INTERNAL INFORMATION SYSTEM POLICY



Date of Approval and Change Log for This Document

Version	Date	Description
1.0.	June 20, 2023	Approval by *the Board of Directors*: Update to the Internal Information Channel (Law 2/2023).
2.0.	September 21, 2023	Amendment at the request of employee representatives.
3.0.	August 8, 2024	Approval by the *Board of Directors*: Phase 1 update of the certification process for the Criminal *Compliance* Management System in accordance with UNE 19601:2017.
4.0.	September 25, 2025	Approval by the Board of Directors: update to *the Criminal Compliance Management System* (organizational changes).
5.0	September 2, 2026	Approval by the *Board of Directors*: international rollout of *the Internal Information System*.

TABLE OF CONTENTS

1. DEFINITIONS 4
2. OBJECTIVE 8
3. MATERIAL SCOPE OF APPLICATION 9
4. SCOPE OF APPLICATION REGARDING PERSONNEL 11
5. BASIC PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM 12
6. GOVERNANCE AND RESPONSIBILITIES 13
6.1 DISTRIBUTION OF RESPONSIBILITIES 13
7. CHANNELS OF COMMUNICATION FOR THE INTERNAL INFORMATION SYSTEM 15
8. PROTECTION OF WHISTLEBLOWERS 16
9. PROHIBITION OF RETALIATION 18
10. DISSEMINATION AND UPDATES TO THE POLICY 20

1. DEFINITIONS

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

- ***Persán Group / the Organization***: This term 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 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 the *Persán Group's* activities, governance, and policies, to which *senior management* reports and is accountable.

- ***Senior Management / Management Committee***: the high-level body within the *Persán Group* that reports directly to *the Board of Directors*. It currently consists of the *Persán Group 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 *the Persán Group* 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 reporting on violations of Union law (the "Whistleblowing Directive"); the Whistleblower Protection Regulations applicable in each country that transposes said Directive, including, in the case of Spain, Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption (Whistleblower Protection Law); and the principles of ISO 37002:2021, on Whistleblowing Management Systems, for the management of *reports* regarding violations of the regulations referred to in this text.

- ***Head of the Internal Information System***: The *Chief Risk & Compliance Officer* has been appointed to ensure the prompt processing of *reports* received through the *Ethics Channel* and must perform his or her duties with full autonomy and independence from the other bodies of *Persán Group*. The *Head of the Internal Information System* has been delegated authority by the *Persán Group Board of Directors* 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 *Persán Group'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*, 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 designation should be confused with the other, nor do they necessarily imply the same scope of authority or the same appointing body.

  In this regard, a distinction is made between the roles of the Local Criminal Compliance Management System Representative, for functions strictly related to the Criminal Compliance Management System, and the Local Internal Information System Representative, for functions strictly related to the Internal Information System.

  Local Delegates must have express written authorization from the appointing body in each case, sign the corresponding confidentiality agreement, meet 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 an *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 categories listed above.

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

- ***Non-compliance***: irregular 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 proceeding, in order to ensure its proper conduct and respect for their rights.

- ***Criminal risk:*** risk related to the commission of conduct that could constitute a crime, in accordance with the regime of criminal or quasi-criminal liability of 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 this *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 made without the intent to seek revenge or to cause employment-related or professional harm to *the person against whom the report is made* or to a *third party*.

- ***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***: the set of corporate provisions contained in this document (hereinafter also referred to as the "Policy").

- ***Corporate Procedure for the Management, Investigation, and Response to Communications Received Through the Internal Information System (GIR)***: 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 *non-compliance*, as well as the procedures required for the internal processing of *consultations*, and the internal processing and investigation of any *Complaints* or known circumstances that must be investigated.

  The local annexes form an integral part of *the GIR Procedure* and detail the specific provisions and requirements mandated by the applicable regulations in each jurisdiction where *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***: an organizational and management system for the prevention of *non-compliance*, whose objective is the prevention, detection, and management of risks through their integration into business processes, as well as the measurement of performance for continuous improvement, and whose essential foundation is represented by the *Criminal Compliance Policy* and the *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

Persán Group, within the framework of its *Criminal Compliance Management System* and in accordance with applicable international best practices, has implemented an *Internal Information System* that allows for the reporting of potential regulatory *violations*, as well as the submission of *consultations* related to external and internal regulations applicable to the *Organization*.

The purpose of this *Internal Information System Policy* is to establish the principles, commitments, and general guidelines governing the operation of ***Persán Group's*** *Internal Information System*, as well as to ensure the protection of *whistleblowers*, the confidentiality of *reports*, the prohibition of *retaliation*, and respect for the rights of all individuals involved.

This *Policy* constitutes the corporate framework of reference for all *Persán* ***Group*** companies, serving as the basis for the development of the internal procedures necessary for managing *reports* received through the *Internal Information System*.

Persán Group fully embraces international standards in this area, particularly the ***Whistleblowing Directive***, the ***Whistleblower Protection Regulations***, and the principles of ISO 37002:2021.

The provisions contained in this *Policy* are supplemented by the *GIR Procedure*, which sets forth the operational aspects necessary for the management, investigation, and response to received *reports*. This *Policy* is intended to serve as a common corporate standard. The application of this *Policy* and its implementing regulations shall in no case result in non-compliance with the legal provisions in force in the markets where *Persán Group* operates.

In the event of a conflict between the content of this Policy and a mandatory requirement of local regulations, the latter shall prevail under the terms specified by the corresponding local regulation.

3. SCOPE OF APPLICATION

This *Policy* protects all individuals and legal entities who report, through any of the channels established in this *Policy*, any:

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

    a. They fall within the scope of the European Union acts listed in the annex to the Whistleblowing Directive, regardless of how they are classified under national law.

    b. Affect the financial interests of the European Union as set forth in Article 325 of the Treaty on the Functioning of the European Union (TFEU).

    c. Have an impact on the internal market, as set forth in Article 26(2) of the TFEU, including violations of European Union rules on competition and state aid, as well as violations relating to the internal market in connection with acts that infringe corporate tax rules or practices intended to obtain a tax advantage that undermines the object or purpose of the legislation applicable to corporate tax.

2. Acts or omissions that may constitute **a criminal offense, a quasi-criminal offense, or a serious or very serious administrative offense**.

3. Additionally, acts or omissions that may constitute a ***violation* of the *Organization's* internal regulations** but do not constitute a violation of European Union law or a serious or very serious criminal, quasi-criminal, or administrative offense, including the principles and values that serve as a guide for the conduct of all *Members of the Organization*.

Reports related to labor issues and those related to professional performance (career development, compensation, vacation time, interpersonal conflicts, etc.) **are excluded** from the scope of application of *the Internal Information System*. In such cases, while these communications may be received through the *Internal Information System,* their investigation and resolution shall fall under the jurisdiction of *the People & Organization* ("P&O") Department or the relevant area or body depending on the subject matter, in accordance with applicable internal regulations. However, the foregoing exclusion shall not apply when the reported facts, even if they involve labor-related elements, may constitute a criminal offense, a quasi-criminal offense, or a serious or very serious administrative violation, or a violation of the *Organization's* internal regulations. In such cases, the *Report* shall be processed in accordance with this *System*.

Furthermore, the process for *submitting reports* through the *Internal Information System* must not be used to report events that pose an immediate threat to life or property. In such cases, the situation must be handled directly through the competent authorities. Additionally, when circumstances so require, the matter must be reported immediately to the appropriate supervisor.

In essence, through the *Internal Information System*, any *non-compliance* committed by *members of the Persán Group*, *business partners*, or *third* parties—relating to the types of *non-compliance* referred to in this section of the *Policy*—may be reported, with *whistleblowers* enjoying the protection established in this *Policy*.

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 *violation* of the

Organization's internal regulations, including the principles and values that serve as a guide for the conduct of all *Members of the Organization*, as well as submit any *consultation* regarding the scope, compliance with, and interpretation of the internal and external regulations applicable to the *Organization*.

4. SCOPE OF APPLICATION

This *Policy* shall apply to all companies comprising the *Persán Group*, without prejudice to any regulatory adjustments that may be necessary to ensure its proper implementation.

This *Policy* applies not only to *Members of the Persán Group, business partners*, *and third parties*, but also to other collaborators such as volunteers, interns, and employees in training periods—regardless of whether they receive compensation—as well as job candidates in the selection process, employees whose employment or business relationship has ended, and employee representatives, as well as any person working for or under the supervision and direction of contractors, subcontractors, and suppliers, and partners, shareholders, and members of the *Board of Directors* and *Senior Management* of *Persán Group* who submit a *Report* regarding any of the matters outlined in the preceding section of this *Policy* (***"Scope of*** Application").

The protective measures provided for in this *Policy* shall also apply, where applicable:

(i) To individuals who, within the framework of the *organization* where 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* coworkers or family members; and

(iii) Legal entities for which I work, with which I have any other type of relationship in a work context, or in which I hold a significant interest.

5. BASIC PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM

The *Internal Information System* is governed by the following principles, which must be observed during the processing of any case:

- **Confidentiality:** The *Internal Information System* shall guarantee the confidentiality of the *Whistleblower's* identity, the identity of any person mentioned in the *report*, and the details regarding the reported incident, except when *a report* is submitted to a 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 Information System* must, in all cases, be guided by the principle of impartiality, treating all *reports* uniformly, regardless of the individuals involved, and avoiding any type of *conflict of interest*.

- **Objectivity**: The investigation shall cover not only the facts and circumstances that establish and aggravate the responsibility of *the Reported party*, but also those that exempt them from such responsibility 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 determine the investigative steps deemed necessary to clarify the reported facts, always pursuing the search for the truth.

- **Documentation:** Each *report* shall give rise to a case file, in which the *Head of the Internal Information System* shall include detailed documentation of the entire investigation process.

- **Good Faith:** The provisions of the *GIR Procedure* and this *Policy* must be interpreted in accordance with the principles and requirements of good faith.

- **Proportionality**: This principle addresses the need for the sanction to be commensurate with the seriousness of the facts, ensuring that it is not a disproportionate measure.

- **Principle of "due process":** Every person has the right to be heard and to assert their legitimate claims before those conducting the investigation.

6. GOVERNANCE AND RESPONSIBILITIES

The Organization's Board of Directors has appointed the *Chief Risk & Compliance Officer* as *the Head of the Internal Information System*. This individual has specific authority to manage the *Internal Information System* and process reports, and provides adequate guarantees of independence, confidentiality, data protection, and the secrecy of communications. This formal appointment was made via *a Board of Directors'* Resolution.

In this regard, the *Head of the Internal Information System* will manage the *Ethics Channel* through *the Persán Group Compliance Office*, which is composed of:

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

Likewise, the *Head of the Internal Information System*, by virtue of the powers of delegation expressly conferred upon him or her by the *Board of Directors* of *Persán Group*, may appoint the person he or she deems appropriate and suitable as *a Local Representative* to support, at the local level and under his or her supervision, the operational management of *the Internal Information System* in the various jurisdictions where the *Organization* operates.

Any member of the *Compliance Office,* as well as any *Local Representatives* who are operationally involved in the receipt, processing, or management of *Reports*, must meet appropriate standards of professional competence, functional independence, and freedom from *conflicts of interest*, and must strictly observe the duties of confidentiality, data protection, and the confidentiality of *Reports* applicable to *the Internal Information System*.

6.1 DISTRIBUTION OF RESPONSIBILITIES

In general, the management of *reports* received through *the Internal Information System* shall be the responsibility *of the Head* of *the Persán Group's Internal Information System*, through the *Compliance Office,* who may rely on the *Local Representatives* designated in each jurisdiction.

In countries where a *Local Representative* exists, that representative may be involved in the receipt, preliminary analysis, investigation, and follow-up of *reports* that exclusively concern the corresponding subsidiary, under the supervision of *the Head of the Internal Information System*, who bears ultimate responsibility for the management of *the System*.

Furthermore, in order to ensure the independence, impartiality, and effectiveness of *the Internal Information System* throughout the *Persán Group*, the *Compliance Office* may directly assume management of any *Report* when circumstances so warrant.

In particular, and without limitation, the *Compliance Office* shall be responsible for the direct management of *Reports* when:

a) The *report* involves members of *senior management* and/or members of *the Board of Directors*, in which case it will be reported to a director who is not involved.

b) There are actual or potential *conflicts of interest* that could compromise the independence or impartiality of the *local representatives* responsible for operational management.

c) The *Whistleblower* expressly requests that the matter be handled by *Persán* or, as appropriate, directs the *report* to the *Persán Group Compliance Office,* regardless of where the incident or event occurred.

d) The *report* may have a significant impact on several companies within *the Persán Group* or affect common corporate interests.

e) The circumstances of the case or the complexity of the facts warrant centralized handling.

f) There are risks regarding the protection of the *Whistleblower's* confidentiality, protection against *retaliation,* or the proper conduct of the investigation.

In such cases, the *Compliance Office* may handle the *report* directly or coordinate its processing with the support of local resources, specialized external advisors, or any other person it deems necessary, ensuring at all times compliance with applicable *local regulations* and the principles set forth in this *Policy*.

In any case, the decision regarding which body is responsible for handling *reports* rests with *the Head of the Internal Information System*, who must document such decision.

Finally, if any of the circumstances described in this section arise during the processing of a *Report*, the *Head of the Internal Information System* may reassign its handling to the body or person deemed most appropriate to ensure the independence, impartiality, and effectiveness of *the System*.

7. COMMUNICATION CHANNELS OF THE INTERNAL INFORMATION SYSTEM

Any *member of Persán Group, business partner*, or *third* party who becomes aware of any *violation* committed by any other *member of the Organization* or *business partner* in a work or professional context may immediately report it without fear of suffering any form of *retaliation*. In this regard, all *members of the Organization*, *business partners*, and *third parties* are encouraged to use the channels established by the *Organization* for reporting *violations*.

The *Ethics Channel* is the preferred means for reporting the actions or omissions described in the *"Scope of* Application" section of this *Policy*, provided that the *non-compliance* can be effectively addressed and the *whistleblower* believes there is no risk of *retaliation*.

Reports may be submitted either by name or anonymously, in cases permitted by the *Whistleblower Protection Regulations*.

The specific characteristics of each reporting channel, the requirements for their use, the minimum content of *reports*, the mechanisms for providing further details or requesting additional information, as well as the rules for documenting, recording, and following up on such reports, are detailed in the *"Reporting* Channels" section of *the GIR Procedure.*

Similarly, the rules governing the management of potential *conflicts of interest* involving individuals handling *reports*, as well as the mechanisms established to ensure the independence and impartiality of the process, are set forth in the *GIR Procedure*.

Without prejudice to the use of *Persán Group's* internal channels, *Whistleblowers* may utilize external reporting channels or communication mechanisms with the competent authorities that are applicable in accordance with the *Whistleblower Protection Regulations* of the relevant jurisdiction. *Reports* submitted through these channels will enjoy the same protection recognized in this *Policy* when the required conditions are met. The competent external authorities in each jurisdiction are identified in the corresponding local appendices.

8. WHISTLEBLOWER PROTECTION

At *Persán Group*, individuals who report or disclose violations in good faith **will enjoy all the protection rights** provided for in this *Policy* and in the *GIR Procedure*, provided that:

1. Have reasonable grounds to believe that the information they report to *Persán Group* is accurate at the time of the *report*, and that said information falls within the material scope of the *Whistleblower Protection Regulations*.

2. They must have made the *report* or disclosure in accordance with the requirements established for that purpose by *Persán Group* and the *Whistleblower Protection Regulations*.

Individuals who have reported or publicly disclosed information in good faith regarding acts or omissions covered by the *Whistleblower Protection Regulations* on an anonymous basis, but who have subsequently been identified and meet the conditions set forth in this section, shall be entitled to the protection provided by the *Whistleblower Protection Regulations* and this *Policy*.

Individuals who, in good faith, report violations falling within the scope of the Whistleblowing Directive to the relevant institutions, bodies, or agencies of the European Union shall be entitled to protection in accordance with the provisions of the *Whistleblower Protection Regulations* and this *Policy*.

Conversely, individuals who communicate or disclose the following **will not be entitled to the protection** provided for in this *Policy* and the *GIR Procedure*:

1. Information contained in *reports* that have been deemed inadmissible for any of the following reasons:

    a. When, following a preliminary analysis, the facts described lack any plausibility, as duly justified.

    b. When the facts described do not constitute a violation of the legal system within the scope of the *Whistleblower Protection Regulations* or the scope of this *Policy*.

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

    d. When the *report* does not contain new and significant information regarding violations that were the subject of a previous *report* for which the corresponding proceedings have been concluded, unless there are new factual or legal circumstances that justify a different course *of* action. In such cases, the *Head of the Internal Information System* shall notify the decision, providing a statement of reasons.

2. Reports related to complaints about interpersonal conflicts or that affect only the *Whistleblower* and the individuals referred to in the *report* or disclosure.

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

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

The whistleblower will be *notified* of the rejection of the *report* submitted through the appropriate channels within a reasonable period of time, no later than **fifteen (15) business days** following acknowledgment of receipt of the *report*, unless the *report* was anonymous or the whistleblower has opted out of receiving *notifications* regarding the proceedings.

9. PROHIBITION OF RETALIATION

Persán Group will take the necessary measures to prohibit any act constituting *retaliation* or *harmful conduct*, including threats of *retaliation* and attempts at *retaliation*, against individuals who submit a *report* regarding actions or omissions falling within the material scope of application of this *Policy*.

"Retaliation" is understood to mean any acts or omissions that are prohibited by law, or that, directly or indirectly, constitute unfavorable treatment that places the persons subjected to them at a particular disadvantage compared 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, but not limited to, the following are considered *Retaliation*:

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

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

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

4. Failure to convert a temporary employment contract into a permanent one, if the employee had legitimate expectations that they would be offered permanent employment.

5. Damages, including reputational harm, or financial losses, coercion, intimidation, harassment, or ostracism.

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

7. Inclusion on blacklists or the dissemination of information within a specific sector that hinders or prevents access to employment or the awarding of contracts for work or services.

8. Denial or revocation of a license or permit.

9. Denial of training.

10. Discrimination, or unfavorable or unfair treatment.

The measures listed in paragraphs 1 through 4 above shall not be considered *retaliation* when carried out within the regular exercise of managerial authority under labor law or regulations governing the status of public employees, based on proven circumstances, facts, or violations unrelated to the submission of the *report*.

Furthermore, it is hereby noted that any person whose rights have been infringed upon as a result of their *report* or disclosure, once the two-year period has elapsed, may request protection from the *Independent Whistleblower Protection Authority* or an equivalent competent body within the relevant local jurisdiction, which, in exceptional and justified cases, may extend the protection

period, following a hearing with the persons or bodies that may be affected (any denial of such an extension of the protection period must be supported by reasons).

Likewise, it is hereby made known that any acts intended to prevent or hinder the submission of *reports* and disclosures, as well as those that constitute *retaliation* or result in discrimination following the submission of such reports under the *Whistleblower Protection Regulations*, shall be null and void and shall give rise, where applicable, to disciplinary or liability measures, which may include the corresponding compensation for damages to the aggrieved party.

In addition, *whistleblowers* may have access, as appropriate, to various support measures provided by the *Independent Whistleblower Protection Authority* and/or the competent body designated in each of the relevant jurisdictions.

10. DISSEMINATION AND UPDATES TO THE POLICY

This *Policy* will be made available to all employees of the *Organization* through the internal corporate communication channels deemed appropriate at any given time. Likewise, it will be accessible to interested *third parties* through the corporate website or through any other means determined by the *Organization* to ensure its adequate dissemination and awareness.

In addition, the *Policy* will be translated into whatever other languages are necessary to ensure its proper understanding by all recipients in the various jurisdictions where *the Persán Group* operates.

Likewise, this *Policy*, as well as any procedures, protocols, or instructions approved for its development and implementation, will be the subject of the communication, awareness-raising, and training initiatives necessary to ensure that all recipients are aware of it, understand it, and apply it correctly.

The *Organization* will promote a culture of compliance, integrity, and transparency, fostering awareness of the *Internal Information System*, the channels established for reporting information, and the protections afforded to whistleblowers, affected parties, and other individuals involved in the process.

This *Policy* will be reviewed periodically and updated when circumstances require it, at the initiative of the *Compliance Office*, to ensure its alignment with applicable legislative and regulatory developments, current standards and best practices, as well as any changes that may occur in the *Persán Group's business* activities, structure, or operating environment. In all cases, care will be taken to ensure its proper implementation and effective compliance.