITINERE GROUP'S INTERNAL WHISTLEBLOWER PROTECTION AND REPORTING SYSTEM**

Communications management and whistleblower protection policy

**1. Introduction.**

Itínere Infraestructuras, S.A. (hereinafter, "ITÍNERE") is the parent company of a large infrastructure operating group made up of legally autonomous companies which are dedicated, in the main, to the operation of roads and other activities directly or indirectly related therewith (hereinafter, when referring to any of these entities, the term "Company" will be used and when referring to all of them as a whole, the "ITÍNERE Group" or "Group").

Law 2/2023 of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption ("Law 2/2023") - which transposes Directive (EU) 2019/937 of the European Parliament and of the Council of 23 October 2019, into Spanish law - determines, inter alia, the obligation for legal entities in the private sector with fifty or more employees to have an Internal Reporting System under the terms provided for therein, as well as to put into place protection measures for those who report internally on the actions or omissions contained in article 2 of Law 2/2023. ITÍNERE has developed this Policy for the management of the internal whistleblower protection and reporting system ("IIS" in Spanish), (hereinafter "the Policy") in compliance with articles 5.2.h), 5.2.i), 9 and 11 of the aforementioned Law 2/2023, which include the general principles regarding the Internal whistleblower protection and reporting System, determining, through this Policy, certain corporate standards applicable in the ITÍNERE Group.

This Policy forms part of the internal regulation of the Compliance area of the "GROUP". It has been approved by the Board of Directors of Itínere Infraestructuras, S.A., availing itself of its duty to determine the general policies and strategies of the entity and the Group, in accordance with the provisions of its Internal Regulatory Framework.

Law 2/2023 explains and clarifies in its preamble, part III, that its purpose is to protect from possible reprisals anyone who, in an employment or professional context, detects serious or very serious criminal or administrative offences and reports them through the mechanisms regulated therein.

To this end, Law 2/2023 requires any body bound by this law to have a preferential channel for reporting the actions and infringements referred to in the law itself, known in said law as the "internal reporting system". It also obliges each body to have a policy or strategy that sets out the general principles of the internal whistleblower protection and reporting system. This policy should be well publicised within each organisation and agency.

Since 2019, the ITÍNERE Group maintained a communications channel, known at a corporate level as the "Compliance Channel", as well as a policy for its use. This was duly adapted to the requirements deriving from Directive (EU) 2019/937 of the European

Parliament and of the Council of 23 October 2019, regarding the admission of anonymous complaints. Both the communications channel and its usage policy are available to the public at the Company's corporate websites and, as regards those which do not make this available, through the ITÍNERE Group's website at www.grupoitinere.es.

**2. Purpose and scope of application.**

2.1. The purpose of this Policy is to put into place protection measures for those who report breaches of applicable law, the ITÍNERE Code of Conduct and the Regulation.

The Compliance Channel is ITÍNERE's internal reporting system and it is the ideal mechanism for communicating any action or omission that infringes the Code of Conduct, any of the Internal Corporate Policies or which is contrary to the legislation applicable to professional activity, allowing feedback to be provided to the whistleblower.

The scope of application of Spanish jurisdiction includes, inter alia, the infringements provided for in article 2 of Law 2/2023, i.e. certain infringements of European Union law of a criminal nature or of a serious or very serious administrative nature.

The Policy on the use of the Group's Compliance Channel is now in force. This document sets out to strengthen the culture of internal communication of infringements at ITÍNERE, formalising the provisions established in Law 2/2023 on the Internal reporting and communications management System.

In this context, the Policy will apply to ITÍNERE and to all companies in which the Group has a direct or indirect shareholding of more than 50% or over which the Group has management control, without prejudice to their separate legal personality and the autonomy and independence of each Company. Compliance will be obligatory for all members of Senior Management, employees and directors of ITÍNERE Group companies in all activities deriving from their position or post in the Group.

The CHIEF COMPLIANCE OFFICER is the person responsible for ITÍNERE's internal reporting system.

His/her appointment or removal by the Board of Directors of ITÍNERE will be notified to the Independent Authority for the Protection of Whistleblowers pursuant to the provisions of the law, in particular article 8.3 of Law 2/2023.

Each Group company that is under the scope of application of Law 2/2023 shall appoint its own Internal Reporting System Manager, in compliance with the provisions of Law 2/2023, who shall ensure compliance with the principles set forth in this Policy, notwithstanding the fact that this “IIS” (in Spanish) policy shall be directly applicable to all Group companies as soon as it has been approved by the administration body.

Notwithstanding the foregoing, the person responsible for the Company's Internal Reporting System may be the same as the person appointed by ITÍNERE.

This Policy shall prevail over any other Internal Regulations at an executive level which it may clash with, as far as the subject matter it regulates is concerned.

**3. General principles.**

3.1. The ITÍNERE Group carries out its activity based on the principles of:

- Integrity. Law 2/2023 defines the person responsible for the internal reporting system as the natural person designated by the administration body of the entity as the person responsible for the management of said system. At ITÍNERE, the internal whistleblower protection and reporting System is configured by the Compliance Channel, its usage protocol, with the Chief Compliance Officer being the manager responsible in this regard.
- Prudence in risk management.
- Transparency.
- Achievement of a profitable and sustainable business in the long-term.
- Compliance with the legislation applicable at any given time.

3.2. In this context, the present Policy sets out the essential operating principles of the ITÍNERE Compliance Channel:

- It is open: it allows any interested party to report, even anonymously, any actions or omissions which, in their opinion, constitute a regulatory infringement.
- It allows for anonymity, guaranteeing the confidentiality and the rights of the whistleblower, the person concerned and any third party: the Compliance Channel is designed in such a way as to safeguard the anonymity (should this be the wish of the whistleblower) or, as the case may be, the confidentiality of the whistleblower, preserving his or her identity, as well as the confidentiality of the information provided, of the actions carried out in the management and processing of the communication, protecting in all cases the rights to the presumption of innocence, respect for the honour and defence of the person concerned and third parties.
- Personal data protection: the processing of personal data that takes place in ITÍNERE's internal reporting system will be carried out in accordance with the applicable regulations on the protection of personal data. The Data Protection Officer for the purposes of the Internal Reporting System is the person designated by ITÍNERE, without prejudice to the fact that, pursuant to the legislation in force, each company must officially designate him/her vis-à-vis the AEPD.
- Autonomy and independence: ITINERE's Chief Compliance Officer, as the person responsible for the operation of the Compliance Channel, carries out his or her function with autonomy and independence, relying on the Compliance Unit for the management thereof.
- Non-retaliation and protection: those who use the ITÍNERE Compliance Channel in good faith enjoy protection from any retaliation and possible adverse consequences arising from their communications, as set out in the Compliance Channel Usage Policy.
- Reporting security and protection: ITÍNERE's Compliance Channel has specific measures in place for the protection and security of information, preventing access by any unauthorised staff.

**4. Provisions of the Policy**

a. General provisions.

The ITÍNERE Compliance Channel allows for the reporting of any Regulatory Breaches. In accordance with article 4 of Law 2/2023, ITÍNERE puts this communications channel at the disposal of any stakeholder so that they can report, preferentially over any external channels, potential breaches of:

1. Any breach of the principles set out in the Code of Conduct;

2. Non-compliance with the ITÍNERE Group's Regulatory Compliance Management System or with any internal rules on ethics and compliance;

3. Acts or conduct that may have criminal implications;

4. Serious or very serious administrative infringements;

5. Infringements of labour law in the field of health and safety at work;

6. Any act or omission which may constitute an infringement of European Union law provided that:

a) they fall within the scope of the acts of the European Union listed in the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019;

b) they affect the financial interests of the European Union as referred to in article 325 of the Treaty on the Functioning of the European Union (TFEU); or

c) they affect the internal market, as referred to in Article 26, section 2 of the TFEU, including infringements of European Union rules on competition and aid granted by States, as well as infringements relating to the internal market in relation to acts that violate corporate tax rules or practices whose purpose is to obtain a tax advantage that distorts the object or purpose of the legislation applicable to corporate tax.

7. Any other type of irregularity that could imply liability for the ITÍNERE Group or any of the companies going to make up the ITÍNERE Group.

In addition, the Internal Reporting System may also be used to raise any doubts or queries regarding this specific policy or any of those in force and forming part of the set of corporate policies that must be complied with.

Pursuant to the Policy on the use of the Compliance Channel, the Chief Compliance Officer is responsible for receiving and processing the communications received through the Compliance Channel, guaranteeing independence and absence of conflicts of interest.

b. Communications management procedure. The internal process for receiving and processing communications on the ITÍNERE Compliance Channel will be carried out in accordance with the provisions of the Compliance Channel Usage Policy.

When the facts reported could be indicative of a criminal offence, the information received shall be forwarded immediately to the Public Prosecutor's Office. If the facts affect the financial interests of the European Union, a referral shall be made to the European Public

Prosecutor's Office. Said provision of information shall respect the rights of the persons concerned under the Constitution and applicable law.

The information will be analysed by the Chief Compliance Officer, who will promote its management, having at his disposal all the areas and addresses to fully review the reported facts. Information will only be shared with those areas whose knowledge is necessary for the proper investigation of the reported facts. Where necessary for the proper conduct of the investigation, the whistleblower may be contacted at any time for the purpose of amplifying or clarifying information. ITÍNERE's communications channel allows two-way communication with the whistleblower, even if the information has been sent anonymously in accordance with the provisions of the Compliance Channel Usage Policy.

In accordance with the provisions of ITÍNERE's Code of Conduct, all employees or areas involved in the management of information must maintain the confidentiality of the actions related with this process.

c. Protective measures for the whistleblower.

- Integration of communication mechanisms: at ITÍNERE, the Compliance Channel is not the only internal channel for communicating Regulatory Infringements; for the purposes of this policy, communication by any means will be considered to be that which takes place, without prejudice to the need to leave a written record of the communication for the purposes of evidence and to initiate the management of the communication received (for example, phone communications will require a transcription of the communication and the signature of the whistleblower). Said communications may not be relevant for these purposes:
    - a) when the facts stated are not at all plausible or are manifestly unfounded;
    - b) where the communication fails to contain any new and/or significant information in comparison with a previous communication that has already been handled internally.
    - As stipulated in the ITÍNERE Code of Conduct, the Subjects subject to this Code are obliged to report any behaviour which deviates from the provisions of the Code or which could violate any Internal Regulations and/or applicable legislation in force. In compliance with article 9.2. g) of Law 2/2023, the recipient of any communication regarding potential Regulatory Infringements must promptly forward said information through the ITÍNERE Compliance Channel.
- Non-retaliation: as established in the ITÍNERE Code of Conduct and the Compliance Channel Usage Policy, those who make communications in good faith will not be subject to retaliation or suffer any other adverse consequence owing to this communication. Retaliation or attempted retaliation may lead to disciplinary action in accordance with Internal Regulations and applicable labour law, in addition to any other applicable liabilities.
- Protection of the whistleblower's identity and prevention of conflicts of interest: the Compliance Channel manager will keep the whistleblower's identity confidential and it will only be shared with those areas of ITÍNERE whose cooperation is essential for the investigation work. Furthermore, only those areas of ITÍNERE will be involved

in which there are no conflicts of interest, present or potential, and mitigation measures will be adopted when they are identified.

- Dissemination of information on competent authorities: ITÍNERE provides the whistleblower with clear and accessible information on the external channels for reporting to the competent authorities and, where appropriate, to the institutions, bodies, offices or agencies of the European Union.
- Information about how it works: ITÍNERE publishes information on the operating principles of the Compliance Channel through the publication of its Usage Policy. It also carries out training and awareness campaigns on its existence and the rights it guarantees.
- Ease of access and use: it is accessible from any device and allows for written or oral submissions.

All of the above means that:

Regarding non-retaliation: those who make the communication in good faith and have reasonable grounds to believe that the information is truthful, even if they do not provide conclusive evidence, and fall, inter alia, into one of the following categories set out in Law 2/2023 itself, will be protected from retaliation:

a) those who are employees of any of the ITÍNERE Group companies.

b) public employees and civil servants.

c) those who are suppliers of ITÍNERE.

d) shareholders, stakeholders and persons belonging to the administration, management or supervisory body of an undertaking, including non-executive members.

e) anyone working for or under the supervision and management of contractors, subcontractors and suppliers.

f) those who report information about information obtained within the context of an employment or statutory relationship that has already ended, volunteers, trainees, workers undergoing training, whether or not they receive remuneration, as well as those whose employment relationship has not yet begun, in cases where the information on infringements has been obtained during the selection process or pre-contractual negotiation.

g) legal representatives of the employees during the course of their duties of advising and supporting the whistleblower.

h) natural persons assisting the whistleblower in the process.

i) natural persons related with the informant and who may suffer reprisals, such as co-workers or family members.

j) legal persons for whom he/she works or with whom he/she has any other relationship in an employment context or in which he/she has a significant shareholding. For these purposes, any interest in the capital or in the voting rights pertaining to shares or stakes is

deemed to be significant when, by dint of its proportion, it enables the holder to have the capacity to influence the legal person in which the interest is held.

Retaliation concept: in addition to that which has already been provided for in the Compliance Channel Usage Policy, for the purposes hereof, retaliation is deemed to be any action taken to the detriment of those who make a communication that qualifies them as a whistleblower and as a consequence thereof. In this regard, retaliation is deemed to be any action regarded as such under the applicable legislation, and specifically the following:

a) Suspension of the employment contract, dismissal or termination of the employment or statutory relationship, including non-renewal or early termination of a temporary employment contract after the trial period, or early termination or cancellation of contracts for goods or services, the imposition of any disciplinary measure, demotion or denial of promotion and any other substantial modification of working conditions and failure to convert a temporary employment contract into a permanent one, where the employee had legitimate expectations that he/she would be offered a permanent job; unless these measures were carried out during the regular course of managerial powers under the relevant labour legislation or legislation regulating the respective public employee statute, due to circumstances, facts or breaches that are proven and unrelated with the submission of the communication.

b) Damage, including reputational damage, or economic loss, coercion, intimidation, harassment or ostracism.

c) Negative evaluation or references regarding work or professional performance.

d) Blacklisting or dissemination of information in a particular sectoral area, which hinders or prevents access to employment or the contracting of works or services.

e) Cancellation of a licence or permit.

f) Denial of training.

g) Discrimination, or unfavourable or unfair treatment.

d. Protective measures for the person (s) concerned.

- Right to the presumption of innocence, honour and defence of the people concerned: during the course of processing any communications received by ITÍNERE, the right to the presumption of innocence, honour and defence of the person(s) concerned will be respected, in accordance with the provisions of Law 2/2023 and the Policy on the use of the Compliance Channel and, at all times, the good name (s) of the person (s) concerned will be preserved.
- Right to information and to be heard: the person to whom the actions or omissions that could constitute an infringement are attributed shall be entitled to be informed in the time and manner deemed appropriate to avoid the destruction, concealment or alteration of evidence and to ensure the proper conduct of the investigation in accordance with the provisions of the Policy on the use of the Compliance Channel.

e. Personal data protection.

Compliance with personal data protection regulations upon the receipt of communications and the management thereof is subject to the provisions of the applicable regulations:

Law 2/2023 of 20 February on the protection of persons who report regulatory infringements and the fight against corruption.

Regulation (EU) 2016/679 issued by the European Parliament and the Council on 27 April 2016 pertaining to the protection of individuals with regard to personal data processing and the free movement of said data.

Organic Law 3/2018 of 5 December on Personal Data Protection and the Guarantee of Digital Rights.

Accordingly:

- The Internal Reporting System should prevent unauthorised access and preserve the identity and ensure the confidentiality of the data pertaining to the persons concerned and to any third party mentioned in the information provided, especially the identity of the whistleblower if he/she has been identified. The identity of the whistleblower may only be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or disciplinary investigation, with these cases being subject to those safeguards laid down in the applicable regulations.
- If the information received contains special categories of personal data subject to special protection, it will be deleted forthwith, unless the processing is necessary on the grounds of essential public interest as provided for in Article 9.2.g of the GDPR, as provided for in Article 30. of Law 2/2023.
- In any case, personal data whose relevance is not evident to process specific information will not be collected or, if collected by accident, will be deleted without undue delay.
- Communications that have not been processed may only be recorded anonymously, without the blocking obligation being applied as foreseen in article 32 of the Organic Law on Personal Data Protection and Guarantee of Digital Rights (LOPDPGDD).

The principles and provisions set out in ITÍNERE's Data Protection Policy must also be complied with.

**5. Governance, review and monitoring model of the Policy.**

5.1. This Policy was drawn up and coordinated by the Compliance area, having been approved by the Board of Directors of ITÍNERE on December, the 10th, 2025.

The heads of the different areas/departments of ITÍNERE companies will provide, in their respective areas of responsibility and where appropriate, sufficient means, systems and organisation to comply with the provisions of this Policy. Control over the degree of compliance both with this Policy and with its implementing regulations will be carried out in accordance with the Internal Control Model determined by the ITÍNERE Group, based on three independent lines of defence.

The Management Body will carry out, directly or through the Compliance Unit, supervision of the application of the Policy, on the basis of periodic or ad hoc reports received from the Chief Compliance Officer of the ITÍNERE Group.

At least once a year or upon the occurrence of any event requiring changes to this Policy, the Compliance Unit will see to a revision thereof at the request of the Chief Compliance Officer, who will submit it to the consideration of ITÍNERE's Board of Directors, unless the modifications are necessary owing to an adaptation to any regulations which may be in force and applicable, in which case they will be carried out by the Compliance Unit without the need to previously submit said changes to the administration bodies.

**6. Coming into force and term of validity.**

The Policy shall take effect as from the day after its approval by the Board of Directors. Its term of validity is indefinite. This Policy shall remain in force until such time as it is amended by the Board of Directors or a new policy is approved to replace it.

**7. Interpretation.**

The ITÍNERE Group Compliance Unit is the only body recognised as having the capacity to interpret the terms or application of this policy. Its judgement in this regard will receive the same publicity as this policy.