ISPD

Procedure of the Ethics & Compliance Channel

Version 1.2 · July 2026
ISPD Network, S.A. and subsidiaries

CONTROL OF VERSIONS

Document Code	Procedure of the Ethics & Compliance Channel
Document Type	Procedure
Version	v 1.2
Date	July 2026
Author	Internal Information System Managers
Publication Date	July 2026
Confidentiality Level	Public
Approval	March 2026

Version history

Version	Date	Author	Summary of changes
v 1.0	November 2022	Internal Information System Managers	Initial version.
v 1.1	November 2023	Internal Information System Managers	Partial alignment with Spanish Law 2/2023.
v 1.2	**July 2026**	**Internal Information System Managers**	**Update of the collegiate body (Internal Information System Managers) and alignment with the requirements of Spanish Law 2/2023.**

Important Notice

This document and its annexes are confidential and are the property of ISPD. Any total or partial reproduction is expressly prohibited, as is the use of any type of information it contains, except where it has been expressly authorized by ISPD, the holder of the intellectual property rights. ISPD reserves the right to initiate such legal actions as it deems necessary for any breach of the indicated limitations by any person who has access to the documentation.

TABLE OF CONTENTS

1. Scope and area of application 4
2. Principles of the Ethics & Compliance Channel 4
2.1. Anonymity 4
2.2. Confidentiality 4
2.3. No Retaliation 5
2.4. Presumption of Innocence 5
2.5. Independence 5
2.6. Communication and Training 5
2.7. Personal data protection and the exercise of rights 5
3. Procedure of the Ethics & Compliance Channel 6
3.1. Process Managers (Internal Information System Managers) 6
3.2. Process Development 7
4. Development of the Process 11
5. External Channels of Communication 12
6. Publicity and entry into effect 12
7. Appendix I — Communication template 13

1. SCOPE AND AREA OF APPLICATION

This procedure regulates the operating rules of the Ethics & Compliance Channel of ISPD on a global level (hereinafter, "ISPD"). The Ethics & Compliance Channel constitutes ISPD's Internal Information System ("IIS") for the protection of persons who report regulatory infringements and for the fight against corruption.

The Ethics & Compliance Channel is established so that all employees or interns, ex-employees, participants in selection processes, shareholders, managers, providers or subcontractors of ISPD may communicate breaches related to the Code of Conduct, criminal acts or — in the case of companies that comprise ISPD located in the European Union — violations of EU Law concerning the following subjects: public contracts; financial services; product, food and transport safety; environmental protection; animal welfare; nuclear safety; public health; consumer protection; data privacy and protection; competition; the interior market or the financial interests of the Union.

Certain geographic zones may have specific procedures that shall prevail over this procedure in the event of any discrepancy; however, all such specific procedures shall be reviewed by Global Corporate before publication.

2. PRINCIPLES OF THE ETHICS & COMPLIANCE CHANNEL

2.1 ANONYMITY

An anonymous channel has been enabled to process those communications in which there is no identifying data of the informant, thereby ensuring anonymity. Note that, where a communication is made anonymously, no questions can be put to the informant to clarify any point of the communication, nor can the informant be notified of its progress, since no contact details have been provided.

2.2 CONFIDENTIALITY

All reports, whether or not anonymous, shall have their confidentiality guaranteed insofar as the identity of the informant, the defendant and any other individuals mentioned in the communication, as well as the contents of the communications, are concerned. The Internal Information System Managers (the "IISM") shall ensure that the parties involved in the procedure — whether the individuals who in each case make up the Investigative Team, or, where applicable, the external experts — sign reinforced confidentiality agreements.

In addition, all employees receive confidentiality training, so that if a communication is forwarded to a reporting channel other than the one established, or to personnel not responsible for handling it, they keep it confidential and forward it to the IISM without delay. Breach of this obligation constitutes a very serious infringement and shall be sanctioned under the internal disciplinary framework.

2.3 NO RETALIATION

The policy guarantees the absence of retaliation of any type against the informant or persons related thereto, as well as the work colleagues or the legal representatives of the employees in the exercise of their duties to advise and support the informant for the complaints that they have submitted in good faith. Retaliation means any act or omission prohibited by law that involves unfavourable treatment placing the affected individuals at a particular disadvantage within the work or professional context, solely on account of their status as an informant or a person related to an informant.

Notwithstanding the foregoing, any manifestly false communication may give rise to disciplinary action by ISPD and, where appropriate, to any legally applicable judicial action.

2.4 PRESUMPTION OF INNOCENCE

Under this procedure, full respect for the presumption of innocence and for the honour of everyone affected by communications and investigations is both guaranteed and required. All investigations shall be conducted with the utmost discretion and sensitivity, ensuring that no one's reputation is damaged without solid evidence supporting the accusations.

2.5 INDEPENDENCE

Both the IISM and the Investigative Team shall carry out their functions independently and autonomously from the other ISPD bodies, may not receive instructions of any kind in exercising them, and shall have all the human and material resources necessary to do so. This is guaranteed, among other measures, through direct reporting to ISPD management and through conflict-of-interest declarations signed by the various persons who are members of the body at any given time.

2.6 COMMUNICATION AND TRAINING

Information shall be provided to employees and interns regarding the existence, objective and operation of the Ethics & Compliance Channel, as well as information regarding the processing of personal data and the data protection rights of the users of the Channel.

Clear, easily accessible information on the use of the Ethics & Compliance Channel and on the essential principles of its management procedure shall likewise be published at www.ispd.com, so that this information is available to all potential informants.

2.7 INFORMATION REGARDING PERSONAL DATA PROTECTION AND THE EXERCISE OF RIGHTS

The informant, the defendant and any other parties involved shall be informed of the processing of their data on the terms set out in the applicable data protection rules.

3. PROCEDURE OF THE ETHICS & COMPLIANCE CHANNEL

3.1. PROCESS MANAGERS

The various bodies that intervene during the communication process are as follows:

Body	Composition	Mission
Internal Information System Managers	Collegiate body comprised of: • Mr. Jordi Ustrell Rivera *(Chief Financial Officer)* • Ms. Paula Bouzas Lestón *(Legal Counsel)* *Appointed by unanimous resolution of the Board of Directors of ISPD Network, S.A. dated 26 March 2026.*	To channel the reports received through the Ethics & Compliance Channel, to ensure the correct operation of the Internal Information System (IIS) and to process investigation files in accordance with this Procedure and applicable regulations.
Investigative Team	Composed on the basis of the specific knowledge required for the analysis of the facts and information set forth in the communication (e.g., information systems, accounting, human resources). It shall be designated by the IISM on a case-by-case basis.	To carry out the pertinent investigations based on the communication, summoning the defendant, the affected parties and third parties who may act as witnesses, and producing the corresponding Investigative File.
Legal Department	Composed of the individuals who are members at any given time.	To ensure the filing of the relevant judicial complaints and compliance with personal data protection regulations, and to keep the ISPD risk map updated in line with the risks recorded through the channel.
Systems Department	Composed of the individuals who are members at any given time.	To ensure that the channel complies with the technical requirements established at any time by the applicable regulations and by the needs identified by the IISM, particularly in terms of confidentiality and information security.

Any member of these bodies who is affected by a communication — whether as an informant or defendant, or through kinship and/or a personal relationship, evident friendship or enmity, or direct hierarchical subordination — shall automatically be barred from taking part in any procedure until their case is closed. In

the event of being the defendant, they shall be automatically banned from any procedure until the resolution of their case. In the event that the circumstances affect both members of the IISM, the functions of the IISM shall be carried out by the President or the CEO of ISPD, or those designated by them.

3.2. PROCESS DEVELOPMENT

3.2.1 How to compose the correspondence

Alternatively, the following methods are established in order to communicate any breach:

- The electronic e-mail address compliance@ispd.com; and
- The anonymous and accessible Compliance mailbox at https://ispd.com/ethics-and-compliance-channel/.
- At the informant's request, by means of an in-person meeting, which shall be held within a maximum of seven (7) days; detailed minutes shall be drawn up, with no need to reveal the informant's identity if they expressly so request. The informant shall be given the opportunity to verify, rectify and accept the minutes by means of their signature.

Likewise, and exceptionally, if the communication involves one of the members of the IISM, the correspondence may be addressed to the personal corporate e-mail of the uninvolved member of the IISM (or the personal corporate e-mail of the President or the CEO of ISPD in the event that the correspondence involves both members). It must be noted that in said case, anonymity shall not be guaranteed, except if the correspondence is sent through an e-mail account that does not contain the name, surnames or any other data that permits identifying the informant.

Both of the foregoing channels shall be deemed the "Ethics & Compliance Channel" and shall be managed by the IISM with restricted access.

The correspondence must specifically describe the facts reported, the affected area or company, the date or period of commission and possible responsible subjects. Where available, supporting evidence shall be included. A model of the communication that the informant is encouraged to use is included as **Appendix I** for the purpose of ensuring compliance with the various required points.

3.2.2 Reception and Processing Phase

Once the communication has been received, the IISM shall send the informant an acknowledgement of receipt within seven (7) calendar days of receipt, unless doing so could jeopardise the confidentiality of the communication.

Within fifteen (15) calendar days, the IISM shall also assess whether the communication should be processed and managed.

Reasons for inadmissibility shall be:

- That there is no violation or breach of the Code of Conduct.
- Clearly unfounded facts without accreditation of any type. Inexistence of reasonable indications.

- Generic, imprecise or vague description. In that case, the deficiencies of the communication shall be communicated to the informant (if their contact data has been facilitated) within a period of fifteen (15) calendar days, so that it is clarified or substantiated in an additional seven (7) calendar day period. If not remedied, the inadmissibility shall proceed.
- There is a specific procedure (for example, a situation of harassment). In that case, the IISM shall send it to the body designated in each case for its procedure within a period of fifteen (15) calendar days from its reception.

Once it has been determined, if appropriate, to accept the communication for processing or, on the contrary, if its non-acceptance is appropriate, the IISM shall communicate its decision to the informant (provided the informant has provided their contact details).

In the event of non-acceptance, the reasons for the non-acceptance of the communication shall be communicated in detail and therefore, the case shall be closed.

If communications are received by any means other than those described here (orally, by telephone, or by e-mail outside the Ethics & Compliance Channel), the recipient shall forward them to the IISM, which shall redirect them so that they follow the established procedure.

If the communication is related to another case that has already commenced in which substantially identical facts are being investigated, the IISM may agree to their joinder and a resolutory decision in a single proceeding.

The IISM shall proceed to inform the defendant, except if it is deemed that said information must be delayed in order to not undermine the investigation and preserve evidence, thereby avoiding its destruction or alteration. In any case, they shall be informed within a maximum period of three (3) months from the presentation of the communication. If it is determined that informing the defendant of the commencement of the proceeding within this period may jeopardize the investigation itself, the IISM must justify in writing and in detail the facts that have led to this decision being adopted.

Information provided to the defendant must be facilitated under terms which protect the confidentiality of the informant, for which reason neither the identity of the informant, nor the area or department from which the communication proceeds, nor any other information that may facilitate the identification thereof shall be included.

3.2.3 Investigation Phase

The objective of the investigative phase shall be (i) to establish the reported facts, (ii) to propose the adoption of the measures necessary in order to prevent the communicated events from occurring again, and (iii) to propose disciplinary measures, if appropriate, that follow from the application of the Collective Bargaining Agreement or the application of the law.

Once the IISM has approved the communication for processing, it shall designate the Investigative Team, thereby taking into consideration the need for specific knowledge that requires the analysis of the facts and information set forth in the communication. The Investigative Team may be comprised of one of the members

of the IISM, in which case this member of the Investigative Team shall not be able to participate in the drafting of the Report of Conclusions (as defined in section 3.2.4).

Prior to transferring any type of information regarding the contents of the communication to the Investigative Team, the IISM shall ensure that the individuals on the Investigative Team have signed reinforced confidentiality agreements as well as a statement on the absence of conflicts of interest.

Once that requirement has been met, the IISM shall forward to the Investigative Team the contents of the communication and any other relevant information that has been collected.

In any event, given the significance of the facts under investigation, the IISM may inform ISPD Management of the contents of the communication in advance and on an exceptional basis, where urgent interim measures need to be adopted.

The Investigative Team shall arrange a hearing with the defendant, thereby ensuring in this manner their right to be informed of the actions or omissions that are attributed to them and to be heard at any time (except if this could involve an obstacle for the correct development of the investigation), as well as the affected parties and third parties who may act as witnesses. Likewise, they may request internal and/or external help that they deem necessary for carrying out the review of documents and/or registries, analyses of processes and procedures, copying and revision of devices; in which case, the identity of said specialists shall be transferred to the IISM so that it may ensure that the experts sign the pertinent reinforced confidentiality agreements as well as a statement on the absence of conflicts of interest prior to collaborating with the Investigative Team.

Once the allegations of the various affected parties have been heard, the Investigative Team shall draft an investigative file (hereinafter, the "Investigative File") that shall contain:

- Descriptive information of the communication with an indication of its reception date.
- Data provided in the communication with a distinction between objective and subjective facts.
- Evaluation of the contents of the communication.
- Analysis of the information and the inclusion of the latter with a statement of the most probable hypothesis and the greatest risk.
- Measures proposed and those already performed preliminarily in the event that they have been deemed urgently necessary or appropriate.
- Allegations of the defendant.

The Investigative File shall be sent to the IISM so that a report on the conclusions of the investigation is drafted (the "Report of Conclusions").

A maximum period of one (1) month is set for completing the Investigative File, running from the date the IISM designates the Investigative Team. This period may be extended by a further period of equal duration where the facts under investigation are complex, where special technical, accounting or computing knowledge is required, or where complaints are joined.

3.2.4 Conclusionary Phase

The IISM, based on the Investigative File forwarded by the Investigative Team, shall draft the Report of Conclusions. Said conclusions may give rise to two possible results:

- **Unfounded Communication. Where the investigation shows that no breach occurred, the IISM shall inform the informant (provided they have given contact details) and the defendant of this decision, together with the reasons supporting it.**
- **Appropriate Communication.** In which case, the facts that sustain said conclusion shall be set forth in detail and the preparation of the report proceeds.

The Report of Conclusions must in addition contain as a minimum the following points:

- **Conclusions.** The conclusions must be presented clearly and concisely and always in regard to the evidence and obtained analysis. Any conclusion based on the knowledge and experience of the Investigative Team must include a warning to such an effect. If any limitation in the development of the investigation has existed, it must be reflected therein.
- **Proposal of measures** to be adopted (organizational measures, internal disciplinary framework or communication of the complaints to the authorities).

Once the Report of Conclusions has been issued and sent to ISPD Management, it falls to ISPD Management to adopt the measures proposed by the IISM. The report shall be issued within one (1) month of the Investigative Team's receipt of the Investigative File.

Where the outcome of the investigation indicates that the facts could constitute a crime, the Legal Team, on prior guidance from Company Management, shall immediately send the relevant information to the Public Prosecutor's Office. In the event that the facts affect the financial interest of the European Union, it shall be sent to the European Public Prosecutor's Office.

The IISM shall communicate the decisions taken to both the informant (provided they have given contact details) and the defendant, and shall then close or shelve the case.

In any event, the maximum term to provide a response to the informant shall not exceed three (3) months, counted from the receipt of the communication or, where no acknowledgment of receipt was sent, from the expiry of the seven (7) calendar days following the communication. The phases described shall be carried out within that term. In cases of special complexity, the term may be extended, on a justified basis, by a maximum of three (3) additional months.

In the event that the communication is inadmissible or is inappropriate, after three months from the reception of the communication, its elimination or anonymization shall proceed.

Said period shall be extended in the event that the investigated facts are complex or require special technical, accounting or computer knowledge, as well as in cases of the joinder of different communications regarding the same incident. Under no circumstances may the data be saved for a period longer than ten years.

Each year, the IISM shall produce a report on the data recorded during the financial year — number of complaints, their content, actions taken and resolution times — omitting the identity of the informant, the defendant and the parties involved in each case. Said report shall be submitted to the Board of Directors.

Independently of the annual report, the IISM shall keep a confidential record (log) of all communications received and the internal investigations to which they have given rise. This record shall be of a non-public nature, access to it shall be restricted to the IISM, and the data contained therein shall be retained in accordance with the periods established in this Procedure. The annual report shall be drawn up on the basis of the recorded information.

Based on said report, the Legal Team shall proceed to adopt a map of compliance risks, thereby modifying, if appropriate, the impact or the probability of said risk, and shall carry out a review of the control actions related to the Compliance Plan.

4. DEVELOPMENT OF THE PROCESS

The process is structured in three consecutive phases. The phases and applicable maximum periods, as described in section 3, are summarized below:

Reception and processing phase

- 7 calendar days to acknowledge receipt of the communication.
- 15 calendar days from reception to assess whether the communication meets the requirements.
- 15 calendar days from reception to communicate that the case requires remedy or redirection to a specific procedure.
- 7 calendar days from notification for the informant to remedy the communication.
- 3 months from reception to inform the defendant (may be extended on justified grounds).

Investigation phase

- 1 month from designation of the Investigative Team, extendable by an equal period in case of complexity or joinder of complaints.

Conclusionary phase

- 1 month for the issuance of the Report of Conclusions from the reception of the Investigative File.
- Overall term to respond to the informant: 3 months from receipt of the communication (or from the expiry of the 7-day acknowledgment period), extendable, on a justified basis, by up to 3 additional months in cases of special complexity.

5. EXTERNAL CHANNELS OF COMMUNICATION

The informant may choose, at any time and alternatively or successively to the internal channel, the external information channels:

- The Independent Authority for the Protection of the Informant, A.A.I., at national level.
- The regional authorities or competent bodies designated by the autonomous communities within their respective territorial scope.
- The competent institutions, bodies or agencies of the European Union, in particular the European Anti-Fraud Office (OLAF) and the European Public Prosecutor's Office, where applicable.

Access information to these channels shall be kept available and updated at www.ispd.com.

6. PUBLICITY AND ENTRY INTO EFFECT

The content of this Procedure is mandatory for all ISPD personnel and shall enter into effect upon its communication to the staff.

It shall remain in effect while it is not modified or replaced by another. The effective Procedure at any time shall be available at www.ispd.com and shall be circulated among the personnel who are part of ISPD.

7. APPENDIX I

Communication template for use in the Ethics & Compliance Channel

To the attention of the Internal Information System Managers:

I STATE

First.- By means of this document I communicate the following situation (describe in detail the facts that are to be reported, the area or affected company, the period during which it has been occurring or the specific moment when they have occurred and who the persons responsible are):

_____

_____

Second.- As evidence of that set forth in the previous point, I attach the following evidence (it is asked to attach all accreditive documents of the facts reported or that may help to clarify them, whether they are copies of electronic communications, recordings, photos or, if the case, documentation):

_____

_____

Third.- I understand that such facts may constitute a breach of the ISPD Code of Conduct or that may constitute a criminal act or an infringement of the Law of the European Union in the following areas: public contracting, financial services, product, food and transport safety, consumer protection, data protection and privacy, competition, interior market or financial interests of the Union.

I REQUEST

That the corresponding communication be hereby formulated, the necessary actions be initiated in order to terminate the reported situation and the corresponding measures be adopted.

In _____, on _____ of _____ of _____

Signed: _____