

Ethical Channel Policy

Document No.:	ISADAK/CS/CS013	Page No.	1 of 8
Issue No.	01	Issue Date	28 June, 2024
Revision No.	--	Revision Date	--



Ethical Channel Policy



COPYRIGHT PROTECTED DOCUMENT

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this document may be reproduced or utilized otherwise in any form or by any means, electronic, including photocopying, or posting on the internet or an intranet, without prior written permission.

Prepared & Reviewed By	Approved By	DOCUMENT CONTROLLED
Corporate Secretarial Department	CEO	

Index

Background	3
1. Purpose and scope of application	3
2. Basic principles	3
3. Specific of guidelines	4
4. Monitoring and control	7
5. Amendment sheet	8

▪ Background

The Board of Directors of Business Units is responsible for approving the Ethical Channel Policy.

In the exercise of these functions, Isadak includes the strategy regarding management of the Ethical Channel, as well as its commitment to the application of best practices according to international reference standards.

1. Purpose and scope of application

1.1 **Purpose.** This document sets out the general principles of the Ethical Channel and the protection of the rights of the natural person (hereinafter, "informant") who reports in good faith, through the Ethical Channel, possible breaches of applicable legislation and/or the Isadak's internal regulations.

1.2 **Scope of application.** This Policy apply to all Companies belonging to Abertis India Group in which Abertis India has majority shareholding or controlling interest.

2. Basic principles:

An Ethical Channel must at all times ensure compliance with the following principles:

2.1 **Confidentiality.** Guarantee the confidentiality of the actions carried out in the management and processing of the communications received through the Ethical Channel, as well as the identity of the informant and third parties mentioned (hereinafter, the investigated persons).

The information processed will only be disclosed to the relevant authorities when they so require and the Business Units are legally obliged to do so, with the necessary safeguards in place at all times.

2.2 **Non-retaliation.** Ensure non-retaliation against any bona fide informant, against third parties related to the informant (such as co-workers and family members), against any person or entity cooperating in the investigation, as well as against any investigated person until the proposed resolution is issued.

Controlled companies: companies in which Abertis holds a stake of more than 50% or otherwise where the shareholders' agreement states that Abertis holds a controlling stake.

Any disciplinary measure imposed in a justified manner on the investigated person by the relevant body shall not be regarded as retaliation.

- 2.3 Personal data protection. Guarantee the protection of personal data contained in communications, with only authorized persons having access to them.

Personal data contained in the information received and in internal investigations shall be kept only for such period as is necessary and proportionate. In no case may data be kept for a period longer than ten years.

In the event that the communication received is archived, the personal data contained therein shall be deleted and the communication shall be retained in an anonymized form for the purpose of leaving evidence of the functioning of the Ethical Channel.

- 2.4 Right to a hearing and presumption of innocence. Guarantee the right to honor and privacy of the investigated person, his/her presumption of innocence, as well as his/her rights to a hearing, defense, the assistance of a lawyer in cases where the facts under investigation may be of a criminal nature, and the right to access to the file, provided that this does not affect the proper conduct of the investigation, being able, where appropriate, to put forward the arguments, allegations and evidence that he/she deem appropriate.

3. Specific guidelines

- 3.1 **ECPC.** Every Ethical Channel must be managed by an ECPC.

- **Governing:** The governing body of Business Units must govern through ECPC and provide it with sufficient personal and material resources.
- **Mission:** To monitor compliance of Business Units and the Local Code of Ethics.
- **Functions:**
 - To implement and manage the Ethical Channel.
 - To resolve all queries on the interpretation of the Isadak Local Code of Ethics.
 - To investigate and propose resolutions to all communications received.
- **Guiding principles applicable to the members of the Committee:**
 - Good repute. They may not have been the subject of disciplinary action by any of Policy of Isadak or have a judicial record for conduct that could be assimilated to any breach of Local Code of Ethics.
 - Autonomy and independence in decision-making.

- Confidentiality, objectivity and fairness in the management and treatment of information, avoiding any kind of conflict of interest.

Failure to comply with these guiding principles shall result in the replacement and where appropriate, permanent disqualification of the member in breach.

- **Composition:** The ECPC shall be composed of at least three permanent members, belonging, as far as possible, to the Internal Audit, People and Compliance areas. A Chairman and a Secretary shall be appointed from among its members. The position of Chairman shall be held by the Local Compliance Officer, who shall be responsible for managing the Ethical Channel and promoting the processing of investigation files. The permanent members of the Committee may agree on the intervention of invited third parties with specialised knowledge in the subject matter of the communication.

3.2 Information management procedure: The Ethical Channel will be the preferred channel for notifying any possible breach of applicable legislation and/or the Isadak's internal regulations.

3.3 An Ethical Channel must guarantee that the management procedure of received information complies with the following requirements:

- **Receipt and acceptance of communications:**
 - Identification of the internal information channel(s) and mode of presentation of the communication:
 - a) In writing: by post or by the electronic means provided for this purpose; and/or
 - b) Face-to-face: only admissible at the request of the informant. The meeting must be recorded, giving prior notice to the informant, and take place within 7 days of the request.
 - Publicize the internal channel on the company's website in a separate and easily accessible section.
 - Acceptance of anonymous communications.
 - Registration of the communication, assigning it an identification code and creating an electronic Registry Book with all communications received.
 - Sending acknowledgement of receipt of communications to the informant within 7 calendar days of receipt, unless this could endanger the confidentiality of the communication, or the informant has expressly waived this.
 - Verification of the plausibility of the communication: The ECPC shall verify that the communication is duly substantiated and generally complies with the requirements of truthfulness and clarity. If this is not the case, the ECPC shall order its immediate closure, notifying the informant.

- The ECPC will refrain from processing those communications dealing with facts over which an administrative resolution or judgement, final or not, has been passed; on which the existence of ongoing investigations by the relevant authorities is known, or about information whose access or acquisition constitutes by itself a criminal or administrative offense.
- **Development of the investigation:**
 - Planning of the investigation (objective, rights and obligations, work plan, precautionary measures, applicable legal framework, budget, investigation methodology, evidence...).
 - Principles and safeguards governing the investigation:
 - Hearing with the informant and possibility of requesting additional information.
 - Independence and fairness in the investigation process.
 - Proportionality.
 - Confidentiality.
 - Respect for the protection of personal data.
 - Respect for the presumption of innocence, honour and privacy of the persons concerned.
 - Establishment of the informant's right to know the status of his/her communication and, where appropriate, the outcome of the investigation.
 - Establishment of the right of the person concerned to be informed of the acts or omissions attributed to him/her, to be heard at any time, to assist with a lawyer and not to testify and/or to remain silent.
 - No retaliation against the bona fide informant.
- **Resolution:**
 - Determination of the maximum time limit for responding to the investigative actions, which may not exceed 3 months from receipt of the communication or, where appropriate, of the acknowledgement of receipt. This period may be extended by further 3 months if duly justified. This justification shall be communicated to the informant.
 - Resolution proposal. The final report shall contain:
 - Responsible body
 - Date of receipt and closure of the communication
 - Identification code
 - Facts as reported
 - Classification of communication
 - Actions carried out
 - Measures taken
 - Conclusions and assessment of the proceedings
- **Disciplinary regime:** disciplinary measures must be proportional to the seriousness of the facts, in accordance with the legal regulations in force, and circumstances such as the seriousness of the breach, recidivism, the damage caused or the acknowledgement of the facts by the investigated person may be taken into consideration for their adoption.

- 3.4** Archiving (data protection and preservation): An Ethical Channel must guarantee that the archiving of information received complies with the following requirements:
- Identification of the controller and limited access to the members of the ECPC
 - Retention of personal data:
 - Personal data obtained in the framework of the internal investigation shall be deleted when they are no longer necessary and relevant and, in any case, no later than three (3) months after the communication is recorded, unless the investigation is still ongoing.
 - Personal data shall not be collected where it is manifestly not relevant for the processing of specific information or, if collected by accident, shall be deleted without undue delay.
 - Respect for the data protection rights of informants (access to personal data at any time, request for rectification, deletion of data, limit of use, usage information).
- 3.5** Training and awareness campaigns. The Compliance area of Isadak will be responsible for promoting awareness and training actions on their respective Ethical Channel and, in particular, on the usefulness of the different information channels and the guarantees and protections for informants.

4. Monitoring and control

This policy constitutes a minimum to be complied with by each Business Units. It will be the responsibility of each company to:

- develop this policy through internal procedures that ensure its proper implementation and its compliance with their respective legal system, and
- establish internal regulations detailing the procedure for managing information received through the Ethical Channel and the appropriate, effective and clear control mechanisms to identify and report any risk and/or non-compliance with this policy.

Controls on the degree of implementation and adequacy of this policy, as well as its internal development regulations, will be the responsibility of the Compliance area of Isadak.

