



ESPUÑA GROUP'S ETHICAL CHANNEL OPERATING POLICY

8 June 2023

IMPORTANT DOCUMENT INFORMATION

Name of document:	Ethical Channel Operating Policy
Standard developed:	ESPUÑA GROUP's Code of Ethics
Author:	System Manager (Compliance Committee)
Responsible for compliance:	System Manager (Compliance Committee)
Approval body:	Governing Body (Sole Administrator)
Approval date of the current version:	8 June 2023

VERSION AND AMENDMENTS HISTORY

Version:	Date:	Author:	Approval body:	Summary of amendments:
V.1	8 June 2023	System Manager (Compliance Committee)	Governing Body (Sole Administrator)	



CONTENTS

1. PURPOSE AND OBJECTIVE.....4

2. SCOPE.....5

3. PRINCIPLES OF THE ETHICAL CHANNEL.....5

 3.1. CONFIDENTIALITY.....5

 3.2. INDEPENDENCE.....6

 3.3. GOOD FAITH.....6

 3.4. PROHIBITION TO RETALIATION.....6

4. OPERATION OF THE ETHICAL CHANNEL.....7

 4.1. SUBMITTING COMMUNICATIONS.....7

 4.1.1. AVAILABLE CHANNELS.....7

 4.1.2. INFORMATION CONTAINED IN THE COMMUNICATION.....7

 4.2. COMMUNICATIONS MANAGEMENT AND RESOLUTION.....8

 4.2.1. SYSTEM MANAGER.....8

 4.2.2. RECEIPT AND ASSESSMENT.....10

 4.2.3. PROCESSING AND INVESTIGATION.....12

 4.2.4. RESOLUTION AND COMMUNICATION.....14

 4.2.5. DISCIPLINARY MEASURES.....15

5. DATA PROTECTION AND PRESERVATION.....16

6. EXTERNAL INFORMATION CHANNELS.....19

7. NON-COMPLIANCE.....19

8. APPLICABLE REGULATIONS.....19

9. ENTRY INTO FORCE, VALIDITY AND REVIEW.....20



1. PURPOSE AND OBJECTIVE

The purpose of this Ethical Channel Operating Policy (hereinafter, the “**Policy**”) is to define and establish a suitable and effective model for the operation of the Internal Information System (hereinafter, the “**Ethical Channel**”) of the companies Esteban España, S.A., Embotits Cuscó, S.A., España R&D, S.L.U. and Pata Negra Jan, S.L.U. (hereinafter, “**ESPUÑA GROUP**” or the “**Group**”, indistinctly), adapted to the regulations in this area, namely EU DIRECTIVE 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 23 October 2019, on the protection of persons who report infringements of Union Law (hereinafter, “**Whistleblower Directive**”) and Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption (hereinafter, “**Whistleblower Protection Law**), as well as to the highest national and international standards in force (UNE-ISO 37002:2021 on Whistleblowing Management Systems. Guidelines, which allows for receiving and processing:

- On the one hand, communications related to breaches and/or practices contrary to the principles established in the Code of Ethics and the Policies and Protocols of ESPUÑA GROUP, as well as in the internal rules and procedures that develop them and in the other rules imposed by the regulatory framework of the organisation and/or,
- On the other hand, acts or omissions that may constitute breaches of European Union law or serious or very serious criminal or administrative offences under Spanish national law.

This Policy establishes the procedure that regulates the functioning of the Ethical Channel of ESPUÑA GROUP, in such a way that it covers the issues relating to communications carried out by the whistleblowers, as well as the management and resolution of such communications by the System Manager.

The purpose of this Policy is to guarantee professional, confidential, impartial management and the highest protection of the rights of the concerned parties (including the rights recognised in the personal data protection regulations) throughout the process of making, managing, processing, investigating and resolving communications made through ESPUÑA GROUP’s Ethical Channel.

In this regard, this Policy sets out three basic safeguards:

- i) guaranteeing the protection of whistleblowers.
- ii) guaranteeing freedom from reprisals for whistleblowers and
- iii) guaranteeing the rights of the defendant during the handling and processing of communications.

2. SCOPE

This Policy is applicable to all members of ESPUÑA GROUP (including employees and managers, shareholders and members of the Governing Body, regardless of the position they hold within the organisation, the legal nature of their relationship and whatever their area of activity or hierarchical level), who become aware, in a work or professional context, of any infringement established in section 1 of this Policy.

Likewise, the provisions of this Policy shall also apply to third parties such as: business partners, collaborating companies, subcontractors, suppliers and other persons or entities that have a professional relationship with ESPUÑA GROUP.

3. PRINCIPLES OF THE ETHICAL CHANNEL

3.1. CONFIDENTIALITY

ESPUÑA GROUP guarantees the utmost confidentiality of the communications received through its Ethical Channel and the data contained therein.

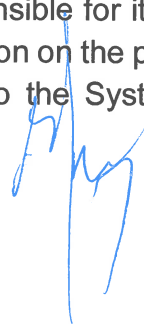
The identity of the person reporting an irregularity through the Ethical Channel will be treated as confidential information and will therefore not be disclosed to the accused person. In the same vein, the confidentiality of the identity of the accused person shall be guaranteed.

Furthermore, it is expressly forbidden for the personal data contained in the communication and resulting from the investigation carried out to be known by any person other than those expressly authorised. In this regard, specific confidentiality commitments will be signed with the persons responsible for managing such communications.

Without prejudice to the foregoing, the details of the person making the communication may be provided to the administrative or judicial authorities or to the Public Prosecutor's Office, insofar as they are required by such authorities because of any criminal, disciplinary or sanctioning proceedings arising from the subject matter of the communication.

This transfer of data will always be carried out in full compliance with the legislation on the protection of personal data, requiring that in all cases third parties are prevented from accessing said data.

When the communication is sent through reporting channels other than those established in this Policy or to members not responsible for its processing or to non-competent personnel, there shall be an obligation on the part of the recipient of the communication to immediately forward it to the System Administrator,

A handwritten signature in blue ink, appearing to be a stylized name, located at the bottom right of the page.

always guaranteeing the confidentiality of such information. Failure to comply with this obligation will be classified as a very serious infringement, and ESPUÑA GROUP may adopt the appropriate disciplinary measures.

3.2. INDEPENDENCE

The procedures for processing, investigation and resolution and, in general, the management of communications received through ESPUÑA GROUP's Ethical Channel shall be governed by maximum objectivity and independence, and this Policy establishes the corresponding mechanisms to avoid the occurrence of possible conflicts of interest.

3.3. GOOD FAITH

All communications submitted through the Ethical Channel must be made in good faith. This means that, at the time of submission of the communication, the whistleblower must have reasonable and sufficient grounds to believe that the information provided is true, accurate and contains possible infringements.

In this sense, false or malicious communications or reports may give rise to the corresponding sanctions by ESPUÑA GROUP, without prejudice to the civil and even criminal liabilities that may arise.

3.4. PROHIBITION TO RETALIATION

ESPUÑA GROUP undertakes not to adopt any form of retaliation, threats of retaliation or attempts of retaliation, directly or indirectly, against persons who, in good faith, have reported any irregularity through the Ethical Channel.

Retaliation should be understood as any act or omission prohibited by law, or which, directly or indirectly, results in unfavourable treatment the people who are suffering such situation in a particular disadvantage compared to another in the employment or professional context, solely because of his or her status as a whistleblower.

Protection against retaliation also extends to persons who report possible infringements through the external whistleblower channels mentioned in section 6 of this Policy.

In addition to whistleblowers, the prohibition of retaliation set out in the Policy also extends to the following persons:

1. individuals who, within the framework of the organisation in which the whistleblower provides services, assist the whistleblower in the process.
2. individuals who are related to the whistleblower and who may suffer retaliation, such as co-workers or relatives of the whistleblower, and

3. legal entities, for whom the whistleblower 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, an interest in the capital or in the voting rights pertaining to shares or holdings is deemed to be significant when, by virtue of its proportion, it enables the person holding it to have the capacity to influence the legal entity in which it has an interest.

If any member of ESPUÑA GROUP, in contravention of the provisions of this Policy, directly or indirectly retaliates, the organisation itself will take the necessary measures to ensure that the retaliations cease as soon as possible and, where appropriate, will take the necessary disciplinary measures against those responsible for any retaliation.

Furthermore, this Policy will also guarantee the rights to privacy, to be heard, to be informed of the actions or omissions attributed to him/her, to defence, to honour and to the presumption of innocence of the persons under investigation, as well as the right of access to the file.

4. OPERATION OF THE ETHICAL CHANNEL

4.1. SUBMITTING COMMUNICATIONS

4.1.1. AVAILABLE CHANNELS

Whistleblowers may make communications through the channels provided for this purpose.

In this sense, ESPUÑA GROUP provides the following channels for the communications included in this Policy:

- E-mail address: canaletico@espuna.es
- Via postal mail to the address: Carrer Mestre Turina, 39-41, 17800 Olot, Girona.

At the request of the whistleblower, the communication may also be submitted by means of a face-to-face meeting with the System Manager, which, where applicable, must take place within a maximum period of seven (7) days following the request.

4.1.2. INFORMATION CONTAINED IN THE COMMUNICATION

The communication shall include the following information:

- Identity of the whistleblower (name, surname and ID document number). Except in cases of anonymous communications. In this sense, ESPUÑA

GROUP's Ethical Channel allows communications to be carried out anonymously, without providing the identity of the whistleblower.

- Relationship with ESPUÑA GROUP (employee, supplier, shareholder, subcontractor, intern, etc.) and, where applicable, position in ESPUÑA GROUP.
- As detailed and complete a description as possible of the conduct, event or alleged wrongdoing being reported.
- Identity of the accused person (name, surname and position), if the person responsible for the event is known, and the department in which the reported event took place.
- Indications, clarifying explanations or evidence on which the information is based. Provide all available evidence or indicate where and how to obtain it (e.g. witnesses, documents, records, etc.).
- Approximate dates of occurrence of the events.
- Where applicable, means of communication (address, e-mail, telephone or other) of the whistleblower so that the System Manager may carry out notifications or communications.

If, after reviewing the content of the communication, it lacks the minimum requirements that are mandatory for its correct assessment, the System Manager will proceed to request the corresponding information and/or documentation from the whistleblower through the means of communication indicated by the latter, proceeding to file the communication, in the event that the necessary information is not available for proceeding with the investigation phase.

4.2. COMMUNICATIONS MANAGEMENT AND RESOLUTION

4.2.1. SYSTEM MANAGER

The Governing Body of ESPUÑA GROUP is the competent body for the appointment, as well as the removal or cessation of the System Manager, who, in turn, is responsible for the management and processing of the communications that are filed through ESPUÑA GROUP's Ethical Channel.

The System Manager may be an individual or a collegial body that must delegate to one of its members (individual) the powers of management and processing of the investigation files.

Both the appointment and the removal of the System Manager shall be notified to the Independent Whistleblower Protection Authority (A.A.I. in Spanish) or, where appropriate, to the competent authorities or bodies of the Autonomous Communities.

In this regard, ESPUÑA GROUP's Governing Body has appointed a collegial body as the System Manager, this being the organisation's Compliance Committee, which in turn has appointed one of its members (an individual) to carry out the management and processing of the communications made through the Ethical Channel.

The System Manager shall act independently of the rest of the functions and hierarchical or functional subordination that may exist, as the case may be, performing the necessary tasks under the premises of confidentiality, respect, independence, neutrality, impartiality, honesty and objectivity towards the persons affected by the communication in question, also ensuring that the procedure is carried out in accordance with the procedures and principles established in this Policy.

If the System Manager has an incompatibility or conflict of interest with the event or persons who are the object of the communication, he/she shall abstain from participating in the management and processing of the communication and shall not, therefore, have access to the information derived from the actions carried out in the management of said communication. In this regard, the System Manager shall be replaced by another person designated and appointed by the Managing Director or, where appropriate, the Governing Body or other competent body.

- **Responsibilities of the System Manager**

The main responsibilities of the System Manager in the management of ESPUÑA GROUP's Ethical Channel are as follows:

- Manage the Ethical Channel tool.
- Receive communications made through the Ethical Channel.
- Analyse the content of the communications received and decide on their admissibility.
- Determine the desirability or necessity of taking immediate action to prevent (stop or mitigate) further damage.
- In the case of named reports (or, if initially anonymous, as soon as the whistleblower discloses his or her identity), he/she shall notify the whistleblower regarding receipt of the report (sending an acknowledgement of receipt), unless this could jeopardise the confidentiality of the communication.
- Ensure that appropriate measures are taken to prevent and avoid possible retaliation against the whistleblower.

- Conduct the investigation/examination of the facts internally in accordance with the rules and principles set out in this Policy (or decide on the appropriateness of their investigation through an external expert manager).
- Draw up a report on the result of the investigation carried out, stating whether the facts reported are accredited and proposing the appropriate measures for the resolution of the incident, as well as, where appropriate, the disciplinary measures to be taken, with the possibility of delegating this power to another competent body.
- Inform the persons concerned (including the whistleblower) regarding the completion of the procedure.
- Extend the resolution period due to reasons of complexity.
- Resolve doubts and queries that may arise in relation to the Channel.
- Keep the complaints register up to date.
- Ensure that the necessary security measures applicable to the Communications Information Management System are in place, including restricting access to said system.
- Draw up an annual report for presentation to ESPUÑA GROUP's Governing Body on the activity carried out in relation to the Ethical Channel, including information on complaints received, complaints processed or rejected, queries made, etc.
- Manage the storage of communication information in the Communication Information Management System.

The System Manager shall carry out these functions and responsibilities independently and autonomously from the rest of the organisation's bodies.

For the performance of the functions and responsibilities, and in those cases in which it is deemed necessary, the System Manager may be assisted by an external consultant or even delegate some of the aforementioned functions to the latter. In this regard, the System Manager must obtain a confidentiality agreement from the external collaborators involved in the management and resolution of the communication. This shall also be obtained from internal collaborators when deemed necessary.

4.2.2. RECEIPT AND ASSESSMENT

Once a communication has been received through the Ethical Channel, the System Manager will proceed to register it in a Communications Logbook, assigning an identification code to the communication.

The Communications Logbook is stored in a secure database (Information Management System) with access restricted to authorised persons only and will record all communications and information received through the Ethical Channel and during the processing thereof.

The following data shall be entered in each of the records of communications entered in the Communications Logbook:

- Date of receipt.
- Identification code.
- Actions carried out.
- Measures adopted.
- Date of closure.

The Logbook shall not be public and only at the reasoned request of the competent judicial authority, by order, and in the framework of judicial proceedings and under the guardianship of that authority, may its content be fully or partially accessed.

Once a communication has been received, within a maximum period of seven (7) calendar days following its receipt, the System Manager shall send an acknowledgement of receipt of the communication to the whistleblower, unless the communication is anonymous; the whistleblower has waived his/her right to receive communications relating to the investigation; or this could jeopardise the confidentiality of the communication.

If the whistleblower agrees, the possibility for the System Administrator to maintain the communication is expressly provided for.

The System Manager shall verify the content of the communication. If documentation is missing or a formal defect is detected, the System Manager shall issue a request for information to the whistleblower. Likewise, the System Manager, when deemed necessary, may request additional information from the whistleblower regarding the communication made.

The System Manager must verify whether the communication sets out facts or conduct that fall within the scope of this Policy and, therefore, whether the communication is admissible.

Once this preliminary analysis has been carried out, the System Manager, within a period that may not exceed ten (10) working days from the date on which the information in the communication is entered in the Logbook, shall:

- a) Grant the processing of the communication.
- b) Deem the inadmissibility of the communication, in any of the following cases:
 1. When the facts reported lack any credibility.
 2. When the facts reported do not constitute a breach of the cases set out in this Policy.

3. When the communication is manifestly unfounded or there are, in the opinion of the System Manager, reasonable grounds to believe that it was obtained through the commission of an offence.
In the latter case, in addition to the inadmissibility, a detailed account of the facts deemed to constitute an offence shall be sent to the Public Prosecutor's Office.
4. Where the communication does not contain significant new information on infringements compared to a previous communication in respect of which the relevant proceedings have been completed, unless there are new factual or legal circumstances that justify a different follow-up.
In such cases, the System Manager shall notify the decision to the whistleblower in a reasoned manner.

Likewise, communications in which the facts described are misleading and/or there is corroboration that the communication was made in bad faith, i.e., with the intention of harming the organisation or third parties related thereto, will not be accepted.

- c) Immediately forward the information to the Public Prosecutor's Office when the facts may be suspected of constituting an offence or to the European Public Prosecutor's Office when the facts affect the financial interests of the European Union.
- d) Forward the communication to the authority, entity or body considered competent for its processing.

The decision on the admissibility, inadmissibility or relaying of the communication shall be communicated by the System Manager to the whistleblower within five (5) business days of the decision being made, unless the communication is anonymous, or the whistleblower has waived the right to receive communications.

The System Manager shall also assess the advisability or necessity of adopting immediate measures to prevent further damage and, if necessary, implement them.

4.2.3. PROCESSING AND INVESTIGATION

Once the communication has been admitted for processing, the System Manager, acting as the investigator, shall carry out all the actions, proceedings and investigations deemed necessary and aimed at verifying the veracity of the

facts of the communication, and may entrust this task to an external expert, if the circumstances so require.

Thus, the veracity and accuracy of the information contained in the communication and, in particular, of the reported conduct will be verified, following at all times the principles set out in this Policy and under a strict regime of confidentiality to respect the rights of the whistleblower and of the person under investigation.

During the investigation, the accused person shall be notified of the communication with a brief account of the facts established therein. This information may be provided during the hearing of the accused person, if it is considered that its provision beforehand could facilitate the concealment, destruction or alteration of evidence.

Without prejudice to the right to make written allegations, the investigation shall, whenever possible, include an interview with the accused person, in which, always with full respect for the presumption of innocence, he/she shall be invited to explain his/her version of the facts and to provide such evidence as he/she considers appropriate and relevant.

To guarantee the right of defence of the accused person, the latter shall have access to the file (without disclosing information that could identify the whistleblower) and may be heard at any time. The accused person will also be advised of the possibility of being assisted by a lawyer.

In addition, the investigator shall give a hearing to all persons concerned and to potential witnesses and shall take any steps deemed necessary (review of documentation, obtaining information from external sources, etc.). In this respect, all members of the organisation are obliged to cooperate loyally in the investigation. The intervention of witnesses and persons concerned shall be strictly confidential.

The investigator may obtain all the information and documentation he/she considers appropriate from any area or department of the organisation to substantiate the investigation.

A written record shall be drawn up of all investigative actions and of the explanations/statements given by the persons involved in the procedure for investigating the communication (provided that their prior consent has been obtained), which shall be duly signed by the persons involved in order to certify its content and that it is in accordance with their statement. The content of these records will be incorporated into ESPUÑA GROUP's Information Management System with the same guarantees of confidentiality as the rest of the file.

In the event that the presence of the accused person during the investigation period could jeopardise the conduct of the investigation or the strict observance

of the guiding principles of the procedure set out in this Policy, the accused person may, at the proposal of the investigator, be granted paid leave of absence from work, without loss of pay, in order to ensure that the necessary investigative activities can be carried out without interference that could be detrimental to the accused person. Paid leave shall be granted for the time necessary to carry out the relevant investigation tasks but may under no circumstances be extended beyond the duration of the investigation process.

External legal advisers shall be allowed to be present at hearings/declarations of affected parties, stakeholders, witnesses, etc., if deemed appropriate by the investigator.

In any investigation procedure, special care shall be taken to ensure compliance with the principles contained in this Policy and to guarantee confidentiality, impartiality, as well as the rights to privacy, defence, honour and the presumption of innocence of the persons under investigation. Furthermore, the procedure shall be transparent and will guarantee the right of information of the persons involved in the procedure.

4.2.4. RESOLUTION AND COMMUNICATION

Upon completion of all investigative actions, the System Manager shall prepare and issue a report containing at least the following content:

- A statement of the facts as reported (descriptive information on the communication) together with the identification code of the communication and the date of registration.
- Assessment of the content of the communication.
- The actions carried out in order to verify the credibility of the facts.
- The conclusions reached in the investigation and the assessment of the proceedings and the evidence supporting them.
- Measures adopted (if any).

Once the report has been issued, the System Manager shall take one of the following actions:

- a) Closure of the file, informing the whistleblower and, where appropriate, the person concerned.
- b) Proposal for the resolution of the file and, where appropriate, the corresponding proposals for action and/or proposal of disciplinary measures, with the possibility of delegating the latter power to another competent body.

A handwritten signature in blue ink, appearing to be "H. M.", located at the bottom right of the page.

- c) Relay to the Public Prosecutor's Office if, although there is no initial indication that the facts may constitute a criminal offence, this is apparent from the course of the investigation. If the offence affects the financial interests of the European Union, it shall be relayed to the European Public Prosecutor's Office.
- d) Forward the communication to the authority, entity or body considered competent for its processing.

The maximum period for responding to the investigation proceedings may not exceed three (3) months from the date of receipt of the communication, except in cases of particular complexity that require an extension of the period, in which case, this may be extended, by decision of the System Manager, up to a maximum of a further three (3) months.

The proposal for a decision shall be sent to the Managing Director or, where appropriate, to the Governing Body or competent body, which shall adopt and implement the final decision.

Whatever the decision, it shall be communicated to the whistleblower within five (5) business days of the decision being made, unless the whistleblower has waived this right or the communication is anonymous, as well as to all other concerned parties.

If the resolution issued concludes that a member of ESPUÑA GROUP has committed an irregularity, the appropriate disciplinary, administrative or legal proceedings will be initiated.

Likewise, if, as a result of the investigation, other facts are discovered that could constitute new irregularities allegedly committed by the same or different persons from those under investigation, the investigator shall propose the opening of a new file, or, if it is related to what has been investigated in the file under investigation, the extension of the investigation file, if it is considered to be more appropriate.

4.2.5. DISCIPLINARY MEASURES

When it is determined that the reported conduct constitutes an infringement in labour matters, ESPUÑA GROUP may adopt the appropriate measures in accordance with the applicable disciplinary regime and, specifically, with the provisions of the Collective Bargaining Agreement applicable to ESPUÑA GROUP and to the Spanish Workers' Statute.

Without prejudice to the fact that the mandatory labour regulations in force at any given time shall be observed in all cases, insofar as this allows it, the following

A handwritten signature in blue ink, appearing to be "J. J. J.", located at the bottom right of the page.

criteria, among others, may be considered for the purposes of assessing the severity of the conduct, for the purposes of grading the penalties to be imposed:

- Degree of intentionality.
- Failure to comply with prior warnings.
- Recurrence.
- Concurrence of several infringements in the same act or activity.
- Concurrence of concealment in the conduct carried out by the offender.
- Concurrence of continuity in the conduct carried out by the offender.
- The remedying of the non-compliance that gave rise to the infringement on the offender's own initiative.
- Compensation for damage caused by the offender.
- Level of responsibility in the organisation of the offender.
- Magnitude of the economic damage resulting from the infringement.
- Magnitude of any other non-financially assessable damage resulting from the infringement.
- Affectation of other employees or third parties.
- Collaboration with the organisation.

Notwithstanding the adoption of disciplinary measures, when the facts could be indicative of a criminal offence, the pertinent information shall be immediately forwarded to the Public Prosecutor's Office. However, if the evidence affects the financial interests of the European Union, the information will be forwarded to the European Public Prosecutor's Office.

5. DATA PROTECTION AND PRESERVATION

5.1. DATA CONTROLLER

In compliance with the provisions of the General Data Protection Regulation and the Data Protection Law, we hereby inform that any personal data that may be included in the communication will be included in a file owned by the company for its processing.

ESPUÑA GROUP undertakes to maintain strict protection of privacy, security and data preservation, as detailed in our policies and procedures and internal regulations on these matters. In this regard, these rules will also apply as regards all personal data relating to communications made in accordance with this Policy.

5.2. DATA COLLECTION

ESPUÑA GROUP collects the following personal data when processing communications (carrying out and investigating the same) in accordance with this Policy:

- Name and contact details of the whistleblower (unless reported anonymously) and their status as an employee of ESPUÑA GROUP.
- Name and other personal details of the persons mentioned in the complaint (witnesses, possible offender, etc.), if such information is provided (description of their functions, contact details and involvement or role in the reported facts).

5.3. PRESERVATION OF THE IDENTITY OF THE WHISTLEBLOWER AND OTHER PERSONS CONCERNED

ESPUÑA GROUP will preserve the identity and guarantee the confidentiality of the data corresponding to the persons concerned and to any third party mentioned in the information provided, especially the identity of the whistleblower if they have identified themselves. In this regard, the person to whom the facts reported in the communication refer shall in no case be informed of the identity of the whistleblower.

In this regard, the person submitting a communication has the right not to have his or her identity disclosed to third parties. The identity of the whistleblower may be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority only in the context of a criminal, disciplinary or sanctioning investigation.

These disclosures will be subject to the safeguards set out in applicable regulations. In particular, this information shall be provided to the whistleblower before his or her identity is revealed, unless such information could jeopardise the investigation or judicial proceedings.

5.4. DATA PRESERVATION

ESPUÑA GROUP will keep a record of all communications received. These records and the personal data contained therein shall be kept confidential in the Information Management System. Records shall be kept for no longer than is necessary and in any event for as long as is necessary to comply with any legal requirements applicable at any given time.

ESPUÑA GROUP will keep the personal data of the whistleblower for the time necessary to decide whether to initiate an investigation into the facts or conduct reported and, once a decision has been made, it will be deleted from the Ethical Channel, and may be processed outside the system to investigate the facts for the time necessary to reach a decision. Once the investigation of the communication has been completed and the appropriate actions have been

taken, if necessary, the data of those complaints that have been processed will be duly blocked to comply with the corresponding legal obligations in each case.

Personal data shall be deleted from the Ethical Channel within a maximum period of three (3) months from receipt of the communication, unless the purpose of its preservation is to provide evidence of the operation of the system and may continue to be processed outside the Ethical Channel if the investigation of the complaint has not been completed, for as long as necessary. In no case may data be kept for a period of more than ten years.

If it is decided not to act on the complaint lodged, the information may be retained in anonymous form.

5.5. ACCESS TO THE DATA

Access to the personal data contained in the Ethical Channel shall be limited, within the scope of their responsibilities and functions, exclusively to:

- a) The System Manager and whoever manages it directly.
- b) The external consultant involved in the investigation, with whom confidentiality agreements will be signed.
- c) The head of human resources of ESPUÑA GROUP or the duly designated competent body, only when disciplinary measures may be taken against an employee.
- d) The person in charge of ESPUÑA GROUP's legal services, should it be necessary to adopt legal measures in relation to the facts described in the communication.
- e) The persons in charge of processing that may be appointed.

5.6. PURPOSE OF THE PROCESSING

Only personal data that are strictly necessary for the purposes of management, processing and investigation of communications relating to the commission of irregularities are processed, as well as to carry out the necessary actions for the investigation of the reported facts, including, where appropriate, the adoption of the corresponding disciplinary or legal measures.

Personal data will not be used for any purpose other than that stated.

5.7. RIGHTS OF THE PERSONS CONCERNED

The parties concerned, at any time and under the terms provided for in the applicable regulations, may exercise the following rights regarding their personal data: access, rectification, deletion (right to be forgotten), limitation of processing, objection, portability, decision on automated processing, information and complaints.

If the person to whom the facts related in the communication relate to exercises the right to object, it shall be presumed that, in the absence of proof to the contrary, there are compelling legitimate grounds legitimising the processing of his or her personal data.

If they consider it appropriate, persons concerned may also lodge a complaint with the competent data protection authority.

5.8. INFORMATION ON DATA PROTECTION AND EXERCISE OF RIGHTS

Anyone wishing to obtain further information about the processing of their personal data may contact ESPUÑA GROUP by e-mail at info@espuna.es

6. EXTERNAL INFORMATION CHANNELS

Whistleblowers may, alternatively, send their communication directly, or after sending the communication through ESPUÑA GROUP's Ethical Channel, to the public authorities by means of the external information systems set up by the Independent Whistleblower Protection Authority (A.A.I. in Spanish) or the corresponding regional authorities or bodies, in accordance with the terms established in Title III of the Law on the Protection of Whistleblowers.

7. NON-COMPLIANCE

This Policy is of mandatory compliance for all members of the organisation. Its breach will constitute an infringement and ESPUÑA GROUP will adopt the appropriate disciplinary measures, in accordance with labour legislation and the Penalties Regime contained in the applicable Collective Bargaining Agreement, without prejudice to other responsibilities that the person in breach may have incurred.

8. APPLICABLE REGULATIONS

- DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 23 October 2019, on the protection of persons who report breaches of Union law ("Whistleblower Directive").

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 27 April 2016, relative to the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (“General Data Protection Regulation”-GDPR).
- Article 31 bis paragraph 5 of the Spanish Criminal Code.
- Law 2/2023, of 20 February, regulating the protection of persons who report breaches of regulations and for combating corruption, which aims to transpose Directive (EU) 2019/1937 into Spanish law. (“Whistleblower protection law”).
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights. (“Data Protection Law” - LOPD-GDD).
- Circular 1/2016 of the State Attorney General’s Office, of 22 January, on the criminal liability of legal entities in accordance with the reform of the Criminal Code carried out through Organic Law 1/2015.
- UNE- ISO 37002:2021 on Whistleblowing Management Systems. Guidelines.
- UNE-ISO 37301:2021 on Compliance management systems. Requirements with guidance for use.

9. ENTRY INTO FORCE, VALIDITY AND REVIEW

The entry into force of this Policy shall take place at the same time as the date of approval, modification or update of this document and shall remain in force until the Policy is repealed.

This Policy shall be reviewed periodically to detect possible weaknesses or points for improvement and to update and/or improve its provisions.

This Policy will be reviewed extraordinarily and, where appropriate, modified when significant circumstances of a legal, organisational or any other nature arise that justify its immediate adaptation and/or updating.

A handwritten signature in blue ink, appearing to be a stylized name or set of initials.