INTERNAL REPORTING SYSTEM POLICY

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.	09/21/2023	Modification at the request of employee representatives.
3.0.	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.
4.0.	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 *senior management* 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***: set of provisions contained in this document (hereinafter also referred to as the "Policy").

- ***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 INTERNAL REPORTING SYSTEM POLICY

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 legislation 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 within the framework 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*.

PERSÁN recognizes all the principles set out in the *Whistleblowing Directive* and the *Whistleblower Protection Law* as its own and, in order to emphasize this commitment, approves this *Internal Reporting System Policy*, whose provisions are complementary to those set out in the *Procedure for the Management, Investigation, and Response to Communications received through the Internal Reporting System*.

The purpose of this *Policy* is to establish the general principles of *PERSÁN's Internal Reporting System*, the rights of *Whistleblowers*, and the procedure governing how they can bring to the attention of *the Head of the Internal Reporting System* any facts relating to the matters referred to in the following section on the scope of application.

Likewise, to regulate the use of *the Internal Information System* and the procedure for investigating and resolving *Communications* received, *PERSÁN* has approved and implemented the *Procedure for the Management, Investigation, and Response to Communications received through the Internal Information System* ("***IRS Procedure***"), the content of which also complies with the requirements of the *Whistleblowing Directive* and the *Whistleblower Protection Law*.

3. MATERIAL SCOPE OF APPLICATION

This *Policy* protects individuals who report, through any of the channels established in the following *Policy*:

1. Actions or omissions that may constitute **a breach of European Union law**, provided that:

    a. These fall within the scope of the acts of the European Union listed in the annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons who report breaches of Union law, regardless of how they are classified under domestic law.

    b. These affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union ("TFEU").

    c. These affect the internal market, as referred to in Article 26(2) TFEU, including infringements of European Union rules on competition and State aid, as well as infringements relating to the internal market in connection with acts that infringe corporate tax rules or practices aimed at obtaining a tax advantage that distorts the object or purpose of the applicable corporate tax legislation.

2. Actions or omissions that may constitute **a serious or very serious criminal or administrative offense**.

3. In addition, the *Internal Reporting System* may also be used to report actions or omissions that may constitute a ***breach* of the *Organization's* internal regulations** that do not constitute a violation of European Union law or a serious or very serious criminal or administrative offense, including the principles and values that guide the conduct of all *Members of the Organization*.

Communications related to strictly labor issues or professional performance (career development, remuneration, vacations, etc.) are excluded from the scope of application of *the Internal Information System*. In such cases, the matter will be referred, if appropriate, to the *P&O* department.

Likewise, the process of reporting *Communications* through the *Internal Reporting System* should not be used to report events that pose an immediate threat to life or property. In such cases, the situation should be handled directly through the competent authorities or by calling the emergency number (112). In addition, when circumstances so require, the relevant superior should be notified immediately.

Essentially, the *Internal Information System* may be used to report any *Breach* committed by *PERSÁN Members*, *Business Partners*, or *Third Parties* who are not members but who have a relationship with *the Organization* in the course of their professional duties, with the *Whistleblowers* enjoying the protection established in this *Policy*, provided that they refer to the *breaches* referred to in paragraphs 1 and 2 of section 3 of this *Policy* ("**Material scope of application**") – that is, actions or omissions constituting infringements of European Union law or serious or very serious criminal or administrative offenses.

Likewise, through the *Internal Information System*, any *Member of the Organization, Business Partner*, or *Third* Party may report actions or omissions that may constitute a *Breach* of the *Organization's* internal regulations—which do not constitute a violation of European Union law or a serious or very serious criminal or administrative offense— including the principles and values that guide the conduct of all *members of the Organization,* as well as submit any queries related to the scope, compliance, and interpretation of the regulations applicable to *PERSÁN*.

4. PERSONAL SCOPE OF APPLICATION

This *Policy* applies not only to *PERSÁN Members*, but also to other collaborators such as volunteers, interns, trainees, regardless of whether or not they receive remuneration, candidates in the selection process, workers who have terminated their employment or commercial relationship, and workers' representatives, as well as any person working for or under the supervision and direction of contractors, subcontractors, and suppliers, and to partners, shareholders*,* and members of *the Board of Directors* and *Senior Management* of *PERSÁN* who make a *Communication* through the *PERSÁN Internal Information System* on any of the issues indicated in section 2 of this *Policy* (**"Material scope of application**").

The protection measures provided for in this *Policy* shall also apply, where appropriate: (i) to individuals who, within the framework of the *Organization* in which the *Whistleblower* provides services, assist the Whistleblower in the process; (ii) to individuals who are related to the *Whistleblower* and who may suffer *Retaliation,* such as *the Whistleblower's* co-workers or family members*;* and (iii) to legal entities for which the Whistleblower works or with which he or she has any other type of relationship in a work context or in which he or she holds a significant stake.

5. OBLIGATION TO REPORT NON-COMPLIANCE

Any *PERSÁN Member, Business Partner*, or *Third* Party who is not a member but who has a relationship with the *Organization* in the course of their professional duties (as set out in section 3 of this *Policy*) and who becomes aware of any *Non-Compliance* committed by any other *Member of the Organization* or *Business Partner* in a work or professional context, may immediately report it through any of the channels established for this purpose, without fear of suffering any type of *retaliation.* In this regard, all *Members of the* Organization, *Business Partners*, and *Third Parties* are encouraged to use the channels provided by the *Organization* for Reporting *Breaches.*

The *Internal Reporting System* is the preferred channel for reporting the actions or omissions referred to in section 2 of this *Policy*, provided that the *breach* can be effectively managed and the *Whistleblower* considers that there is no risk of *reprisals*.

6. ROLE OF THE PERSON RESPONSIBLE FOR THE INTERNAL REPORTING SYSTEM

The Organization's Board of Directors has appointed the *Chief Risk & Compliance Officer* as *the person responsible for the Internal Information System*, who has specific powers to manage the *Internal Information System* and process information files, and who offers adequate guarantees of independence, confidentiality, data protection, and secrecy of communications. This formal appointment has been recorded in the minutes.

In this regard, the *Head of the Internal Information System* will manage the *Ethics Channel* through *PERSÁN's Compliance Office*, within the *Risk & Compliance Department*, which is composed of:

- *Chief Risk & Compliance Officer*.
- *Compliance Manager*.
- *Compliance* Support Team.

7. INTERNAL REPORTING CHANNEL

PERSÁN has set up an *Internal Information System* comprising the following communication channels:

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 means of communication used, the *Whistleblower* may designate a preferred means of communication 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** (without providing personal data).

Commun*ications* should contain, as far as possible, the following information:

- Minimum content of a *Communication*:

  i. Date on which the *Communication* is submitted.

ii. Name and contact details of *the Informant* submitting the *Consultation*, unless they wish to remain anonymous. In order to facilitate a response to the *Consultation*, it is advisable to include the identity of *the Informant* in the *Consultation*, which will be actively protected so that it remains confidential.

iii. A clear and detailed explanation of the issue requiring clarification or response, as well as the reason for requesting such clarification, response, or criteria.

- Minimum content of a *Complaint*:

i. Date of the events reported.

ii. A clear and as detailed as possible explanation of the events.

iii. Identification of the perpetrator of the act, as well as other possible participants and persons who may have knowledge of the act in question.

iv. Name and contact details of *the Informant*, unless they wish to remain anonymous.

Under no circumstances will the personal details of *the Informant* be disclosed beyond the knowledge of the persons in charge of the investigation, who will, in any case, comply with the basic principles established in this *Policy*.

In the event that an external advisor is engaged to support the *Compliance Office* in the management of *the Internal Reporting System*, the external advisor will be required in all cases to provide adequate guarantees of respect for independence, confidentiality, data protection, and secrecy of communications.

v. The time at which the *Breach* was committed or, if it is ongoing, the time at which the *Complaint* is being made.

vi. Any other information and/or documentation that the *Informant* may provide to aid in understanding the incident in question. The person in charge of conducting the investigation may request additional information to be provided by the *Whistleblower*.

The *IRS Procedure* sets out the investigation process that will be followed after a regulatory *breach* has been reported, in line with the guidelines of the *Whistleblowing Directive* and the *Whistleblower Protection Law*.

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 this investigation, with the *Member of the Compliance Office* affected being recused from the management of said *Communication*.

The same will apply when *the Head of the Internal Information System* is unable to deal with a specific matter due to a conflict of interest. In such cases, he or she will voluntarily recuse themselves 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.

8. EXTERNAL REPORTING CHANNEL AND PUBLIC DISCLOSURE

Notwithstanding that the *Internal Information System* is the preferred channel for reporting actions and omissions that constitute a violation of European Union rights, or a serious or very serious criminal or administrative offense, any individual may directly contact:

- The external information channel created by the *Independent Whistleblower Protection Authority, A.I.I.*

    - Regarding matters related to the External Reporting Channel:

      canal.externo@proteccioninformante.es (any personal data relating to *third parties* must be omitted for reasons of confidentiality).

    - For matters related to the Internal Information Channel:

      canal.interno@proteccioninformante.es (you must omit any personal data of *third parties* for reasons of confidentiality).

- To the European Anti-Fraud Office: Reporting fraud - European Anti-Fraud Office - European Commission

- In matters of competition defense: Reporting prohibited conduct / CNMC.

- For tax offenses: Tax Agency: Reports.

Both Internal *Communications* and *Communications* made through external channels shall enjoy the protection granted in this *Policy*, provided that the requirements expressly set forth in section 9 below are met.

9. WHISTLEBLOWER PROTECTION

At *PERSÁN*, individuals who report or disclose violations in good faith **shall enjoy all the protection rights** provided for in this *Policy* and in the *IRS Procedure*, provided that:

1. They have substantial reasons to believe that the information they report to *PERSÁN* is truthful at the time of *Report*, and that the information falls within the material scope of *the Whistleblower Protection Law*—that is, actions or omissions that may constitute violations of European Union law and actions or omissions that may constitute serious or very serious criminal or administrative offenses.

2. They have made the *Communication* or disclosure in accordance with the requirements set forth for this purpose by *PERSÁN* and the *Whistleblower Protection Law*.

Individuals who have communicated or disclosed information about actions or omissions in good faith, as referred to in *the Whistleblower Protection Law*, anonymously, but who have subsequently been identified and meet the conditions set out in this section, shall be entitled to the protection provided for in the *Whistleblower Protection Law* and this *Policy*.

Persons who report in good faith to the relevant institutions, bodies, or agencies of the European Union on infringements falling within the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, shall be entitled to protection in accordance with the provisions of the *Whistleblower Protection Law* and this *Policy*.

Conversely, persons who communicate or disclose the following **shall not enjoy the protection** provided for in this *Policy* and the *GIR Protocol*:

1. Information contained in <u>*Communications* that have been rejected</u> for any of the following reasons:

    a. When, after preliminary analysis, the facts reported lack any credibility, duly justified.

    b. When the facts reported do not constitute a violation of the legal system included in the scope of application of the *Whistleblower Protection Law* or the scope of application of this *Policy*.

    c. When the *Communication* is manifestly unfounded or, in the opinion of *the Head of the Internal Information System*, there are reasonable grounds to believe that it has been obtained through the commission of a crime.

d. When the *Communication* does not contain new and significant information about violations that were the subject of a previous *Communication* for which the corresponding proceedings have been concluded, unless there are new factual or legal circumstances that justify a different follow-up. In these cases, the *Head of the Internal Reporting System* will notify the resolution, stating the reasons.

2. Information related to complaints about interpersonal conflicts or that only affect the *Whistleblower* and the persons referred to in the *Communication* or disclosure.

3. Information that is already fully available to the public or that constitutes mere rumors.

4. Information relating to actions or omissions not covered by the scope of this *Policy*.

The rejection of the *Communication* made through the appropriate channels will *be notified* to *the Whistleblower* within a reasonable period of time, within **fifteen (15) business days** of acknowledgment of receipt of the *Communication*, unless the *Communication* was anonymous or the whistleblower had waived the right to receive *notifications* regarding the procedure.

10. NON-RETALIATION POLICY

PERSÁN shall adopt the necessary measures to prohibit any act constituting *Retaliation* or harmful conduct, including threats of *Retaliation* and attempts at *Retaliation*, against persons who submit a *Communication* relating to actions or omissions within the scope of this *Policy*.

Retaliation is understood to mean any acts or omissions that are prohibited by law or that, directly or indirectly, involve unfavorable treatment that places the persons suffering them at a particular disadvantage in relation to others in the workplace or professional context, solely because of their status as *Whistleblowers* or because they have made a public disclosure.

For the purposes of this *Policy*, and by way of example only, the following are considered *Retaliation*:

1. Suspension of the employment contract, dismissal, or termination of the employment or statutory relationship, including non-renewal or early termination of a temporary employment contract once the probationary period has been completed.

2. Early termination or cancellation of contracts for goods or services.

3. Imposition of any disciplinary measure, demotion, or denial of promotion.

4. Failure to convert a temporary employment contract into a permanent one, in cases where the worker had legitimate expectations that they would be offered permanent employment.

5. Damages, including reputational damage, or economic losses, coercion, intimidation, harassment, or ostracism.

6. Negative evaluations or references regarding work or professional performance.

7. Inclusion on blacklists or dissemination of information in a specific sector, which hinders or prevents access to employment or the contracting of works or services.

8. Denial or cancellation of a license or permit.

9. Denial of training.

10. Discrimination, or unfavorable or unfair treatment.

The measures set forth in paragraphs 1 to 4 above shall not be considered *Retaliation* when carried out within the regular exercise of managerial authority under labor legislation or regulations governing the status of the public employee concerned, due to circumstances, facts, or proven violations unrelated to the submission of the *Communication*.

Likewise, it is hereby made known that any person whose rights have been violated as a result of their *Communication* or disclosure may, after a period of two years has elapsed, request the protection of the *Independent Whistleblower Protection Authority*, which, in exceptional and justified cases, may extend the period of protection, after hearing the persons or bodies that may be affected (the refusal of such an extension of the period of protection must be justified).

Likewise, it is hereby noted that any acts intended to prevent or hinder the submission of *Communications* and disclosures, as well as those that constitute *Retaliation* or cause discrimination after their submission under the *Whistleblower Protection Law*, shall be null and void and shall give rise, where appropriate, disciplinary or liability corrective measures, which may include the corresponding compensation for damages to the injured party.

In addition, *Whistleblowers* may have access, as appropriate, to the following support measures provided by the *Independent Whistleblower Protection Authority* and/or the competent regional body:

1. Comprehensive and independent information and advice, easily accessible to the public and free of charge, on the procedures and remedies available, protection against *Retaliation*, and the rights of the person concerned.

2. Effective assistance from the competent authorities before any relevant authority involved in their protection against *Retaliation*, including certification that they are eligible for protection under the *Whistleblower Protection Law*.

3. Legal assistance in criminal proceedings and cross-border civil proceedings in accordance with EU regulations.

4. Financial and psychological support, on an exceptional basis, if so decided by the *Independent Whistleblower Protection Authority* and/or the competent regional body, after assessing the circumstances arising from the submission of the *report*.

All of the above is in addition to any assistance to which the Whistleblower may be entitled under Law 1/1996 of January 10 on free legal aid for representation and defense in legal proceedings arising from the submission of the *Report* or public disclosure.

11. PROTECTIVE MEASURES AGAINST RETALIATION

PERSÁN will take the necessary measures to ensure that *Whistleblowers* are protected against *Retaliation*.

The main protection measures provided for in both the *Whistleblowing Directive* and the *Whistleblower Protection Law*, to which *PERSÁN* adheres and undertakes to facilitate their effective application, are set out below and made known to all potential *Whistleblowers*:

- Persons who report information on the actions or omissions referred to in paragraphs 1 and 2 of section 3 of this *Policy* or who make a public disclosure in accordance with the *Whistleblower Protection Law* shall not be considered to have breached any restriction on disclosure of information, and they shall not incur any liability whatsoever in connection with such *communication* or public disclosure, provided that they had reasonable grounds to believe that the *communication* or public disclosure of such information was necessary to disclose an action or omission under this *Policy* and the *Whistleblower Protection Law,* all without prejudice to the provisions of Article 2.3 of the *Whistleblower Protection Law*[1] . This measure shall not affect criminal liability.

  The provisions of the previous paragraph extend to the *communication* of information by workers' representatives, even if they are subject to legal obligations of secrecy or non-disclosure of confidential information. All of this is without prejudice to the specific protection rules applicable under labor regulations.

- Whistleblowers shall not be liable for the acquisition of or access to information that is publicly communicated or disclosed, provided that such acquisition or access does not constitute a criminal offense.

- Any other potential liability of whistleblowers arising from acts or omissions that are not related to the *Communication* or public disclosure or that are not necessary to disclose a violation under the *Whistleblower Protection Law* shall be enforceable in accordance with applicable regulations.

- In proceedings before a court or other authority concerning damages suffered by *Whistleblowers*, once the *Whistleblower* has reasonably demonstrated that they have reported or made a public disclosure in accordance with the *Whistleblower Protection Law* and that they have suffered damage, it shall be presumed that the damage occurred as *retaliation* for reporting or making a public disclosure. In such cases, the person who took the harmful measure

[1] Article 2.3 of the Whistleblower Protection Law: "*The protection provided for in this Act for workers who report violations of labor law in the field of occupational health and safety is understood to be without prejudice to that established in specific regulations*."

shall b d to prove that the measure was based on duly justified grounds unrelated to the *Communication* or public disclosure.

- In legal proceedings, including those relating to defamation, copyright infringement, breach of confidentiality, violation of data protection rules, disclosure of trade secrets, or claims for compensation based on labor or statutory law, persons who make a *Communication* in accordance with this *Policy* and the *Whistleblower Protection Law* shall not incur any liability as a result of communications or public disclosures protected by that Act. Such persons shall be entitled to plead in their defense and in the context of such legal proceedings that they made a communication or public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure was necessary to bring to light a violation under the *Whistleblower Protection Law.*

12. PROTECTIVE MEASURES FOR THE INDIVIDUALS REPORTED

PERSÁN shall ensure that the *Reported Party* or the persons referred to in the *Communication* are heard in the internal investigation, have the right to the presumption of innocence, the right to defense, and the right of access to the file under the terms regulated in the *Whistleblower Protection Law*.

In addition, the identity of *the Reported Party* or the persons referred to in *the Report* shall be protected and treated confidentially, as will the facts referred to *in the Report*, in the same way as the identity of *the Whistleblower*, subject to any limits and exceptions that may be necessary to guarantee the successful completion of the investigation or the eventual disclosure to the competent authorities.

13. 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 Agreement, or in the applicable labor legislation, and shall be graded according to the seriousness of the acts committed, taking into consideration circumstances such as the damage or harm caused, the circumstances of the victims, if any, among others.

Likewise, possible sanctions may also be imposed on *business Partners* who commit any type of *Breach* under the terms established in this *Policy*, which include, among others, the termination of business relations.

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

14. CONFIDENTIALITY

Without prejudice to the provisions of other sections of this *Policy*, *PERSÁN* guarantees the confidentiality of the identity of *the Whistleblower* and any person mentioned in the *Communication*, and of the actions taken in the management and processing thereof, as well as data protection, preventing access by unauthorized personnel.

By virtue of the foregoing, access to data relating to the *Communication* is limited to members specifically authorized by *PERSÁN* to receive, follow up on, or resolve *Communications* received, as well as those *Third Parties* (e.g., a judicial authority, the Public Prosecutor's Office, or the competent administrative authority) when it constitutes a necessary and proportionate obligation imposed by applicable regulations, in the context of an investigation carried out by national authorities or in the context of legal proceedings, and, in particular, when the disclosure is intended to safeguard the right of defense of the person concerned.

In any case, except in the cases provided for, *PERSÁN* guarantees that no unauthorized person will know the identity of *the Whistleblower* or any other information that could help to directly or indirectly deduce their identity. Specifically, *PERSÁN* guarantees that the *Reported Party* will in no case be informed of the identity of *the Whistleblower* or, where applicable, of the person who made the public disclosure.

In addition, *PERSÁN* guarantees the confidentiality of the data and facts provided when the *Communication* is sent through channels other than those established or to members of staff not responsible for its processing. To this end, *PERSÁN* has adequately trained its staff in this matter and has warned them about breaches of the duty of confidentiality and, likewise, has established the obligation of the recipient of the *Communication* to immediately forward it to *the Head of the Internal Information System.*

In compliance with the foregoing, *PERSÁN* has implemented technical and organizational measures in the *Internal Information System* to preserve the identity and guarantee the confidentiality of the data corresponding to the persons concerned and to any person mentioned in the information provided, especially the identity of *the Whistleblower,* if identified.

In relation to the persons affected by the *Communication*, *PERSÁN* guarantees that during the processing of the file, the persons affected by the *Communication* will have the same protection established for *Whistleblowers*, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure.

For their part, those who receive public disclosures have the same obligations as described above and, under no circumstances, will they obtain data that allows the identification of *the Whistleblower* and must have adequate technical and organizational measures in place.

Disclosures made under this section shall be subject to the safeguards established in the applicable regulations and, in particular, *the Whistleblower* shall be informed before their identity is disclosed, unless such information could compromise the investigation or legal proceedings. When the competent authority informs the *Whistleblower*, it shall send them a letter explaining the reasons for the disclosure of the confidential data in question.

In any case, *PERSÁN* shall endeavor to ensure that the competent authorities receiving information on infringements that includes trade secrets do not use or disclose them for purposes beyond what is necessary for the proper follow-up of the proceedings.

15. DATA PROTECTION

Personal data processed in accordance with this *Policy* and the *IRS Procedure*, including the exchange or transmission of personal data with the competent authorities, will be processed by *PERSÁN,* with Tax ID Number A.91.380.014 and registered address at Calle Pino Albar, 2, Postal Code 41016, Seville, and email address gdpr@persan.es , as the data controller in accordance with the provisions of the regulations on personal data protection.

Personal data provided through the *Internal Information System* will be processed for the purpose of receiving and analyzing the reported actions or omissions and, where appropriate, deciding whether to admit the case for processing and initiate an investigation into the reported events. In addition, certain information may be processed to leave evidence of the functioning of *the Internal Information System*. In the latter case, *PERSÁN* guarantees that the information stored as evidence will be anonymized.

If information is received that is not necessary for the processing and investigation of the actions or omissions referred to in section 3 of the *Policy*, the data controller will proceed to delete it immediately.

Likewise, all personal data that may have been communicated and that refer to conduct not included in the scope of application of the *Whistleblower Protection Law* and this *Policy* will be deleted, as well as any information or part thereof that is proven to be untrue, unless such lack of truthfulness may constitute a criminal offense.

The data controller will process the personal data provided by the *Whistleblower* in compliance with a legal obligation, specifically in compliance with the *Whistleblower Protection Law*. In addition, in the case of verbal *Communications*, the *Whistleblower's* consent will be required to document such *Communication*, including those made through face-to-face meetings, telephone calls, or voice messaging. For its part, the processing of specially protected data may be carried out by the controller for reasons of substantial public interest in accordance with the provisions of Article 9.2.g) of Regulation (EU) 2016/679.

In the case of the processing of personal data derived from a public disclosure, the legal basis that legitimizes it is that it is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the data controller (Article 11 of Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation, and prosecution of criminal offenses and the execution of criminal penalties).

Personal data collected through the *Internal Information System* will be stored in accordance with the provisions of applicable legislation. Specifically, in accordance with 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 the

Guarantee of Digital Rights, three (3) months after receipt of the *Communication*, if no investigation has been initiated, the data will be deleted, unless the purpose of its 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.

In order to fulfill the purposes described above, the data controller may provide access to personal data to:

- Third-party companies that provide services, such as external advisors and collaborators who provide support in the management or, where appropriate, investigation of *Communications* received through the *Internal Information System*.

- Those areas or departments relevant to the processing of the *Communication* and, where appropriate, to the investigation and possible measures to be taken with regard to the conduct reported, provided that this is necessary.

- Similarly, personal data may be transferred to judges and courts, the Public Prosecutor's Office, and the competent public administrations as a result of any investigation that may be launched.

In relation to the above, *PERSÁN* informs interested parties at that it does not carry out international transfers of the personal data provided.

However, *PERSÁN* informs that, in the event that the *Respondent* referred to in the *Communication* or in the public disclosure exercises the right to object, it will be presumed that, unless proven otherwise, there are compelling legitimate grounds that justify the processing of their personal data.

Without prejudice to the rights of the informant, in accordance with data protection regulations, if the *Communication* has been made verbally, *PERSÁN* offers the opportunity to request access to your personal data, rectification, deletion or cancellation, limitation of processing, opposition or portability by sending a written request to PERSÁN, S.A., at Calle Pino Albar, nº 2 – Postal Code 41016 Seville, or by sending an email to gdpr@persan.es. We may ask you for a copy of your ID card if necessary to verify your identity.

Furthermore, the data subject is informed that, under the conditions established in the applicable regulations, they may exercise the rights recognized in the data protection regulations by sending a *communication* through the *Internal Information System*.

Likewise, interested parties have the right to file a complaint with the Spanish Data Protection Agency, either through its website (at www.aepd.es) or at its address at Calle Jorge Juan, nº 6, Postal Code 28001, Madrid.

The *Internal Information System Manager* will periodically review the proper functioning of *the Internal Information System* and the provisions of this *Policy*.

16. KEY PRINCIPLES OF THE IRS PROCEDURE

The *IRS Procedure* is governed by the following principles, which shall be observed during the processing of any case:

- **Confidentiality:** the *IRS Procedure* shall guarantee the confidentiality of the identity of *the Whistleblower*, of any person mentioned in the *Communication*, and of the data relating to the reported incident, except in the case of *Communication* to the judicial authority, the Public Prosecutor's Office, or the competent administrative authority in the context of a criminal, disciplinary, or sanctioning investigation.

- **Impartiality:** the *Head of the Internal Reporting System* must be guided in all cases by the principle of impartiality, treating all *Reports* equally, regardless of the persons involved, and avoiding any type of conflict of interest.

- **Objectivity**: Not only will the facts and circumstances that establish and aggravate the responsibility of *the Reported Party* be investigated, but also those that exempt them from it or extinguish or mitigate it.

- **Independence of the Head of the Internal Information System:** the *Head of the Internal Information System* shall enjoy full independence and autonomy to agree on the steps they deem necessary to clarify the reported facts, always pursuing the search for the truth.

- **Documentation:** each *Communication* shall give rise to a file, in which the *Head of the Internal Information System* shall include detailed documentation of the entire investigation procedure.

- **Good faith:** the provisions of the *IRS Procedure* and this *Policy* shall be interpreted in accordance with the principles and requirements of good faith.

- **Proportionality**: this principle responds to the need for the sanction to be commensurate with the seriousness of the facts, avoiding it being a disproportionate measure.

- **Principle of "due process":** everyone has the right to be heard and to assert their legitimate claims before those in charge of the investigation.

17. RECORD OF REPORTS

PERSÁN will keep a record of all communications and inquiries it may receive through the *Internal Information System*, compiled in the so-called "***record book***," 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.

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

- By recording the conversation in a durable and accessible format, with the prior consent of *the Whistleblower*.
- Through a complete and accurate transcript of the conversation made by the *Internal Reporting System Manager*.

In any case, the *Whistleblower* has the right to check, rectify, and accept the transcript by signing it. If the *Whistleblower* refuses to sign the transcript, the *Head of the Internal Information System* may call on a witness.

When the *Whistleblower* has requested a personal interview with the *Head of the Internal Information System* to make the *Communication*, *PERSÁN* will ensure, subject to the *Whistleblower's* consent, that complete and accurate records of the meeting are kept in a durable and accessible form.