PROCEDURE FOR MANAGING, INVESTIGATING AND RESPONDING TO REPORTS RECEIVED THROUGH THE INTERNAL REPORTING SYSTEM

persán

Date of approval and registration of changes to the document

Version	Date	Description
1.0.	06/20/2023	Approval by the Board of Directors: update of the Internal Information Channel (Law 2/2023).
2.0.	08/08/2024	Approval by the Board of Directors: update of Phase 1 of the certification process for the Criminal *Compliance* Management System in accordance with UNE 19601:2017.
3.0.	09/25/2025	Approval by the Board of Directors: update of *the Criminal Compliance Management System* (organizational changes).

TABLE OF CONTENTS

1. DEFINITIONS

The following are the definitions of those concepts that will be used frequently in this document (shown in *Cursive*):

- ***PERSÁN/the Organization/the Company***: includes the company PERSÁN, S.A..

- ***Compliance Office***: an internal collegiate body within *PERSÁN* that has autonomous powers of initiative and control and is entrusted, among other tasks, with the responsibility of supervising the operation and observance of *the Organization's Criminal Compliance Management System* both within and outside Spanish national territory. The existence of this body responds both to the requirements established in Spanish legislation (Article 31 bis of the Spanish Criminal Code) and to international best practices in terms of the supervision of *the Criminal Compliance Management System*.

- ***Risk & Compliance Department:*** composed of the *Compliance Office*, as well as the Risk Management and Internal Audit areas. In addition to the powers established for the *Compliance Office*, its main function is to supervise financial and non-financial integrity, the effectiveness of internal controls, and corporate risk management. *The Risk & Compliance Department* will be led by the *Chief Risk & Compliance Officer*.

- ***Board of Directors***: the body with fundamental responsibility and authority for *PERSÁN's* activities, governance, and policies, to which *Management Committee* reports and is accountable.

- ***Management Committee***: the high-level body within *PERSÁN* that reports directly to *the Board of Directors*. Currently composed of the *PERSÁN* Management Committee.

- ***Members of the Organization***: members of the *Board of Directors*, members of *Management Committee*, defined workers or employees, temporary or under collaboration agreements, volunteers of the *Organization*, and all other persons under the hierarchical subordination of any of the above.

- ***Business partners***: any legal or natural person, except for *Members of the Organization*, with whom the *Organization* maintains or plans to establish some type of business relationship. This includes, but is not limited to, suppliers, customers, and, in general, natural and legal persons who contract with *PERSÁN* for the delivery of goods or provision of services.

- ***Third party***: natural or legal person independent of the *Organization*.

- ***Ethics Channel/Internal Reporting System***: set of measures adopted in accordance with Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption (also referred to as the "Whistleblower Protection Law") for the management of communications relating to violations of the regulations referred to in said text.

- ***Head of the Internal Reporting System***: the *Chief Risk & Compliance Officer* has been appointed as the person responsible for the diligent processing of *inquiries* or *complaints* received through the *Ethics Channel*, and must perform their duties with full autonomy and independence from the rest of *PERSÁN's* bodies.

- ***Communication/Report:*** statement by which any *Member of the Organization*, *Business Partner*, or *Third* Party records a question regarding the scope, interpretation, or compliance with the regulations applicable to the *Organization*. Depending on its content, a *Communication* may contain a *Consultation* or a *Complaint*.

- ***Consultation:*** *Communication* by which any *Member of the Organization*, *Business Partner*, or *Third* Party requests clarification, a response, or criteria regarding the scope, interpretation, or compliance with the regulations applicable to *PERSÁN*.

- ***Complaint:*** *Communication* relating to a possible *breach* of the regulations applicable to *PERSÁN*.

- ***Whistleblower/Complainant***: natural or legal person who files a *Consultation* or *Complaint*. The figure of *the Whistleblower* includes *Members of the Organization, Business Partners, Third Parties*, and any person with a present or future connection to the above contexts.

- ***Reported party***: natural or legal person accused of an alleged breach that is being investigated by *the Head of the Internal Reporting System*.

- ***Breach/Failure/Non Compliance***: behavior, whether active or omissive, that constitutes a violation of the regulations applicable to *PERSÁN*. Depending on its severity, a *breach* can range from a mere formal *breach* of a requirement included in an internal regulation to the commission of acts constituting a crime potentially attributable to *PERSÁN*.

- ***Notification***: the act of informing the parties involved in the procedure in order to ensure its proper conduct and respect for their rights.

- ***Good faith report***: a report made in accordance with the provisions of this *Policy* and based on facts or evidence from which the existence of a *breach* of current legislation or internal regulations can reasonably be inferred. *A report* is considered to be made in good faith when it is made without the intention of revenge or of causing professional or employment harm to *the reported party* or a *third party*.

- ***Record book***: a tool used by the *Head of the Internal Information System* to ensure the traceability and security of *communications* received through the *Ethics Channel*.

- ***Whistleblower Protection Authority (AAI)***: an independent administrative authority, as a public law entity at the state level, which will act in fulfillment of its main function of protecting *whistleblowers*. Its functions include, among others, the management of its own external channel, the processing of disciplinary proceedings, and the imposition of sanctions.

- ***Retaliation***: an act or omission prohibited by law, or which, directly or indirectly, involves unfavorable treatment that places the *Whistleblower* or the parties involved at a particular disadvantage in relation to others in the workplace or professional context, solely because of their status in relation to the *Report*, or because they have made a public disclosure.

- ***Internal Information System Policy***: document establishing the principles governing the *Organization's Internal Information System*, as well as the rights and obligations of its users.

- ***Procedure for the Management, Investigation, and Response to Communications received through the Internal Information System (IRS)***: set of provisions contained in this document (hereinafter also referred to as the *"Procedure*").

- ***Criminal Compliance Management System***: an organizational and management system for the prevention of non-compliance, whose objective is the prevention, detection, and management of risks through its integration into business processes, as well as measurement for continuous improvement, and whose essential basis is represented in the Criminal *Compliance* Policy and the *Compliance Program*. Hereinafter also referred to as the *"System*."

- ***Criminal Risk/Compliance Risk***: risk related to the development of conduct that could constitute a *crime/breach* attributable to *PERSÁN* or any of the entities within the scope of criminal control.

2. OBJECTIVE OF THE PROCEDURE

On 23 October 2019, 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, hereinafter also referred to as the "***Whistleblowing Directive***", was adopted with the aim of strengthening the application of Union law and policies in specific areas by setting common minimum standards which ensure a high level of protection of persons who report breaches of European Union law.

On 20 February 2023, Law 2/2023 of 20 February on the protection of persons who report regulatory infringements and the fight against corruption, was approved in Spain in order to transpose the Whistleblowing Directive. This law (hereinafter, the "***Whistleblower Protection Law***") came into force on 13 March 2023.

PERSÁN, within the framework of its *Criminal Compliance Management System* and in accordance with the provisions of the *Whistleblower Protection Law*, has implemented an *Internal Reporting System*, through which any *Member of the Organization, Business Partner, or Third Party* who knows or suspects a Regulatory *breach* (either of the law or its implementing regulations, or of internal corporate regulations) committed by a *Member of PERSÁN* or by *Third Parties* who are in contact with it in the course of their work or professional activities, may bring it to the attention of *the Organization,* either identified or anonymously.

The *Internal Reporting System* may also be used to refer to *PERSÁN* any *queries* relating to the scope, compliance, and interpretation of the regulations applicable to *PERSÁN*.

To this end, *PERSÁN* has approved an *Internal Information System Policy* that sets out the general principles of *the Internal Information System* and the protection of *whistleblowers*, such as the material and personal scope of application, the role of *the Head of the Internal Information System*, the protection of *whistleblowers*, the prohibition of *retaliation*, measures to protect against *retaliation*, sanctions, etc.

Likewise, and as a complement to the *Internal Information System Policy,* the *Organization* has approved and implemented this *Procedure for the management, investigation, and response to communications received through the Internal Information System* ("**IRS *Procedure***") with the aim of regulating the use of *the Internal Information System* and the procedure for managing, investigating, and resolving *Communications* received regarding possible infringements, guaranteeing the confidentiality, independence, and protection of *the Whistleblower,* as well as compliance with the guarantees and requirements of the *Whistleblowing Directive* and the *Whistleblower Protection Law.*

3. SCOPE OF APPLICATION

This *Procedure* shall apply to all *Communications* received in the *Internal Information System,* through any of the communication channels enabled within the framework of *the Ethics Channel*.

This *Procedure* affects all *Members of the Organization*, so that everyone must comply with its content, regardless of their position and role.

Likewise, this *Procedure* also applies to any person who intends to report a possible *Breach* that may have occurred in a professional context.

In this regard, the *Procedure* is binding on persons who, although not *Members of the Organization*, are aware that a *Breach* has occurred in their relationship with *PERSÁN*. Examples include *business partners* and *third parties*.

Communications received may relate to any *breach* of the law or regulations applicable to *PERSÁN*.

4. INTERNAL REPORTING CHANNEL ASSOCIATED WITH THIS PROCEDURE

PERSÁN has set up an internal reporting channel to report any matters included in the material scope of application defined in Section 2 of the *Internal Reporting System Policy*. These reports may be sent as follows:

1. **Written *communications***, via the technological platform set up by *PERSÁN* https://persan.integrityline.com/.

2. **Verbal *communications*,** requesting the *Head of the Internal Information System* to hold a face-to-face meeting to present the *Communication*. In this case, the meeting must be held within a maximum period of seven (7) calendar days from the request.

3. **Through a superior,** who will be obliged to forward this *Communication* to *the Head of the Internal Information System* within a period not exceeding two (2) working days from receipt of the information, or, where appropriate, to enter the *Communication* received via the platform indicated in point 1 above.

In the case of verbal *Communications*, with the prior consent of *the Whistleblower*, the conversation between the Whistleblower and the *Head of the Internal Information System* may be recorded—informing the Whistleblower of the processing of their data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 – (in a secure, durable, and accessible format) or transcribed accurately by the *Internal Reporting System Manager,* with the *Whistleblower* having the right to check, correct, and accept the transcript with their signature.

Regardless of the communication channel used, the *Whistleblower* may designate a preferred communication channel for receiving *Notifications* about the status of their *Communication* or for contacting them to request additional information and/or clarification.

Notwithstanding the above, any formal *Communication* from a judicial body or Public Administration shall be considered a valid means of becoming aware of a *Breach*.

The *Internal Reporting System* **is also open to *Business partners* and *Third parties*** outside *PERSÁN*.

Communications may be made either **nominatively** or **anonymously**.

5. PERSONAL CONFLICT OF INTEREST

In the event of **a conflict of interest**, i.e., if the person affected by the *Communication* is one of the *Members of the Compliance Office,* the *Whistleblower* may address the *Communication* to any of the other *Members of the Compliance Office,* who will then take over the management of the investigation, with the affected *Member of the Compliance Office* being recused from the management of the *Communication*.

The same shall apply when there is a conflict of interest/recusal of *the Head of the Internal Information System* in dealing with a specific matter, who shall voluntarily withdraw from the outset or from the moment their involvement becomes known during the investigation. In this regard, it will be the *Board of Directors* (in the case of *complaints* about events that may give rise to criminal liability for *PERSÁN)* who will decide on the replacement for the proceedings.

6. CONFIDENTIALITY

All information provided within the material scope of application of the *Internal Reporting System Policy*, regardless of the material format in which it is contained and the form in which it was provided, is strictly confidential ("**Confidential Information**").

All individuals who receive this type of information undertake the obligation to maintain the strictest secrecy regarding the confidential information that they may have access to, especially any information considered to be of a personal nature or, as applicable, the identity of the *whistleblower*.

The *Members of the Compliance Office* shall use the confidential information only for the purposes of performing the functions entrusted to them and in strict compliance with the *Internal Reporting System Policy* and this *Procedure*. They are also committed to ensuring the integrity of the information contained in the internal channel, and will not disclose their passwords or usernames of applications and systems owned by PERSÁN to any *third party*.

According to the applicable regulations, the identity of the *whistleblower* may only be disclosed to the judicial authority, the Prosecution Ministry or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation.

Any *Failure* to comply with this obligation by those who have access to Confidential Information shall be grounds for disciplinary dismissal. In this case, the perpetrator shall be liable for all damages arising for PERSÁN or the *whistleblower* as a result of willful or negligent *non-compliance* with this obligation.

7. PROTECTIVE MEASURES FOR INDIVIDUALS INVOLVED IN THE FACTS REPORTED

PERSÁN will ensure that the persons *reported* are heard in the context of the internal company investigation, enjoy the right to the presumption of innocence, the right to defense, and the right to access the file under the terms regulated in the *Whistleblower Protection Law,* as well as the other rights that protect them as established in the *Internal Information System Policy*.

Likewise, the identity of the person who is the subject of *the report* will be protected and treated confidentially, as will the facts *reported*, in the same way as the identity of *the whistleblower* themselves, always within the limits and exceptions that may be necessary to ensure the successful outcome of the investigation or any communication to the competent authorities.

8. RECEIPT OF REPORTS AND FILE CREATION

8.1 Acknowledgement of receipt

Upon receipt of any *Communication* through the *Internal Information System*, the *Head of the Internal Information System* will acknowledge receipt of the *Communication* within a maximum of seven (7) calendar days of receipt, unless such action could jeopardize the confidentiality of the *Communication*.

The acknowledgment of receipt will include initial information on the processing of personal data in accordance with section 15, "*Data Protection*," of the *Internal Information System Policy*. In addition, you will be told where you can find information on the processing of your personal data.

Similarly, the *Whistleblower* will be expressly informed that their identity (if they have identified themselves) will be preserved in all cases and will not be disclosed to the persons to whom the reported events refer or to *third parties*.

8.2 Request for additional information

If the information received is considered insufficient, the *Internal Information System Manager* will request, at the time of acknowledging receipt—or even subsequently—that *the Whistleblower* provide further information. It is advisable that the request sent details the specific aspects of the information provided that need to be expanded upon. In this process, exhaustive information on the reported *breach* will not be necessary, only that which is strictly essential for the preliminary formation and management of the file.

8.3 Creation of the initial file

With the information received, the *Head of the Internal Information System* will create a file for each individual case, which will be conveniently numbered and classified with an identification code and the date of registration, for the purposes of better identification within the *Register* regulated in section 12.2 *"Register of communications*."

If different communications are received about the same event or related events, the *Head of the Internal Information System* may combine the different files.

9. ANALYSIS AND PRELIMINARY DECISION ON THE REPORT RECEIVED

9.1 Preliminary analysis of the report received

Once the *Communication* has been received and its receipt acknowledged to the *Whistleblower*, the *Head of the Internal Information System* will carry out a preliminary analysis to verify the substance of the information, its sufficiency and plausibility, the credibility of *the Whistleblower, and* the relevance of the reported events, determining whether they may constitute a violation of European Union law, a serious or very serious criminal or administrative offense, or *a breach* of internal regulations.

For this preliminary analysis, as well as for the other phases defined below, the *Head of the Internal Information System* may request advice from any internal department deemed appropriate, as well as from external *third-party* experts in the field, depending on the factual or legal complexity of the *report* received.

9.2 Preliminary decision on the report received

Based on the results of the preliminary analysis, the *Head of the Internal Information System* shall adopt one of the following decisions , within ten (10) business days of acknowledgment of receipt, and shall record the reasons for the decision:

a. Non-admission of the report and immediate dismissal of the file in the following cases:

- When the reported facts do not constitute any of the cases referred to in the material scope of application *of the Internal Reporting* System—defined in section 3, "*Material scope of application*," of the *Internal* Reporting *System Policy*.
- When the *Communication* is a mere reproduction of a previous one that has been previously rejected or duly investigated, without providing new information.
- When the content of the *report* is manifestly irrelevant or the reported facts are implausible or the *reporter* lacks credibility.
- When the information is insufficient to proceed with any further action.

b. Admission of the report and initiation of the corresponding investigation file in relation to the facts reported, in accordance with the provisions of this *Procedure*.

c. Immediately forward the information to the Prosecution Ministry when the facts reported could be indicative of a crime or to the European Public Prosecutor's Office in the event that the facts affect the financial interests of the European Union.

9.3 Information to the whistleblower about the file

In all of the above cases, the *Head of the Internal Reporting System* will send *a notification* to *the Whistleblower* regarding the rejection or acceptance of the *report*, as well as any additional measures that may have been taken, within five (5) business days of the conclusion of the preliminary analysis, unless the report was anonymous or the *Whistleblower* has opted out of receiving *notifications*.

9.4 Additional measures

Parallel to the adoption of the decisions described in section 9.2 above, the *Head of the Internal Information System* may adopt, in coordination with the *P&Or,* where appropriate and following the procedure established in the applicable Collective Agreements or labor regulations, all measures that, in view of *the* reported *Breach*, are considered necessary to strengthen *PERSÁN's Criminal Compliance Management System*, for the successful outcome of the future investigation and/or for the effective protection of *the Whistleblower*.

10. INVESTIGATION PROCEDURE

When, in accordance with section 9.2.b), it is decided to initiate an investigation procedure, the following steps shall be taken:

- Choose the investigation strategy (see section 10.1).
- Plan the investigation (see section 10.2).
- Notify the individuals concerned (see section 10.3).
- Conduct the investigation itself (see section 10.4).
- Document the investigation procedure (see section 10.5).
- Prepare the final report (see section 10.6).
- Final actions (see section 10.7).

10.1 Choice of investigation strategy

Depending on the scope, extent, and persons allegedly involved in the *breach* in question, the *Head of the Internal Reporting System* will assess the investigation strategy to be developed for the specific case, choosing one of the following options:

a. The investigation procedure will be led and managed by one of the *members of the Regulatory Compliance Office*, appointed by the *Head of the Internal Information System*, without prejudice to any consultations or specific support that may be required from other departments for its full substantiation. These departments are expressly obliged to provide the *Head of the Internal Information System* with any information that may be required and that is in their possession or knowledge.

b. The investigation procedure may be supported by a specific internal body or department of the *Organization,* when this is advisable due to its specialization or the specific knowledge required for the investigation.

c. The investigation procedure will be outsourced in whole or in part, depending on whether the circumstances of the case warrant the specific advice of a *third party* expert in a particular area or a fully developed investigation from outside *PERSÁN.* The choice of this strategy will be particularly advisable in cases where it is considered that the investigation may require a special standard of confidentiality.

If there is any kind of conflict of interest involving any of the members of the specific team assigned to the investigation, that member must withdraw from the investigation and may not participate in it.

All persons actively participating in the investigation shall be obliged to maintain strict confidentiality regarding the facts, data, or names they learn as a result of the investigation.

10.2 Plan the investigation

Both the designated *member of the Regulatory Compliance Office* and any other designated investigator shall plan the investigation with the aim of clarifying the facts and identifying those responsible. Such planning may include the following elements:

a. Identifying the legislation, policies, procedures, or internal regulations affected, as well as the *criminal or compliance risks* that may arise from *the breach*.

b. Identifying all information and documents that may be relevant and whose review is considered useful (emails, websites, audiovisual surveillance and security media of the entity, attendance lists, passwords or electronic security devices, accounting media, etc.).

   In the event of accessing any document that may contain personal content but is stored on professional media and/or equipment, access must be carried out prudently (always taking into account the triple assessment of suitability, necessity, usefulness, and proportionality) and ensuring the chain of custody.

c. Determine, if necessary, in a sufficiently reasoned manner and with the collaboration of the *P&O* Department, the need and, where appropriate, the urgency of adopting precautionary measures with respect to the subjects affected by the *Communication*. Precautionary measures are not limited, but may include the following:

   - Transferring the subjects under investigation to another division, area, or department or temporarily changing their location.
   - Modify the usual tasks or responsibilities of the subjects affected by the *Communication*.
   - Immediately suspend the individuals affected by the *Communication* from their employment and salary.

d. Define the steps to be followed in the investigation and in the various meetings with those affected in order to ensure its proper conduct, identifying interviewees, relevant questions to be asked, possible witnesses to the reported incident, among others.

e. Include in the investigation file all information that may be of interest in relation to the working life of the person affected at *PERSÁN* (employment history, previous contingencies, policies, procedures, and regulations of the *Organization* that are particularly applicable, etc.).

f. When planning the investigation, always try to promote:

   - The objectivity and fairness of the process;
   - The privacy of the subjects under investigation; and
   - Minimizing the impact of the investigation.

Always ensuring compliance with the principles governing the *Internal Information System* established in the *Internal Information System Policy*.

10.3 Communication to affected parties

Prior to initiating the investigation, the designated *member of the Regulatory Compliance Office* or the person leading the investigation (hereinafter, ***"the* investigator**") will contact the *reported* parties*,* identifying themselves as the person in charge of investigating the possible irregularity or infringement reported, informing them of the facts attributed to them and the main milestones that may occur during the investigation.

In addition, the person concerned will be informed of their right to submit written allegations and of the processing of their personal data, their right to be heard at any time, and other rights to which they are entitled under the *Whistleblower Protection Law* and the *Internal Information System Policy*.

The above will be carried out unless, in the opinion of the investigator, and in order to prevent evidence from being destroyed and/or concealed, or otherwise prejudicing the investigation itself, the *Notification* to *the Accused* must be made at a later date and, in any case, when the statement of the person concerned is required, at the time of the hearing or before the end of the investigation process.

Under no circumstances shall the identity of *the Informant* be disclosed to the persons concerned, nor shall access to the *Communication* be granted.

Without prejudice to the right to submit written arguments, the investigation shall include, whenever possible, an interview with the person affected by the *Communication* in which, always with absolute respect for the presumption of innocence, they shall be invited to present their version of the facts and to provide any evidence they deem appropriate and relevant.

10.4 Conduct of the investigation

The investigation shall include all investigative procedures that are appropriate for clarifying the facts, identifying those responsible, and determining any corrective measures that may need to be taken. The investigation shall always be conducted with the utmost respect for the duty of confidentiality and protection of *the Whistleblower* and, in all cases, respecting the presumption of innocence, the right to be heard, and the right to honor of *the Accused*.

Some of the main steps that may form part of the investigation are detailed below:

a. Conducting an interview with the *Whistleblower* in order to obtain more information about the *Communication* submitted.

b. Statements from the subjects affected by the *Communication*.

c. Conducting questionnaires and interviews with witnesses.

d. Arranging hearings with the superiors and colleagues of the individuals affected by the *Communication*, as well as with any other persons deemed necessary.

e. Gathering as much information as possible through *PERSÁN* documentation.

f. If essential to clarify the facts, adopt surveillance measures through detectives or computer, telematic, or audiovisual means, provided that these meet criteria of reasonableness, suitability, and proportionality, ensuring at all times the right to privacy of *the Member of the Organization* and the right to secrecy of communications.

g. Seek external assistance from other professionals.

h. Any other steps that the *Head of the Internal Information System* deems necessary to clarify the facts, including the potential maintenance of *Notifications* with the *Informant* and, if deemed necessary, the request for additional information from the Informant.

The duration of the investigation proceedings may not exceed three months from the date of receipt of the *notification*. Exceptionally, in particularly complex cases requiring an extension of the deadline, this may be extended for up to a maximum of three additional months, provided that reasons are given.

10.5 Documentation of the investigation procedure

It shall be essential to include in the file detailed documentation of the entire investigation procedure carried out, including the initial investigation plan, all documents collected, and the minutes of the interviews conducted.

All interviews conducted shall be duly documented, either by means of a complete and accurate transcript prepared by *the Head of the Internal Information System*, which shall be signed by the interviewees—after they have been given the opportunity to check and correct it—and by the *Head of the Internal Information System*, or by means of a recording in a secure, durable, and accessible format , after warning the *Whistleblower* that the *Communication* will be recorded and informing them of the processing of their data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016. Likewise, in all cases, the collection, processing, and disclosure of personal data will be reported in accordance with current data protection legislation.

10.6 Final report

Once all the investigation procedures have been completed, the investigator will prepare a report of conclusions that must contain a brief description of the following elements:

a. **Nature of the incident**: The individuals involved, the nature of the events, the date, the place, and the circumstances in which they allegedly occurred, the legal provisions or internal regulations that were violated or jeopardized shall be identified, to the extent possible, including a statement of the facts reported together with the identification code of the *Communication* and the date of registration.

b. **Identity of the investigator**: The person or persons on the working team who carried out the investigation shall be duly identified.

c. **Classification of the *report*** for the purposes of determining its priority or otherwise in its processing.

d. **The actions taken** to verify the veracity of the facts.

e. **List of relevant facts and findings**: The most relevant facts identified during the investigation procedure shall be reported, differentiating them according to the source of information from which they were identified, for example:

- *PERSÁN* documentation;
- Information provided by the *informant*, or;
- Information obtained from interviews with the subjects affected by the *Communication* and with witnesses.

f. **Conclusions and assessment of the facts**: The conclusions drawn by the investigator and the evidence supporting them shall be specified, as well as their assessment of the facts reported, and two possible actions may be proposed:

- **Proposal to continue the proceedings** if it is considered that, based on the proceedings carried out, there is sufficient evidence that the subject concerned has committed any of the infringements set out in section 3 of the *Internal Information System Policy*.
- **The proceedings will be closed** if it is deemed that the act does not constitute one of the infringements referred to in section 3 of the *Internal Information System Policy*, if there is insufficient evidence to justify its perpetration, or if the perpetrator cannot be identified. The closure of the proceedings will be communicated to *the Whistleblower* and, where applicable, to the person affected by the *Communication*.

10.7 Final actions

Once the final investigation report has been prepared, it shall be immediately forwarded to *the Head of the Internal Information System*.

The final investigation report shall be filed together with the rest of the investigation file.

11. CONCLUSION OF THE PROCEDURE

11.1 Responsible body

The *members of the Compliance Office*, as *the Internal Information System Manager*, are the persons responsible for responding to any *breaches* that occur at *PERSÁN*, resolving the proposals submitted by the investigator.

However, in the event that the investigation has affected a *member of the Compliance Office*, that member must refrain from participating in the part of the meeting or meetings in which this matter is addressed.

11.2 Hearing procedures

Once the final investigation report has been received, the *Head of the Internal Information System* will inform the *accused* of the outcome of the investigation, who will be given a reasonable period of time to submit any relevant arguments in writing or in an interview. The *notification* to *the accused* of the final report shall omit any information about the nature of the procedure followed, the facts, or the measures taken that could reveal the identity of *the whistleblower or* violate the *Whistleblower Protection Law* and/or personal data protection regulations.

11.3 Decisions of the Head of the Internal Information System

Once the deadline for the *accused* to submit their arguments has passed, one of the following decisions may be taken:

a. **Admit or reject the evidence requested by the affected party**, giving reasons.

b. **Request that** the investigator **carry out additional investigative procedures**.

c. **Close the case** due to insufficient evidence or lack of relevant facts, proceeding to file it.

d. **Declare a *breach* of *PERSÁN***, with the possibility of imposing a penalty or taking additional measures.

e. When, after the final report has been issued, it is determined that the facts could constitute a crime, the information obtained in **the investigation will be forwarded to the Public Prosecutor's Office** immediately. If the facts affect the financial interests of the European Union, the information will be forwarded to the European Public Prosecutor's Office.

11.4 Sanctions

The sanctions that may be imposed on *Members of the Organization* in each case shall be those provided for in the Workers' Statute, in the applicable Collective Agreements, or in the applicable labor legislation.

Such sanctions shall be graded according to the seriousness of the acts committed, taking into account circumstances such as recidivism, damage or harm caused, the circumstances of the victims, if any, among others.

Additional measures may also be taken in addition to disciplinary measures, including the filing of appropriate claims or the reporting of the facts to the appropriate administrative, police, or judicial authorities.

The application of these sanctions will be channeled through the *P&O* Department.

11.5 Additional measures

Additional response and reaction measures may be taken, including but not limited to:

a. Reporting the facts to any authority with jurisdiction over them, whether administrative or judicial.

b. Evaluating previous indications of similar violations and ensuring that appropriate measures are taken to understand the cause of *the non-compliance*.

c. Taking compensatory action against any person or entity that may have been harmed by the events.

d. Establishing processes, procedures, and controls to prevent similar *breaches* and proposing organizational or preventive measures of any kind.

e. Make decisions related to the *communication*, training, or internal dissemination of the facts, both at the level of *PERSÁN's* body or unit (division, area, or department) and at the general level (to all *members of the organization*) when this is considered an effective tool to prevent similar *breaches* in the future (always with due caution in matters of personal data protection).

11.6 Notification of decisions

The decisions taken once the internal investigation has been completed shall *be notified* immediately and in writing to the persons concerned, as well as to *the Whistleblower*. In the notification to the *accused* or the *complainants*, any information on the nature of the procedure followed, the facts or the measures taken may be omitted in order to comply with the regulations governing the protection of personal data.

12. RETENTION OF DOCUMENTATION

12.1 Retention periods

Personal data collected through the *Internal Information System* will be retained in accordance with the provisions of applicable legislation. Specifically, pursuant to the provisions of Article 32.4 of the aforementioned Law 2/2023 and Article 24.4 of Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights, i.e., three (3) months after receipt of the *Communication* without any investigation having been initiated, the data will be deleted, unless the purpose of the retention is to leave evidence of the functioning of *the System,* in which case it will be kept anonymized.

However, if it is necessary to process the personal data for a longer period of time in order to continue the investigation or, where appropriate, because it is considered necessary to initiate the appropriate legal actions, the data will be retained for as long as necessary to conclude the investigation or for *PERSÁN* to take the corresponding actions.

12.2 Record of reports

PERSÁN will keep a record of all *Reports* and *Queries* it may receive through the *Internal Information System*, compiled in the so-called "*Record book*," managed through the EQS platform, complying at all times with the established confidentiality requirements, and for the time strictly necessary and proportionate to comply with the legal and regulatory requirements of the European Union.

The Internal Reporting System Manager will record the *Communications* received, including the following information:

- Date of receipt.
- File number.
- Date on which the maximum investigation period of three (3) months ends.
- Means or channel of receipt of the *Communication*.
- Identity of *the informant* or, where applicable, indication that the *communication* is anonymous.
- Identity of *the person* or *persons* reported in the *communication*.

Likewise, the *Head of the Internal Information System* shall record the actions and investigations carried out in each file, including the following information:

- Acknowledgment of receipt of the *Communication*.
- Admission/non-admission of the *Communication*.
- Notification to *the Whistleblower* of the acceptance or rejection of the *Report*.

- If requested, meeting with the *Whistleblower* within a maximum period of seven (7) calendar days.

- Where appropriate, request for additional information from *the Whistleblower*.

- Notification to *the accused* of the allegations against them and their rights.

- Hearing with the *accused*.

- Investigation proceedings carried out.

- Issuance by the *Head of the Internal Information System* of the final report with the proposed resolution.

- Notification of the final report to the person(s) *reported*.

- Final decision by *the Head of the Internal Information System*.

- Where appropriate, communication to the competent authorities if the facts constitute a crime.

- Other actions.

When the *communication* has been made verbally, *PERSÁN* reserves the right to document the verbal *communication* in one of the following ways:

1. By recording the conversation in a durable and accessible format.

2. Through a complete and accurate transcript of the conversation made by the *Head of the Internal Information System*.

In any case, the *Whistleblower* has the right to check, rectify, and accept the transcript by signing it. *PERSÁN* will ensure, subject to the *Whistleblower's* consent, that complete and accurate records of the meeting are kept in a durable and accessible format.

Only at the reasoned request of the competent judicial authority, by means of a court order, and always within the framework of legal proceedings and under the supervision of that authority, may the contents of *the Register* be accessed in whole or in part.

The data contained in this *Register* shall be kept only for as long as necessary and, in any case, shall not be kept for a period exceeding <u>ten (10) years</u>.