PROCEDURE FOR THE MANAGEMENT, INVESTIGATION, AND RESPONSE TO COMMUNICATIONS RECEIVED THROUGH THE INTERNAL INFORMATION SYSTEM (GIR PROCEDURE)



Date of Approval and Record of Changes to the Document

Version	Date	Description
1.0.	June 20, 2023	Approval by the Board of Directors: Update to the Internal Information Channel (Law 2/2023 (Whistleblower Protection Law)).
2.0.	August 8, 2024	Approval by the Board of Directors: Update to Phase 1 of the certification process for the Criminal *Compliance* Management System in accordance with UNE 19601:2017.
3.0.	September 25, 2025	Approval by the Board of Directors: update to *the Criminal Compliance Management System* (organizational changes).
4.0	September 2, 2026	Approval by the *Board of Directors*: International rollout of the Internal Information System.

TABLE OF CONTENTS

1. DEFINITIONS ..... ¡ERROR! MARCADOR NO DEFINIDO.
2. OBJECTIVE 9
3. SCOPE OF APPLICATION 10
4. COMMUNICATION CHANNELS AND CONTENT OF COMMUNICATIONS 11
4.1 Means of *Communication* 11
4.2 Minimum Content of *Communications* 11
4.3 External Channels for Information and Communication with the Competent Authorities 12
5. SUITABILITY, INDEPENDENCE, AND CONFLICTS OF INTEREST 14
6. CONFIDENTIALITY 15
7. PROTECTIVE MEASURES FOR INDIVIDUALS AFFECTED BY THE REPORT 17
8. PROHIBITION OF RETALIATION AND PROTECTION OF THE WHISTLEBLOWER 18
9. RECEIPT OF REPORTS AND COMPILATION OF THE CASE FILE 20
9.1 Acknowledgment of Receipt 20
9.2 Request for Additional Information 20
9.3 Compilation of the initial case file 20
9.4 Handling of Reports Related to Harassment 20
9.4.1 Receipt and Forwarding of Reports of Harassment 21
9.4.2 Safeguards Regarding Reports of Harassment 21
9.4.3 Traceability and Data Protection in Reports of Harassment 21
10. ANALYSIS AND PRELIMINARY DECISION ON THE REPORT RECEIVED 23
10.1 Preliminary Analysis of the Report Received 23
10.2 Preliminary Decision on the Information Received 23
10.3 Precautionary Measures 24
11. INTERNAL INVESTIGATION PROCEDURE 25
11.1 Selection of the investigation strategy 25
11.2 Planning the investigation 25
11.3 Notification to the individuals concerned 26
11.4 Conducting the investigation 27
11.5 Documentation of the research procedure 28
11.6 Final Report 28
11.7 Final Actions 29
12. CONCLUSION OF THE PROCEDURE 30
12.1 Responsible body 30
12.2 Hearing proceedings 30

12.3 Decisions of the Head of the Internal Information System 30
12.4 Sanctions 30
12.5 Other measures 31
12.6 Notification of Decisions 31
13. RETENTION OF DOCUMENTATION 32
13.1 Retention Periods 32
13.2 Communications Log 32
14. PERSONAL DATA PROTECTION 34
14.1 General Principles 34
14.2 Data Controllers 34
14.3 Categories of Data Processed 34
14.4 Purposes of Processing and Legal Bases 34
14.5 Confidentiality 35
14.6 Data Retention 35
14.7 Recipients of the data 36
14.8 International data transfers 36
14.9 Rights of Data Subjects 37
15. DISTRIBUTION, REVIEW, AND UPDATE OF THE PROCEDURE 38

1. DEFINITIONS

The following are the definitions of the terms that will be frequently used in this document (listed in *italics*):

- ***Persán Group / the Organization***: This refers to the group of all companies in which *PERSÁN*, S.A. holds, directly or indirectly, more than 50% of the share capital.

- ***PERSÁN / the Company***: includes the parent company of *the Persán Group*, Persán, S.A.

- ***Regulatory Compliance Office / Compliance Office***: an internal collegiate body of *the Persán Group*, endowed with sufficient authority and autonomous powers of initiative and control, responsible for supervising the proper functioning and observance of *the Organization's Criminal Compliance Management System*, both domestically and internationally.

  The Compliance Office ensures the proper identification, prevention, and management of *compliance risks*, with special attention to *criminal risks*, ensuring that the *System* complies with the provisions of applicable local regulations in the countries where the *Persán Group* operates and with international best practices, including ISO 37301:2021.

- ***Board of Directors***: the body with fundamental responsibility and authority over *Grupo Persán's* activities, governance, and policies, to which *senior management* reports and is accountable.

- ***Senior Management / Management Committee***: the high-level body within *Grupo Persán* that reports directly to *the Board of Directors*. It currently consists of the *Grupo Persán Management Committee*.

- ***Members of the Organization***: members of the *Board of Directors*, members of *Senior Management*, permanent, temporary, or contract employees, volunteers of the *Organization*, and all other individuals reporting hierarchically to any of the foregoing.

- ***Business Partners***: any legal entity or individual, other than *Members of the Organization*, with whom the *Organization* maintains or intends to establish some type of business relationship. By way of example, but not limited to, this includes suppliers, customers, and, in general, individuals and legal entities that contract with *Grupo Persán* for the delivery of goods or the provision of services.

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

- ***Ethics Channel / Internal Information System***: a set of measures adopted by the *Organization* in accordance with 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; the Whistleblower Protection Regulations applicable in each country that transposes said Directive, including, in the case of Spain, Law 2/2023 (Whistleblower Protection Law) of February 20, regulating the protection of persons who report regulatory violations and combating corruption; and the principles of ISO 37002:2021, on Whistleblowing Management Systems, for the management of *communications* regarding violations of the regulations referred to in this text.

- ***Head of the Internal Information System***: The *Chief Risk & Compliance Officer* has been designated as the person responsible for the prompt processing of *reports* received through the *Ethics Channel* and must perform their duties with full autonomy and independence from the other bodies of *the Persán Group*. The *Head of the Internal Information System* has the authority, delegated by *the Grupo Persán Board of Directors* itself, to appoint *Local Representatives* to assist him or her in managing *reports* received through the *Internal Information System*.

- ***Local Delegate:*** an internal body, either consisting of a single individual or a committee, formally designated by the *Compliance Office*, which is generally entrusted with the responsibility of monitoring the operation and compliance with *Grupo Persán's Criminal Compliance Management System*, solely within its geographic scope of operation. When the *Chief Risk & Compliance Officer*, in his capacity as *Head of the Internal Information System (RSII)*, additionally designates this same person to support the operational management of the Internal Information System within that jurisdiction, such specific designation and its functions shall be governed by the provisions of the *Internal Information System Policy* and the *GIR Procedure*; neither should these two designations be confused, nor do they necessarily imply the same scope of authority or the same appointing body.

  In this regard, a distinction is made between the *Criminal Compliance Management System Local Delegate*, whose duties are strictly related to the *Criminal Compliance Management System*, and the *Internal Information System Local Delegate*, whose duties are strictly related to the *Internal Information System*.

  Local Delegates must have express written authorization from the body that appoints them in each case, sign the corresponding confidentiality agreement, meet the appropriate criteria for professional competence and functional independence with respect to the *Organization's* operational and business areas, and comply with any other requirements set forth in applicable local regulations. Such designation shall not imply a transfer of responsibility for the *System*, which shall in all cases remain with the *Compliance Office*.

- ***Communication:*** a statement by which any *Member of the Organization*, *Business Partner*, or *Third Party* raises an issue regarding the scope, interpretation, or compliance with external regulations applicable to the *Organization*, as well as the *Organization's* internal corporate regulations. Depending on its content, a *Communication* may constitute a *Consultation* or a *Complaint*.

- ***Consultation:*** *A communication* through which any *Member of the Organization*, *Business Partner*, or *Third Party* requests clarification, a response, or guidance regarding the scope, interpretation, or compliance with regulations applicable to *the Persán Group* and/or corporate regulations.

- ***Complaint:*** *A communication* regarding a possible *violation* of external regulations applicable to the *Organization*, as well as the *Organization's* internal corporate regulations.

- ***Whistleblower***: A natural or legal person who files a *Consultation* or *Report*. The term *"Whistleblower"* includes *Members of the Organization, Business Partners, Third Parties*, and any person who currently falls under or may in the future fall under the aforementioned categories.

- ***Reported party***: a natural or legal person accused of an alleged violation that is under investigation by the *Head of the Internal Information System*.

- ***Breach***: Improper conduct or potential acts that are unlawful or contrary to the law or internal corporate regulations (including, in particular, any conduct that could constitute a crime, a serious or very serious administrative offense, or a violation of European Union law).

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

- ***Criminal risk:*** Risk related to the commission of acts that could constitute a crime, in accordance with the criminal or quasi-criminal liability regime for legal entities established in the local legislation applicable to each jurisdiction where the *Persán Group* operates.

- ***Good-faith report***: A report made in accordance with the provisions of the *Internal Information System Policy* and based on facts or evidence from which the existence of a *violation* of applicable law or internal regulations can reasonably be inferred. A *report* is considered to be made in good faith when it is submitted without the intent to seek revenge or to cause employment-related or professional harm to the *Reported party* or a *Third Party*.

- ***Report Log***: A tool used by the *Head of the Internal Information System* to ensure the traceability and security of *reports* received through the *Ethics Channel*.

- ***Retaliation / Harmful Conduct***: an act or omission prohibited by law, or one that, directly or indirectly, constitutes unfavorable treatment that places the *Whistleblower* or the affected parties at a particular disadvantage compared to others in the workplace or professional context, solely because of their status in relation to the *Report*, or for having made a public disclosure.

- ***Internal Information System Policy***: a corporate document that establishes the principles governing the *Organization's Internal Information System*, as well as the rights and obligations of its users (hereinafter also referred to as the "Policy").

- ***Procedure for the Management, Investigation, and Response to Communications received through the Internal Information System (GIR Procedure)***: a corporate document, consisting of the document itself and its Annexes for local adaptation, which establishes the necessary mechanisms for the early reporting and management of any *breach*, as well as the procedures required for the internal processing of *consultations*, and the internal processing and investigation of those *Complaints* or any known circumstances that must be investigated.

  The local annexes form an integral part of *the GIR Procedure* and detail the specific requirements and particularities mandated by the applicable regulations in each jurisdiction where *the Persán Group* operates (hereinafter, the document and its annexes as a whole will also be referred to as ***the "GIR*** Procedure").

- ***Criminal Compliance Management System (SGCP***): an organizational and management system for the prevention of breach, whose objective is the prevention, detection, and management of risks through their integration into business processes, as well as

measurement for continuous improvement, and whose essential foundation is represented by the Criminal *Compliance* Policy and the *Regulatory Compliance Program*.

- ***Whistleblower Protection Regulations***: a set of legal provisions applicable in each jurisdiction designed to regulate the reporting of violations, the protection of whistleblowers, and the management of internal reporting systems.

- ***Conflict of Interest***: A situation in which there is a personal (financial, relational, professional, or any other type of) or organizational interest, whether direct or indirect, that may compromise or appear to compromise a person's ability to act impartially in the performance of their professional duties and in the defense of *the Organization's* best interests.

2. OBJECTIVE

Grupo Persán, within the framework of its *Criminal Compliance Management System* and in accordance with international *best practices*—such as ISO 37002:2021, and specifically the *Whistleblowing Directive* and the *Whistleblower Protection Policy*—has implemented an *Internal Information System* through which any *Member of the Organization, Business Partner*, or *third* party who is aware of or suspects a regulatory *violation* (whether of legislation or its implementing regulations, or of internal corporate policies) committed by a *member of Grupo Persán* or by *Third Parties* who are in contact with the Group in the course of their work or professional activities, may report it to the *Organization*, either anonymously or by providing their identity.

The *Internal Information System* may also be used to submit to *Grupo Persán* any *consultation* regarding the scope, compliance with, and interpretation of external regulations applicable to the *Organization*, as well as the *Organization's* internal corporate regulations.

To this end, *Grupo Persán* has adopted a *Internal Information System Policy* that sets forth the general principles governing the *Internal Information System* and the protection of *whistleblowers*.

In addition, this *GIR Procedure* establishes the operational framework applicable to the management of *communications* received through the *Internal Information System*, defining the actions, responsibilities, deadlines, safeguards, and monitoring mechanisms that must be observed during the receipt, analysis, investigation, and resolution of *consultations* and *complaints*.

Furthermore, the *GIR Procedure* incorporates the local Annexes corresponding to the regulatory requirements regarding the Internal Information System in each jurisdiction where *the Persán Group* operates; these Annexes form an integral part of the Procedure and are intended to adapt the corporate provisions contained herein to the specific characteristics, requirements, and obligations established by the *Whistleblower Protection Regulations*.

Consequently, this *GIR Procedure* establishes the common corporate criteria that must be applied throughout the *Persán Group*, ensuring uniform, coordinated, traceable, and legally compliant management of *Communications*, without prejudice to the local specificities set forth in the corresponding local Annexes.

All of this is intended to ensure the proper detection, reporting, investigation, and response to potential *violations*, while guaranteeing confidentiality, independence, the protection of *the whistleblower*, the rights of the individuals involved, and compliance with the applicable regulations in each jurisdiction.

3. SCOPE OF APPLICATION

This *Procedure* applies to all *reports* received through the *Internal Information System* via any of the communication channels established under the *Ethics Channel*.

Likewise, this *Procedure* applies to all *Members of the Organization*, who must comply with its provisions regardless of their position or role, or the jurisdiction in which they are located; it also applies to any person who wishes to report a potential *violation* that may have occurred in a professional context.

In this regard, the *Procedure* applies to *Business Partners* and *Third Parties* who become aware that a *violation* has occurred in their relationship with *the Persán Group*.

Reports received may concern any *violation* of the law or of *Grupo Persán's* internal regulations. However, in accordance with the provisions of the *Policy*, *reports* related to strictly labor-related matters, those related to professional performance, or those whose scope of application specifically falls under another area or body of the *Organization* are excluded from the scope of this *Procedure*.

This *Procedure* shall apply without prejudice to the local provisions contained in the applicable local Annexes, as required by the applicable law in the jurisdictions where the *Persán Group* operates. In the event of a conflict between the provisions of the local Annexes and those of local regulations, with respect to the provisions of this *GIR Procedure*, the provisions of the relevant local Annex or local specification shall prevail.

The application of this *GIR Procedure* shall in no case result in a breach of applicable legal provisions or of the specific provisions set forth in the local annexes of the countries where the Persán Group operates. Such local provisions shall, in all cases, take precedence over *the GIR Procedure*. In the absence of applicable legal provisions in the relevant market, or as a supplement to existing ones, the provisions of this *Procedure* shall apply, without prejudice to the provisions of the *Policy* and any other applicable internal regulations of *the Persán Group*.

4. COMMUNICATION CHANNELS AND CONTENT OF COMMUNICATIONS

4.1 Means of Making a *Report*

The Persán Group has established an *Internal Information System* comprising the following communication channels:

1. **Written *reports***, via the technological platform provided by *the Persán Group* at https://persán.integrityline.com/.

2. **Verbal *reports*,** by requesting that *the Head of the Internal Information System* schedule an in-person meeting to present the *report*. In such cases, the meeting must be held within a maximum of seven (7) calendar days from the date of the request.

3. **Through a line manager,** who is required to forward this *report* to *the Head of the Internal Information System* within a period not exceeding two (2) business days from receipt of the information, or, where applicable, to submit the received *report* via the platform indicated in point 1 above.

In the case of verbal *reports*, with *the Whistleblower's* prior consent, the conversation between the Whistleblower and the *Head of the Internal Information System* may be recorded—provided the Whistleblower is informed 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 – (on a secure, durable, and accessible medium) or will be accurately transcribed by the *Head of the Internal Information System*, and the *Whistleblower* has the right to review, correct, and accept the transcription by signing it.

Regardless of the means of communication used, the *Whistleblower* may designate a preferred method of communication to receive *notifications* regarding the status of their *Report* or to be contacted for the purpose of requesting additional information and/or clarification.

Notwithstanding the foregoing, any formal *communication* from a judicial body or a public administration shall be considered a valid means of becoming aware of a *violation*.

The *Internal Information System* **is also open to *Business Partners* and *Third Parties*** outside the *Persán Group*.

Reports may be submitted either by **name** or **anonymously**.

4.2 Minimum Content of *Communications*

Communications must include, to the extent possible, the following elements:

- **Minimum Content of a *Consultation*:**

  i. Date the *consultation* was submitted.

  ii. Name and contact information of *the Whistleblower* submitting the *Consultation*, unless *the Whistleblower* wishes to remain anonymous. To facilitate a response to the *Consultation*, it is recommended that the *Whistleblower's* identity be included in the *Consultation*; this information will be actively protected and kept confidential.

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

- **Minimum content of a *complaint*:**

i. Date of the events being reported.

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

iii. Identification of the perpetrator of the incident, as well as any other possible participants and individuals who may have knowledge of the incident in question.

iv. Name and contact information of *the whistleblower*, unless the report is submitted anonymously.

Under no circumstances will personal information identifying the *whistleblower* be disclosed beyond the knowledge of the individuals in charge of the investigation, who, in any case, will comply with the basic principles established in the *Internal Information System Policy*.

If an external advisor is engaged to assist the *Compliance Office* in managing the *Internal Information System*, that advisor must, in all cases, provide adequate guarantees regarding respect for independence, confidentiality, data protection, and the secrecy of *communications*.

v. The time at which the *violation* occurred or whether it is still occurring at the time the *report* is being filed.

vi. Any other information and/or documentation that the *Whistleblower* may provide to aid in understanding the matter in question. The person in charge of conducting the investigation may request additional information, which must be submitted by the *Whistleblower*.

The *GIR Procedure* and its local annexes outline the investigation process to be followed upon receipt of a *report* of a regulatory *violation*, in accordance with international *best practices*, the *Whistleblowing Directive*, and the *Whistleblower Protection Policy*.

4.3 External Channels for Reporting and Communication with the Competent Authorities

Notwithstanding the fact that the *Internal Information System* is the preferred channel for reporting actions and omissions that constitute violations of European Union law, or a criminal, quasi-criminal, or serious or very serious administrative offense, any person may also make use of the external channels established by the competent authorities, in accordance with the applicable regulations in each case, including, where appropriate, before the institutions, bodies, or agencies of the European Union, to report actions or omissions that may fall within the material scope of the *Whistleblowing Directive* and, where applicable, the respective local regulations that may apply.

Specifically, in the case of Spanish jurisdiction, they may use the following channels:

- External reporting channel established by the *Independent Authority for the Protection of Whistleblowers (A.I.I.).*

    - Regarding matters related to the external reporting channel:

      canal.externo@proteccioninformante.es (You must omit any personal information of *Third Parties* for confidentiality reasons).

    - For matters related to the internal reporting channel:

      canal.interno@proteccioninformante.es (You must omit any personal information about *Third Parties* for confidentiality reasons).

- Regarding antitrust matters: Report of prohibited conduct / CNMC.

- Regarding tax violations: Tax Agency: Reports.

Both internal *communications* and *communications* made through external channels shall be protected as provided in this *Procedure* and its local annexes.

5. SUITABILITY, INDEPENDENCE, AND CONFLICT OF INTEREST

The *Head of the Internal Information System*, the members of the *Compliance Office*, and the *Local Representatives* must, in the performance of their duties related to the *System*, possess professional competence and functional independence from the operational and business areas that may be the subject of a *Report*. Additionally, the *Head of the Internal Information System* shall perform his or her duties with full autonomy from the *Organization's* other bodies, without receiving instructions of any kind in the performance of those duties, and the *Organization* shall ensure that he or she has the necessary personnel and material resources to do so.

The *Head of the Internal Information System* shall verify compliance with these conditions by the members of the *Compliance Office* and by the *Local Representatives* at the time of their appointment and on an annual basis; the *Board of Directors* shall conduct the same verification with respect to the *Head of the Internal Information System*.

In the event of ***a conflict of interest***—that is, if the Reported party is the *Head of the Internal Information System*, a *member of the Compliance Office*, or, as the case may be, a *Local Representative* involved in handling said *report*—the affected person must recuse themselves from participating in the processing and investigation of the case. In such a case, the *Head of the Internal Information System* shall designate another *Member of the Compliance Office* or *Local Representative* who is not involved to take over the handling of said *report*.

The same shall apply when *the Head of the Internal Information System* is in a conflict of interest regarding a specific matter; he or she shall voluntarily recuse himself or herself, either from the outset or from the moment his or her involvement becomes known, should this come to light during the investigation. In this regard, the *Board of Directors* shall decide on the replacement to carry out the procedure.

Furthermore, as a general rule, any person involved in the receipt, analysis, investigation, or resolution of a *Report*—including the *Head of the Internal Information System*, members of the *Compliance Office,* and *Local Representatives*—must recuse themselves if any of the following circumstances apply with respect to any of the parties involved: (i) direct hierarchical subordination or relevant functional or organizational dependence, even if there is no direct hierarchical subordination; (ii) kinship by blood or marriage up to the second degree; (iii) close friendship or open enmity; or (iv) a personal interest, direct or indirect, in the outcome of the investigation. The affected person shall report the grounds for recusal to the immediately superior body in the *System's* structure (the *Head of the Internal Information System*, or the *Board of Directors* if the grounds involve the *Head of the Internal Information System* himself or herself), who shall reassign the matter.

When the person affected by the *complaint* is a member of *the Board of Directors*, the *Compliance Office* shall conduct the relevant investigation and report its findings to another unaffected board member.

6. CONFIDENTIALITY

Without prejudice to the provisions set forth in other sections of this *Procedure* and in the local Annexes, *the Persán Group* guarantees the confidentiality of the *Whistleblower's* identity and that of any person mentioned in the *Report*, as well as the confidentiality of the actions taken in the handling and processing of the Report, and ensures data protection by preventing access by unauthorized personnel.

Accordingly, access to data related to the *Report* is limited to members specifically authorized by *the Head of the Internal Information System* to receive, monitor, or resolve the *Reports* received, as well as to *Third Parties* (for example, a judicial authority, the Public Prosecutor's Office, or the competent administrative authority) when such disclosure constitutes a necessary and proportionate obligation imposed by applicable regulations, in the context of an investigation conducted by national authorities or within the framework of judicial proceedings, and, in particular, when disclosure is intended to safeguard the right of defense of the affected individual.

In any case, except as provided for, *Grupo Persán* guarantees that no unauthorized person will learn the identity of *the Whistleblower* or any other information that could help directly or indirectly deduce their identity. Specifically, *Grupo Persán* guarantees that the *Reported party* will under no circumstances be informed of the *Whistleblower's* identity or, where applicable, of the identity of the person who made the public disclosure.

Furthermore, *Grupo Persán* guarantees the confidentiality of the data and facts provided when the *Report* is submitted through channels other than those established or to staff members not responsible for processing it. To this end, *Grupo Persán* has adequately trained its staff on this matter and has warned them of the consequences of breaching the duty of confidentiality; furthermore, it has established the obligation for the recipient of the *report* to immediately forward it to *the Head of the Internal Information System*.

In compliance with the foregoing, *Grupo Persán* has implemented technical and organizational measures within the *Internal Information System* to protect the identity and ensure the confidentiality of data pertaining to the individuals concerned and any person mentioned in the information provided, particularly the identity of *the Whistleblower,* should they have been identified.

With regard to the individuals affected by the *report*, *Grupo Persán* guarantees that, during the processing of the case, those affected by the *report* will be entitled to the same protection afforded to *whistleblowers*, ensuring the preservation of their identity and the confidentiality of the facts and information related to the proceedings.

For their part, those who receive public disclosures are subject to the same obligations described above and, under no circumstances, shall obtain information that would allow for the identification of *the Whistleblower*; they must also have adequate technical and organizational measures in place.

Disclosures made pursuant to this section shall be subject to the safeguards established in applicable local regulations; in particular, the *Whistleblower* shall be informed prior to the disclosure of their identity, unless such information could compromise the investigation or legal proceedings. When the competent authority notifies the *Whistleblower*, it shall provide a written explanation of the reasons for disclosing the confidential information in question.

In any case, *Grupo Persán* will ensure that the competent authorities receiving information regarding violations that include trade secrets do not use or disclose such information for purposes beyond what is necessary for the proper conduct of the proceedings.

7. PROTECTIVE MEASURES FOR INDIVIDUALS AFFECTED BY THE COMMUNICATION

Grupo Persán will ensure that the individuals *against whom a complaint has been filed* are heard as part of the internal corporate investigation, enjoy the right to the presumption of innocence, the right to a defense, and the right to access the case file in accordance with the terms set forth in the *Whistleblower Protection Policy,* as well as all other principles and rights that protect them as established in the *GIR Procedure*.

Likewise, the identity of the person who is the subject of the *report* will be protected and treated confidentially, as will the facts described in *the report* and the identity of the *whistleblower*, in accordance with the provisions of the "Confidentiality" section of this *Procedure*.

8. PROHIBITION OF RETALIATION AND PROTECTION OF THE WHISTLEBLOWER

Grupo Persán will take the necessary measures to ensure that *whistleblowers* are protected against *retaliation*.

The following sets forth and informs all potential *Whistleblowers* of the main protective measures provided for in both the *Whistleblowing Directive* and the *Whistleblower Protection Regulations*, to which *Grupo Persán* adheres and is committed to ensuring their effective implementation:

- Persons who report information regarding the acts or omissions listed in the *"Material Scope of* Application" section of the *Internal Information System Policy* or who make a public disclosure in accordance with the *Whistleblower Protection Regulations* shall not be deemed to have violated any restriction on the disclosure of information, and such persons shall not incur any liability whatsoever in connection with such *communication* or public disclosure, provided they had reasonable grounds to believe that the *communication* or public disclosure of such information was necessary to reveal an act or omission under this *Procedure,* its local annexes, and the *Whistleblower Protection Regulations*. This measure shall not affect criminal or quasi-criminal liabilities.

  The provisions of the preceding paragraph extend to the *reporting* of information by employee representatives, even if they are subject to legal obligations of confidentiality or non-disclosure of confidential information. All of the foregoing is without prejudice to the specific protection rules applicable under current local labor laws.

- Whistleblowers shall not incur liability with respect to the acquisition of or access to information that is reported or publicly disclosed, provided that such acquisition or access does not constitute a crime.

- Any other potential liability of *whistleblowers* arising from acts or omissions that are not related to the *report* or public disclosure, or that are not necessary to disclose a violation under the *Whistleblower Protection Policy*, shall be governed by applicable local law.

- In proceedings before a court or other authority concerning harm suffered by *Whistleblowers*, once the *Whistleblower* has reasonably demonstrated that he or she has reported or made a public disclosure in accordance with the *Whistleblower Protection Policy* and that he or she has suffered harm, it shall be presumed that the harm occurred as *retaliation* for reporting or for making a public disclosure. In such cases, the burden of proof shall rest with the person who engaged in the *harmful conduct* to demonstrate that the action was based on duly justified grounds unrelated to the *report* or public disclosure.

- In legal proceedings, including those relating to defamation, copyright infringement, breach of confidentiality, violation of data protection regulations, disclosure of trade secrets, or claims for compensation based on labor or statutory law, individuals who make a *Report* in accordance with this *Procedure,* its local Annexes, and the *Whistleblower Protection Policy*— —shall not incur any liability whatsoever as a result of reports or public disclosures protected by said law. Such individuals shall have the right to assert, in their defense and within the framework of the aforementioned legal proceedings, that they made a report or public disclosure, provided they had reasonable grounds to believe that the *report* or public disclosure was necessary to bring to light a violation under the *Whistleblower Protection Policy*.

9. RECEIPT OF REPORTS AND COMPILATION OF THE RECORD

9.1 Acknowledgment of Receipt

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

The acknowledgment of receipt will include an initial overview of the processing of personal data in accordance with the provisions of the *"Data* Protection" section of this Procedure.

Furthermore, the *Whistleblower* will be expressly informed that their identity (if they have identified themselves) will be protected at all times and will not be disclosed to the individuals to whom the reported facts refer or to *Third Parties*.

Similarly, in accordance with the provisions of the *Internal Information System Policy*, explicit mention will be made of which body will be responsible for managing the *Report*; this may be either the *Local Representative* or the *Compliance Office*, in the cases provided for in the *"Distribution of* Responsibilities" section of the aforementioned *Policy*.

This distribution of responsibilities refers exclusively to the management of *the Internal Information System* and does not prejudge which body is competent to investigate and resolve the merits of the matter when, in accordance with this *Procedure* (for example, in the section *"Handling of Reports Related to* Harassment") or applicable internal regulations, such authority falls to another department or body within the *Organization.*

9.2 Request for Additional Information

If the information received is deemed insufficient, the *Head of the Internal Information System* shall request, at the time of acknowledging receipt—or even subsequently—that *the Whistleblower* provide additional information. It is advisable that the request specify the specific aspects of the information provided that require further detail. This process does not require exhaustive information about the reported *breach*, but only what is strictly necessary for the preliminary compilation and management of the case file .

9.3 Initial Case File Preparation

Based on the information received, the *Head of the Internal Information System* will create an individual file for each case, which will be appropriately numbered and classified with an identification code and the date of registration, to facilitate its identification in the *logbook* specified in the section *"Record of Reports*."

If multiple reports are received regarding the same incident or related incidents, the *Head of the Internal Information System* may consolidate the various files.

9.4 Handling of Reports Related to Harassment

Reports concerning workplace harassment, sexual harassment, harassment based on sex, or situations of discrimination may be submitted through the *Internal Information System*, which serves as a channel for communication in accordance with the *Organization's* internal regulations.

The use of *the Internal Information System* as a reporting channel does not grant the *Head of the Internal Information System* the authority to investigate, examine, or resolve these matters, which fall exclusively under the jurisdiction of the *People & Organization* (*P&O*) Department, in accordance with internal regulations.

In local jurisdictions that have their own regulations regarding harassment, the provisions of such regulations and any applicable local protocols shall apply. In the absence of specific local regulations or protocols, this *GIR Procedure* shall apply on a supplementary basis, and the matter shall be referred to *the Company's P&O* Department, which may rely on *Local Representatives* for operational management.

These *Reports* must be forwarded to the *P&O* Department within seven (7) calendar days from the completion of the preliminary analysis mentioned in the following section, *"Preliminary Analysis of the Report Received*," unless this preliminary analysis indicates the existence of a criminal offense or a *conflict of interest*.

9.4.1 Receipt and Forwarding of Reports Regarding Harassment

Upon receipt of the *report*, the preliminary analysis will verify whether the reported facts relate, in whole or in part, to a situation of workplace harassment, sexual harassment, harassment based on sex, or discrimination.

If it is concluded that the *report* must be processed in accordance with the specific internal regulations on this matter, a preliminary decision will be made to forward it to the *People & Organization* Department, in accordance with the provisions of the section ***"Preliminary Decision on the Information*** Received" of this *Procedure*, transferring only the minimum information necessary for its processing.

The referral shall be purely administrative in nature and shall not imply an assessment of the merits of the case or the exercise of investigative powers by the *Head of the Internal Information System.* In this regard, the matter shall be documented in a reasoned report and communicated to *the Whistleblower*—except in the case of *an* anonymous *report* or a waiver of *notifications*—indicating the body that will conduct the investigation.

9.4.2 Safeguards Regarding Reports of Harassment

Receipt of the *Report* through the *Internal Information System* will not affect the protections afforded to *the Whistleblower*: the confidentiality of their identity and protection against *retaliation,* as provided for in the *Internal Information System Policy* and in this *Procedure,* continue to apply during and after the matter is processed by *P&O*.

The *Head of the Internal Information System* remains responsible for ensuring these protections and may request information regarding the status of the matter solely for this purpose.

When a *report* of harassment involves facts that fall outside the scope of the aforementioned Anti-Harassment Protocol—for example, indications of a crime, associated *retaliation*, or implications for *Senior Management* or the *Board of Directors*—the *Head of the Internal Information System* and *P&O* will coordinate their actions, and the *Compliance Office* may retain or jointly investigate the relevant portion of the case.

9.4.3 Traceability and Data Protection in Harassment Reports

The *Head of the Internal Information System* shall maintain the corresponding record in the *System's Logbook*, documenting the receipt of the *report*, its referral, and the date of administrative closure of the case file, for the purpose of providing evidence of *the System's* operation. The transfer of information to *P&O* shall be carried out in accordance with applicable data protection regulations and shall be limited to what is strictly necessary.

10. ANALYSIS AND PRELIMINARY DECISION ON THE REPORT RECEIVED

10.1 Preliminary Analysis of the Report Received

Once the *Report* has been received and acknowledgment of receipt has been sent to the *Whistleblower*, the *Head of the Internal Information System* will conduct 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 facts, determining whether they may constitute a violation of European Union law, a criminal offense, a quasi-criminal offense, or a serious or very serious 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 seek advice from any internal department deemed appropriate, as well as from external experts in the field, depending on the factual or legal complexity of the *report* received.

10.2 Preliminary Decision on the Information Received

Depending on the outcome of the preliminary analysis, the *Head of the Internal Information System* shall, by issuing a reasoned decision, adopt one of the following decisions within ten (10) business days following acknowledgment of receipt:

a. **Dismissal of the *Report* and** immediate **closure** of the case in the following circumstances:

- When the reported facts do not fall under any of the circumstances covered by the material scope of application of *the Internal Information System*—as defined in the *"Material Scope of* Application" section of the *Internal Information System Policy*.
- When the *report* is a mere repetition of a previous report that was previously deemed inadmissible or has already been duly investigated, without providing any new information.
- When the content of the *report* is manifestly irrelevant or the reported facts are implausible.
- When the information is insufficient to proceed with any further action.

b. **Acceptance of the *Report* and initiation of the corresponding** investigation **file** regarding the reported facts, in accordance with the provisions of this *Procedure* and the local Annexes.

c. **Immediately forward the information to the Public Prosecutor's Office or the competent authority in each country** when the reported facts may, on the face of it, constitute a crime, or to the **European Public Prosecutor's Office** if the facts affect the financial interests of the European Union.

d. **Delegation of the handling of the *report*** to other areas of the *Organization* that have the authority to address specific matters, such as those related to labor issues to the *P&O* department.

In all of the cases described above, the *Head of the Internal Information System* will send *a notification* to *the Whistleblower* regarding whether the *Report* has been accepted or rejected, as

well as any additional measures that may have been taken, within five (5) business days following the conclusion of the preliminary review, unless the *Report* was anonymous or the *Whistleblower* has opted out of receiving *notifications*.

10.3 r precautionary measures

In parallel with the adoption of the decisions described in the preceding section, the *Head of the Internal Information System* may adopt, in coordination with the *P&O* Department when appropriate and in accordance with the procedure established in applicable local labor regulations, all measures deemed necessary in light of *the* reported *breach* to strengthen *Grupo Persán's Criminal Compliance Management System*, to ensure the successful outcome of the future investigation, and/or to effectively protect the *Whistleblower*.

11. INTERNAL INVESTIGATION PROCEDURE

When, in accordance with the provisions of section 10.2.b), the decision is made to initiate an investigation, the following procedure must be followed:

- Select the investigation strategy (see section 11.1).
- Plan the investigation (see Section 11.2).
- Notify the affected parties (see section 11.3).
- Conduct the investigation (see section 11.4).
- Document the investigation process (see section 11.5).
- Prepare the final report (see section 11.6).
- Final steps (see section 11.7).

11.1 Selection of the Investigation Strategy

Depending on the scope, extent, and individuals allegedly involved in the *breach* in question, the *Head of the Internal Information System* will assess the investigation strategy to be implemented for the specific case and may choose one of the following options:

a. The investigation procedure will be led and managed by one of the *members of the Compliance Office* or *a Local Representative*, designated by the *Head of the Internal Information System*, without prejudice to any consultations or ad hoc support that may be required from other departments to fully carry out the investigation. These departments are expressly required to provide the *Head of the Internal Information System* with any information requested that is in their possession or of which they are aware.

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

c. The investigation may be conducted with the advice of an expert *third party.* This approach is particularly recommended in cases where the investigation is deemed to require a high level of complexity and/or confidentiality.

If any member of the specific team designated for the investigation has *a conflict of interest*, that member must recuse themselves from the investigation and may not participate in it.

All persons actively participating in the investigation are obligated to maintain strict confidentiality regarding the facts, data, or names they become aware of as a result of the investigation.

11.2 Investigation Planning

Both the designated *member of the Compliance Office* or *the Local Delegate*, as applicable, will plan the investigation with the aim of clarifying the events that occurred and identifying those responsible. Such planning may include the following elements:

a. Identify the applicable laws, policies, procedures, or internal regulations, as well as any *criminal or compliance risks* that may arise from *the violation*.

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

   The Compliance Office or, where applicable, the *Local Representative* expressly reserves the right to implement the necessary monitoring and control measures regarding the IT tools and resources that the *Organization* makes available to all *Members of the Organization*. In the event of accessing any document that may contain personal information but is stored on professional media and/or equipment, such access must be conducted prudently (always taking into account the principles of appropriateness, necessity, utility, and proportionality) and ensuring the chain of custody.

c. Determine, if necessary, with sufficient justification and in collaboration with the *P&O* Department, the need and, where applicable, the urgency of adopting precautionary measures with respect to the individuals affected by the *Communication*. Precautionary measures are not limited, but may include the following:

   - Transfer the individuals under investigation to another division, area, or department, or temporarily relocate them.
   - Modify the usual duties or responsibilities of the individuals affected by the *Notice*.
   - Immediately suspend the individuals affected by the *Report* from duty with pay.

d. Define the steps to be taken in the investigation and in the various meetings with those involved, with the aim of ensuring the investigation proceeds properly, including identifying individuals to be interviewed, relevant questions to ask, and potential witnesses to the reported incident, among other matters.

e. Include in the investigation file all information that may be of interest regarding the affected individual's work history at *Grupo Persán* (employment history, prior incidents, and *the Organization's* policies, procedures, and regulations that are particularly applicable to them, etc.).

f. When planning the investigation, efforts will always be made to promote:

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

   Always ensuring compliance with the principles governing the *Internal Information System* as set forth in the *Internal Information System Policy*.

11.3 Communication with Affected Parties

Prior to initiating the investigation, the designated *member of the Compliance Office* or *Local Delegate* (hereinafter, the "investigator") will contact the subjects *of the complaint*, identifying themselves as the person in charge of investigating the reported possible irregularity or violation, and informing them of the allegations against them and the main milestones that may occur during the investigation.

In addition, the *Reported party* will be informed of their right to submit written statements and of the processing of their personal data, their right to be heard at any time, and other rights to which they are entitled as set forth in the *Whistleblower Protection Regulations* and the *Internal Information System Policy*.

The foregoing shall be carried out unless, in the investigator's judgment, and in order to prevent evidence from being destroyed and/or concealed, or otherwise to avoid prejudicing the investigation itself, the *notification* to *the Reported party* must be made at a later time and, in any case, when the Reported party's statement is required, either at the time of the hearing or before the conclusion of the investigation process.

Under no circumstances will the identity of *the Whistleblower* be disclosed to the parties affected by the *Complaint,* nor will they be granted access to the *Complaint*.

Without prejudice to the right to submit written statements, the investigation shall include, whenever possible, an interview with the *Reported party* in which, always with absolute respect for the presumption of innocence, the Reported party will be invited to present their version of the facts and to provide whatever evidence they deem appropriate and relevant.

11.4 Investigation Process

The investigation will include all investigative procedures deemed appropriate to clarify the facts, identify those responsible, and determine any corrective measures that may need to be taken.

In any case, the investigation will always be conducted with the utmost respect for the principles governing the *Internal Information System*, as set forth in the section *"Basic Principles of the Internal Information* System" of the *Policy*—particularly with regard to the duty of confidentiality and protection of *the Whistleblower*—and always respecting the presumption of innocence, the right to be heard, and the right to a good reputation of *the Reported party*.

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

a. Conducting an interview with the *Whistleblower* to obtain further information regarding the *Report* submitted.

b. Taking statements from the individuals affected by the *report*.

c. Conducting questionnaires and interviews with witnesses.

d. Scheduling meetings with the *Reported party's* superiors and colleagues, as well as with any other individuals deemed necessary.

e. Gathering as much information as possible from *Grupo Persán*'s documentation.

f. If essential for clarifying the facts, implement surveillance measures using private investigators or computer, telecommunications, or audiovisual means, provided that such measures meet criteria of reasonableness, appropriateness, and proportionality, while ensuring at all times the right to privacy of *the Member of the Organization* and the right to confidentiality of communications, as well as compliance with any other applicable local regulations in this matter.

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 maintaining *communication* with the *Whistleblower* and, if deemed necessary, requesting additional information from the Whistleblower.

The duration of the investigation shall not exceed 3 months from the date of *receipt* of the *Report*. In exceptional cases of particular complexity that require an extension of the deadline, this period may be extended, with justification, for up to an additional 3 months.

11.5 Documentation of the investigation procedure

It is essential to include in the case file detailed documentation of the entire investigation process, including the initial investigation plan, all documents collected, and the transcripts of the interviews conducted.

All interviews conducted must be properly documented, either by preparing a complete and accurate transcript by the *Head of the Internal Information System*—which must be ratified and signed by the interviewees (after giving them the opportunity to review and correct it) and by the *Head of the Internal Information System*—or by recording the interview in a secure, durable, and accessible format —after notifying the interviewees that the *interview* will be recorded and informing them of the processing of their personal data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016—.

Furthermore, in all such cases, information will be provided regarding the collection, processing, and disclosure of personal data in accordance with current data protection legislation.

11.6 Final Report

Once all investigative proceedings have been completed, the investigator will prepare a report of findings that must contain a brief description of the following elements:

a. **Nature of the incident**: To the extent possible, the report shall identify the parties involved, the nature of the events, the date, location, and circumstances in which they allegedly occurred, and the legal provisions or internal regulations that were violated or je , including a statement of the facts along with the *case* identification code and the date of registration.

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

c. **Classification of the *Report*** for the purpose of determining whether it requires priority processing.

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

e. **List of relevant facts and findings**: The most relevant facts identified during the investigation process shall be described, distinguishing them based on the source of information from which they were identified, for example:

- *Persán Group* documentation;
- Information provided by the *Whistleblower*; or
- Information obtained from interviews with the individuals affected by the *report* and with witnesses.

f. **Conclusions and Assessment of the Facts**: The investigator's conclusions and the evidence supporting them shall be specified, along with the investigator's assessment of the facts described. The investigator may propose two possible courses of action:

- **A proposal to continue the proceedings** if it is determined that, based on the investigative steps taken, there is sufficient evidence that the affected individual committed any of the violations set forth in the *"Material Scope of* Application" section of the *Internal Information System Policy*.
- **The proceeding will be closed** if it is determined that the incident does not constitute one of the violations referred to in the *"Material Scope of* Application" section of the *Internal Information System Policy*, if there is insufficient justification for its commission, or if the perpetrator could not be identified. The *whistleblower* and, where applicable, the Reported party will be notified of the closure of the proceeding.

11.7 Final Actions

Once the final investigation report has been prepared, it will be immediately forwarded to *the Head of the Internal Information System* within the same business day.

The final investigation report must be filed along with the rest of the investigation file.

12. CONCLUSION OF THE PROCEEDINGS

12.1 Responsible Body

It is the responsibility *of the Head of the Internal Information System* to make a determination, based on the recommendation contained in the investigator's final report, and to adopt one of the decisions set forth in Section 12.3 of this *Procedure*.

If the person *against whom the complaint is filed* is a *member of the Compliance Office* or the *Local Representative*, that person must recuse themselves from participating in the assessment and resolution of the case involving them.

12.2 Hearing Procedure

Upon receipt of the final investigation report, the *Head of the Internal Information System* shall inform the *Reported party* of the outcome of the investigation, and the Reported party shall be granted a reasonable period of time to present their case in writing or through an interview, as they deem appropriate.

The notification of the final report to *the Reported party* must omit any information regarding the nature of the proceedings, the facts, or the measures taken that could reveal the identity of *the Whistleblower* or violate the *Whistleblower Protection Policy* and/or regulations governing the protection of personal data.

12.3 Decisions of the Head of the Internal Information System

Once the deadline for the *Reported party* to submit their arguments has passed, one of the following decisions may be made:

a. **To admit or reject the evidence submitted by the *Reported party***, providing a reasoned decision.

b. **Request that** the investigator **conduct additional investigative proceedings**.

c. **Dismiss the case** due to insufficient evidence or because the facts are not relevant for these purposes, and proceed to close the file.

d. **Determine that a *violation* has been committed within *Grupo Persán*** and, where appropriate, propose a sanction or measure to the *P&O* Department, the body authorized to impose it.

e. If, following the issuance of the final report, it is determined that the facts may, on the face of the evidence, constitute a crime, the information obtained during **the investigation shall be forwarded** immediately **to the Public Prosecutor's Office or the competent authority in each country**. In the event that the facts affect the financial interests of the European Union, such information shall be forwarded to the European Public Prosecutor's Office.

12.4 Sanctions

The sanctions that may be imposed on *Members of the Organization* in each case shall be those provided for in the applicable Collective Agreements (or, where applicable, equivalent documents) or in the labor laws applicable in each jurisdiction.

Such sanctions will be determined based on the severity of the acts committed, taking into account circumstances such as repeat offenses, the harm or damages caused, and the circumstances of the victims, if any, among others.

Measures in addition to disciplinary actions may also be taken, including filing the appropriate claims or reporting the facts to the relevant administrative, police, or judicial authorities.

The application of these sanctions will be handled by the *P&O* Department.

Likewise, potential sanctions may also be imposed on *Business Partners* who commit any type of *breach* under the terms established in this *Procedure* and its local annexes, which include, among others, the termination of business relationships.

12.5 Other Measures

Additional measures may be adopted in response, such as, by way of example but not limited to:

a. Reporting the facts to any competent authority, whether administrative or judicial.

b. Evaluating prior indications of similar violations and ensuring that appropriate measures are taken to understand the cause of *the breach*.

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

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

e. Make decisions regarding *communication*, training, or internal dissemination of information, both at the level of *a Persán Group* body or unit (division, area, or department) and at the general level (to all *Members of the Organization*) when this is deemed an effective tool for preventing similar *violations* in the future (always with due regard for personal data protection).

12.6 Communication of Decisions

Decisions adopted upon completion of the internal investigation will be immediately notified in writing to the affected parties, as well as to the *Whistleblower*. In the *notification* to the *Reported party* or the *Whistleblowers*, any information regarding 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 and the principles established in this *Procedure* and the *Internal Information System Policy*.

13. RETENTION OF DOCUMENTATION

13.1 Retention periods

Personal data collected through the *Internal Information System* will be retained in accordance with the provisions of applicable local law. Specifically, three (3) months after receipt of the *Report*, if no investigative proceedings have been initiated, the data will be deleted, unless the purpose of retention is to provide evidence of *the System's* operation, in which case the data will be kept in anonymized form.

However, if it is necessary to process personal data for a longer period to continue the investigation or, where applicable, because it is deemed necessary to initiate appropriate legal action, the data will be retained for as long as necessary to conclude the investigation or for *Grupo Persán* to take the corresponding legal action.

13.2 Record of Communications

Grupo Persán will maintain a record of all *Reports* and *Consultations* it may receive through the *Internal Information System*, compiled in the so-called "Logbook," managed via the EQS platform, complying at all times with established confidentiality requirements, and for the time strictly necessary and proportionate to comply with the applicable legal and regulatory requirements of the European Union.

The *Head of the Internal Information System* will record the *reports* received, including the following information:

- Date of receipt.
- Case number.
- Date on which the maximum investigation period of three (3) months ends.
- Method or channel through which the *report* was received.
- Identity of *the Whistleblower* or, if applicable, an indication that the *report* is anonymous.
- Identity of *the person* or *persons* named in the *report*.

In addition, the *Head of the Internal Information System* shall record the actions taken and investigations conducted in each case file, including the following information:

- Acknowledgment of receipt of the *report*.
- Dismissal or acceptance of the *report*.
- Notification to *the Whistleblower* of the acceptance or rejection of the *report*.
- If requested, a meeting with the *Whistleblower* within a maximum of seven (7) calendar days.
- If applicable, a request for additional information from *the Whistleblower*.

- Notification to *the Reported party* of the allegations against them and their rights.
- Hearing with the *Reported party*.
- Conduct of the investigation.
- The *Head of the Internal Information System* will issue the final report with a proposed resolution.
- Notification of the final report to the *Reported* party(ies).
- Final decision by *the Head of the Internal Information System*.
- If applicable, notification to the competent authorities if the facts constitute a crime.
- Other actions.

When the *report* has been made verbally, *Grupo Persán* reserves the right to document the verbal *report* 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 prepared by the *Head of the Internal Information System*.

In any case, the *Whistleblower* has the right to review, correct, and accept the transcript by signing it. *Grupo Persán* will ensure, subject to *the Whistleblower's* consent, that complete and accurate records of the meeting are preserved in a durable and accessible format.

Only upon a reasoned request from the competent judicial authority, by means of a court order, and always within the framework of judicial proceedings and under the authority's supervision, may the contents of *the logbook* be accessed in whole or in part.

The data contained in this *logbook* will be retained only for as long as necessary and, in any case, may not be retained for a period exceeding ten (10) years, except when the retention of the data for a longer period may be necessary for the proper exercise of the right to defense.

The aforementioned *logbook*, as well as the processing carried out by those involved in handling *reports* received through the *Ethics Channel*, will comply with the appropriate technical and organizational measures to ensure a level of personal data security commensurate with the risk and, where applicable, those provided for by the applicable data protection regulations.

14. N PROTECTION OF PERSONAL DATA

14.1 GENERAL PRINCIPLES

Grupo Persán guarantees that personal data obtained through the *Ethics Channel* will be processed in accordance with the provisions of Regulation (EU) 2016/679 (GDPR), the national data protection laws applicable in each jurisdiction where the *Organization* operates, and the corresponding *Whistleblower Protection Regulations.*

The processing of personal data will be carried out in accordance with the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, integrity, confidentiality, and proactive accountability at all times.

14.2 DATA CONTROLLERS

In the context of managing *reports* received through the *Internal Information System*, the following entities shall be considered data controllers:

- The *Persán Group* company with which the *Whistleblower*, the Reported parties, or any other person involved maintains an employment, commercial, contractual, or professional relationship.

- PERSÁN, S.A., as the parent company of *Grupo Persán*, when it participates in the supervision, coordination, management, or investigation of *reports* through the *Compliance Office* or the *Head of the Internal Information System*.

14.3 CATEGORIES OF DATA PROCESSED

In the context of receiving, analyzing, investigating, and resolving *Reports*, the following categories of personal data may be processed:

- Identifying and contact information of *the Whistleblower*, *the Reported party,* or *Third Parties* related to the reported facts, such as first and last names, mailing address, email address, and phone number.

- Professional, employment, or business data, including job title, role, or relationship with the *Persán Group.*

- Alleged *violations* reported.

- Documentation substantiating the alleged *violations* being reported.

Only data that is adequate, relevant, and limited to what is necessary for fulfilling the purposes set forth in this *GIR Procedure* will be processed.

14.4 PURPOSES OF PROCESSING AND LEGAL BASES

Personal data will be processed for the following purposes:

- To receive, record, manage, and respond to *reports* submitted through the *Internal Information System.*

- To analyze, verify, and investigate potential *violations.*

- Protect *whistleblowers* and ensure the effectiveness of the measures set forth in the *Whistleblower Protection Policy.*

- Manage the implementation of disciplinary, corrective, organizational, administrative, judicial, or any other appropriate measures.

- Ensure the proper functioning of *the Internal Information System*.

Therefore, the legal basis for the processing of personal data will be, as applicable in each case:

- Compliance with a legal obligation in cases where regulations require the establishment of a system that allows individuals working for a private entity to report matters of which they are aware regarding potential regulatory violations and anti-corruption issues.

- The public interest in cases where there is no specific regulation governing the need to create an internal reporting system or whistleblower channel, and it is necessary to process personal data to prevent and address potential regulatory violations and to combat corruption.

- The legitimate interest of the *Persán Group* in ensuring compliance with and preventing violations of its internal regulations.

- The execution and management of the existing employment, professional, commercial, or contractual relationship between the data subject and any of the entities of *the Persán Group* when necessary for the processing of the *report.*

14.5 CONFIDENTIALITY

The Persán Group will adopt the necessary technical and organizational measures to preserve the confidentiality of the information received and protect the identity of the Whistleblower, the Reported party, and any third party mentioned in a Report.

Access to the Whistleblower's identity will be strictly limited to individuals authorized to manage the Internal Information System and may only be disclosed in cases required by law and in accordance with the safeguards provided for in applicable regulations.

Reported parties will be informed about the processing of their personal data and about the facts concerning them in accordance with the terms set forth in applicable law, provided that such information does not compromise the investigation or the protection of *the Whistleblower*. In any case, the exercise of *the affected individual's right* of access shall be limited to their own personal data; personal data relating to *the whistleblower* shall not be considered included within the exercise of that right. Likewise, the right to object is also generally limited, as it is understood that there are compelling legitimate grounds that justify the processing of personal data.

14.6 DATA RETENTION

Personal data processed in the *Internal Information System* will be retained only for as long as necessary to fulfill the purpose for which it was collected and to comply with applicable legal obligations.

In general, personal data obtained in the context of an internal investigation will be deleted when it is no longer necessary or relevant and, in any case, within a maximum period of three (3) months from the date the *report* is filed, unless the investigation is still ongoing or in cases where the purpose is to demonstrate the functioning of *the System*, in which case the data will be kept in anonymized form.

Personal data that falls outside the scope of the *Ethics Channel*, is not necessary for the conduct of the investigation, and/or is not the subject of the investigation—or when it is established that the information is untrue—will be deleted or anonymized, except in cases provided for by applicable regulations.

14.7 RECIPIENTS OF THE DATA

To fulfill the aforementioned purposes of processing, personal data may be disclosed to or made accessible exclusively to those individuals and entities whose involvement is necessary for the proper handling of the *Report*, including:

- The *Head of the Internal Information System*.
- Duly authorized Local Representatives.
- *The Compliance Office*.
- Those areas, departments, or entities within *the Persán Group* that are relevant to the investigation and any measures to be taken regarding the reported conduct in question.
- The management or governing bodies of *the Persán Group* when necessary.
- External advisors, professionals, or specialized service providers who assist in the management or investigation of a Report.
- Competent judicial, administrative, prosecutorial, law enforcement, or regulatory authorities.

All recipients will be subject to the applicable confidentiality and data protection obligations.

14.8 INTERNATIONAL DATA TRANSFERS

Some entities within the *Persán Group*, as well as certain service providers, may be located outside the European Economic Area and, therefore, may not provide a level of data protection comparable to that of the European Union.

In such cases, *the Persán Group* will implement the appropriate safeguards required by applicable regulations regarding international data transfers, such as Standard Contractual Clauses or any other relevant supplementary measures. The content of the Standard Contractual Clauses can be viewed at the following link: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en.

14.9 RIGHTS OF DATA SUBJECTS

Finally, subject to the conditions set forth in applicable regulations, you may exercise the following rights:

- **Right of Access**: You have the right to request that the *Organization* confirm whether it is processing your personal data and, if so, to request access to such data. The information provided includes—among other things—the purposes of the processing, the categories of personal data involved, and the recipients or categories of recipients to whom the personal data have been or will be disclosed. You may obtain a copy of the personal data being processed.

- **Right to rectification**: You have the right to request that the *Organization* correct any inaccurate or incomplete personal data.

- **Right to erasure (right to be forgotten):** You have the right to request that the *Organization* erase your personal data.

- **Right to restriction of processing:** You have the right to request that the *Organization* restrict the processing of your personal data; however, the *Organization* will conduct a case-by-case analysis to determine whether the exercise of this right is appropriate.

- **Right to object:** Under certain circumstances, you have the right to object to our processing of your personal data.

Data subjects may exercise their rights by sending an email togdpr@persan.es or by mail to PERSÁN, S.A., located at C/ Pino Albar, 2, 41016 Seville, with the **subject line "Data** Protection" and specifying the right they wish to exercise. They also have the right to file a complaint with the competent data protection authority in each case.

15. DISSEMINATION, REVIEW, AND UPDATE OF THE PROCEDURE

This *Procedure* will be made available to all *Members of the Organization* through the internal corporate communication channels deemed appropriate at any given time. It will also be made available to *Business Partners*, *Third Parties*, and other stakeholders via the corporate website or through other means that the *Organization* deems appropriate under certain circumstances to ensure its proper dissemination and understanding.

In order to ensure its proper implementation, the *Organization* will promote the communication, training, and awareness-raising initiatives necessary to foster knowledge, understanding, and compliance with the provisions contained in this *Procedure* by its intended audience.

This *Procedure* will be subject to periodic review and may be updated as necessary, at the recommendation of the *Compliance Office*, in order to ensure its alignment with applicable regulatory changes, evolving best practices in this area, and any changes that may occur in the *Persán Group's business* activities, organizational structure, or operating environment.

Any updates will be duly communicated to the intended recipients, and appropriate measures will be taken to ensure their effective implementation and compliance.