

Título: **WHISTLEBLOWING CHANNEL**

Nº: **CMP.PO.01.V.1**

Date of BoD Approval: **30/10/2025**

UNCLASSIFIED

Proprietary Notice

This document contains data that is the property of PAP TECNOS. Duplication, use, or disclosure, in whole or in part, is prohibited for any purpose other than the implementation and enforcement of this IMS.

INDICE

1. INTRODUCTION.....	4
2. PURPOSE AND OBJECTIVE	4
3. SCOPE OF APPLICATION.....	4
4. REGISTRATION	4
5. MONITORING, REVIEW AND TRAINING	5
6. DATA PROTECTION GUARANTEES.....	7
7. SANCTION REGIME.....	10
8. RECORDS	10
9. ANNEXES	11

CHANGE CONTROL SHEET

VERSION	DATE	SECTION	MODIFICATION MADE
1	30.10.2025		First edition

1. INTRODUCTION

PAP Tecnos Innovación, S.A.U. (hereinafter, "PAP Tecnos" or the "Company"), is committed to complying with national and international legislation that regulates all aspects of its activity.

By virtue of this commitment, the Board of Directors of PAP Tecnos, in compliance with its responsibilities, has promoted the drafting and application of this Whistleblowing Channel Procedure (hereinafter, the "Procedure") that regulates the "internal information system of PAP Tecnos" known as the Whistleblowing Channel.

This Procedure establishes a series of rules and guidelines for action in relation to the procedure to be followed to process and resolve any complaint received regarding possible breaches of the Company's internal regulations or of the legislation in force and applicable.

2. PURPOSE AND OBJECTIVE

The purpose of this Procedure is to establish a process through which any individual can report or inform PAP Tecnos of any breach or suspected breach of its internal regulations or applicable legislation in force, as well as any other matter not covered by such systems. This allows PAP Tecnos to manage and resolve reports in accordance with the legislation in force at any given time.

3. SCOPE OF APPLICATION

This Procedure shall apply to all individuals associated with PAP Tecnos, including members of the Board of Directors, executives, and employees, as well as Third Parties, suppliers, and clients who do business with PAP Tecnos. It also extends to any natural or legal person who maintains any kind of relationship with PAP Tecnos and may become aware of possible regulatory breaches in the course of their activity.

Likewise, this Procedure applies to all those who report alleged breaches through the channels indicated in this document. Non-compliance with this Policy may lead to serious employment consequences, including termination of the employment relationship.

4. REGISTRATION

The reporting procedure shall be governed at all times by the following principles and guarantees:

- Guarantee of confidentiality regarding the identity of the whistleblower, the subject of the investigation, and any other affected person or third party, as well as the handling of information and the investigation itself.
- Protection of the privacy and dignity of all individuals involved.
- Priority and urgent processing, depending on the nature of the report.
- Thorough investigation of all facts and any relevant documentation provided, carried out by specialized professionals if necessary.
- Possibility of maintaining communication with the person submitting the report.

- Guarantee of the presumption of innocence and the right of defense for all affected parties.
- Assurance of appropriate actions being taken, including disciplinary measures where necessary.
- Prohibition of retaliation against whistleblowers acting in good faith, and the possibility of compensation in cases of retaliation.
- Option to submit anonymous reports.

5. MONITORING, REVIEW AND TRAINING

The Compliance Officer, appointed by the Board of Directors as the Person Responsible for the Reporting System, shall be in charge of internally monitoring the correct application of the provisions of this Procedure.

All PAP Tecnos personnel are required to be aware of, apply, and comply with the contents of this Procedure, regardless of the fact that the Person Responsible for the Reporting System is tasked with overseeing its internal implementation. Therefore, this Procedure shall be made available to all such individuals for consultation.

If a complaint is made against the Compliance Officer or employees within their area of responsibility, in order to avoid a conflict of interest, the General Director (moises@paptecnos.es) will be responsible for its oversight and review.

5.1. PROCEDURE

PAP Tecnos has created the role of the Person Responsible for the Reporting System, whose primary function, as the person in charge of the Whistleblowing Channel, is to oversee the Whistleblowing Channel. This role also entails the responsibility of ensuring the effective implementation and operation of the Whistleblowing Channel.

5.1.1. START: FILING THE REPORT

Initially, the whistleblower may inform the Information System Officer, confidentially and, if desired, anonymously, of the subject and nature of their report, either in writing (including anonymously) or verbally.

The designated complaints channel for submitting any complaint has been set up through the ithikios.com platform ithikios.com (paptecnos.ethic-channel.com) which offers various options for filing a complain:

1. **In writing without anonymity.** In all cases, full confidentiality of the personal data of any person involved is guaranteed, including the whistleblower, the subject of the report, witnesses, and any other individuals involved in the report and its subsequent investigation.
2. **In writing with anonymity.** If the whistleblower prefers, they have the option to submit their report anonymously by selecting the appropriate checkbox on the whistleblowing channel's digital platform.
3. **Verbally without anonymity.** The technological platform has enabled the possibility of making complaints orally, through an audio recording and in a secure, durable, and accessible format. In the case that the informant does not intend to preserve anonymity, once their audio recording is made, they can uncheck the enabled option for audio distortion.

4. **Verbally with anonymity.** The technological platform has enabled the possibility of reporting any complaint orally, through audio recording and in a secure, durable, and accessible format. If the informant intends to preserve anonymity, once their audio recording is made, they must check the enabled option for audio distortion and, if they wish, remove the metadata from the audio file.

Within a maximum period of seven (7) days from the receipt of the report, an acknowledgment of receipt will be sent to the whistleblower, unless doing so could compromise the confidentiality of the report. For this reason, the whistleblower must retain the password used to access the status of the case. Through the platform, the whistleblower may also provide additional information or evidence if deemed necessary.

Additionally, the whistleblower may request an in-person meeting with the Information System Officer to report a misconduct. In any case, the conversation will either be recorded in a secure, durable, and accessible format or the content of the meeting will be documented in writing by means of a full and accurate transcript of the conversation, which must be signed by both the whistleblower and the Information System Officer, depending on who attends the in-person meeting with the whistleblower.

The contact details of the Information System Officer are as follows:

- Pedro Marcos, Chief Financial and Human Resources Officer and Compliance Officer – pjmarcos@paptecnos.es.

The internal channel described in this procedure shall be the preferred method for reporting. However, if the whistleblower perceives a risk of retaliation from using the internal channel, they may submit their report through various external reporting channels:

- European Union: <https://commission.europa.eu/about-european-commission/contact/problems-and-complaints_en>.
- Independent Authority for the Protection of Whistleblowers.
- Community of Madrid <<https://www.comunidad.madrid/servicios/consejo-transparencia-proteccion-datos/canal-externo-informante>>

The information provided regarding the observed breach may affect other individuals; therefore, the whistleblower must verify and ensure the accuracy of the information and proceed with the utmost confidentiality.

5.1.2. INVESTIGATION OF THE REPORT

The Information System Officer shall have sufficient authority to communicate with any person at PAP Tecnos, regardless of their hierarchical level, to obtain any information or data deemed necessary for the proper development of the investigation.

If the report concerns matters within the scope of the Human Resources department, the Information System Officer shall assign its management to a member of this department.

During the investigation period, the Information System Officer and/or the specialized professionals tasked with conducting the investigation shall carry out the necessary procedures to ensure an effective inquiry into the events (through interviews with all parties involved, requests for documents, etc.), guaranteeing full respect for the presumption of innocence, the right of defense, and the honor of the affected persons.

In any case, the formal investigation process shall not exceed three (3) months from the receipt of the report or complaint, except in particularly complex cases that require an extension, in which case it may be extended for a maximum non-extendable period of an additional three (3) months.

Additionally, when the facts could potentially constitute a criminal offense, the Information System Officer is obliged to refer the matter to the Public Prosecutor's Office.

5.1.3. CORRECTIVE MEASURES

Once the investigation process has been completed, the Information System Officer shall issue a written report within the aforementioned period. This report shall (i) identify the facts and outline the investigation process followed; (ii) establish corrective or disciplinary measures deemed appropriate, in the event that the investigation concludes that a regulatory breach has indeed occurred and is subject to correction or sanction; or, conversely, if it is determined that no regulatory breach has taken place, (iii) the report shall order the closure of the case.

5.1.4. ADDITIONAL PROVISIONS

The President of PAP TECNOS' Board of Directors will be notified within 7 labour days of any matters that may be received in relation to the provisions of this procedure.

- **Precautionary measures:** During the handling of the procedure, the Information System Officer shall adopt the necessary measures aimed at the immediate cessation of any proven misconduct, or any measures required to effectively carry out the investigation.
- **Assistance to the parties:** During the investigation process, the parties involved may be assisted by a trusted person, provided that this person maintains confidentiality regarding any information they become aware of during the process.
- **Prohibition of retaliation:** Retaliatory acts, including threats of retaliation against whistleblowers, witnesses, or those who assist or participate in investigations concerning any regulatory non-compliance, are strictly prohibited.
- **False reports:** Any report that does not reflect the truth, or that the Information System Officer deems false, is expressly prohibited. Accordingly, disciplinary action may be taken against any person linked to PAP Tecnos who submits a false or misleading report.

6. DATA PROTECTION GUARANTEES

The following data protection considerations are described in accordance with the following legal provisions:

- Regulation (EU) 2016/679 General Data Protection Regulation (GDPR),
- Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD)
- Organic Law 7/2021, May 26, on the protection of personal data processed for the purpose of the prevention, detection, investigation, and prosecution of criminal offenses and the execution of criminal penalties

6.1. LAWFULNESS OF THE PROCESSING

When the implementation of the Information System is mandatory, it shall be presumed lawful as a result of compliance with an applicable legal obligation¹. If not established as mandatory or through a public disclosure, data processing shall be justified by the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller².

Likewise, in cases where data is **shared within the organization** (always confidentially and only with authorized individuals), such communication shall be considered lawful based on regulatory criteria.

When **special category data is processed for reasons of substantial public interest**, such processing shall be lawful pursuant to Article 9.2(g) of the GDPR.

6.2. TRANSPARENCY AND INFORMATION

Whistleblowers who use the channel must be informed in accordance with Article 13 of the GDPR and Article 11 of the LOPDGDD.

Whistleblowers and those who make a public disclosure must also be expressly informed that their identity will in all cases be kept confidential and will not be disclosed to the individuals referred to in the reported facts or to third parties.

The person referred to in the reported facts shall not, under any circumstances, be informed of the identity of the whistleblower.

Likewise, both **Personnel and third parties** must be informed about the processing of personal data within the framework of the information systems.

Employees must have been previously informed of the existence of these systems and of the data processing involved in submitting a report.

This information may be provided through several channels:

- Directly in the employment contract.
- Individually or collectively when implementing or modifying the system.
- Through information circulars to staff and their representatives, informing them of the existence and purpose of the data processing associated with these mailboxes or whistleblowing systems.

¹ Articles 6.1.c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 8 of Organic Law 3/2018 of 5 December 2018 and 11 of Organic Law 7/2021 of 26 May, when, in accordance with the provisions of Articles 10 and 13 of this Law, it is mandatory to have an internal information system.

² Article 6.1 e) GDPR.

6.3. DATA SUBJECT RIGHTS

Data subjects may exercise their rights regarding data protection. However, if the person referred to in the reported facts exercises their **right to object**, it will be presumed—unless proven otherwise—that there are compelling legitimate grounds justifying the processing of their personal data.

6.4. DATA ACCESS

Access to the data contained in the internal reporting system is strictly limited to the following individuals:

- The Information System Officer and any person directly managing it,
- The Human Resources Officer or the duly appointed competent body, **only when disciplinary action against an employee may be necessary**,
- The Legal Services Officer of the entity or organization, **if legal action related to the reported facts may be required**,
- Any data processors (if applicable for this procedure).

Access to the data by individuals other than those listed above will only be permitted when necessary for the implementation of corrective measures at PAP Tecnos or for the processing of disciplinary or criminal proceedings, where applicable

6.5. DATA MINIMIZATION

Personal data whose relevance is not required by the investigation will not be collected. In the event that personal data is collected by accident, it will be deleted without undue delay.

Under no circumstances will personal data that are not necessary for the knowledge and investigation of the actions or omissions be processed, proceeding, where appropriate, to their immediate deletion. Likewise, all personal data that may have been communicated and that refer to conduct that is not included in the scope of application of the law will be deleted.

6.6. SPECIALLY PROTECTED DATA

If the information received contains personal data included within the **special categories of data**, it will be immediately deleted, without registering and processing them.

6.7. DATA RETENTION

The data subject to processing may be retained in the reporting system only for the time strictly necessary to decide whether to initiate an investigation into the reported facts.

If it is proven that the information provided, or part of it, is untrue, it must be immediately deleted once this circumstance is known, unless the falsehood may constitute a criminal offense, in which case the information shall be retained for the necessary period while judicial proceedings are underway.

In any case, if **three months** have passed since the receipt of the report without initiating an investigation, the information must be deleted, unless the purpose of its retention is to preserve evidence of the system's operation.

Reports that are not pursued may only be kept in **anonymized** form, and the data blocking obligation under data protection regulations will not apply.

6.8. CONFIDENTIALITY

The identity of the people who report will not be revealed to third parties.

Internal or external information systems must not obtain data that allows the identification of the informant.

In addition, these systems must have adequate technical and organisational measures to preserve the identity and guarantee the confidentiality of the data corresponding to the affected persons and to any third party mentioned in the information provided, especially the identity of the informant if he or she has been identified.

The identity of the informant may only be communicated in the context of a criminal, disciplinary or sanctioning investigation to the judicial authority, the Public Prosecutor's Office or the competent administrative authority. In such cases, the whistleblower will be disclosed before his or her identity is revealed, unless such information would compromise the investigation or judicial proceedings.

6.9. RECORD OF PROCESSING ACTIVITIES

The processing of personal data carried out through the Internal Reporting System requires the creation of a record of processing activities. This record must contain, at a minimum:

- the purposes of the processing;
- a description of the categories of data subjects and the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations;
- where applicable, the transfers of personal data to a third country or an international organization, including suitable safeguards;
- where possible, the envisaged time limits for the erasure of the different categories of data;
- where possible, a general description of the technical and organizational security measures.

6.10. DATA PROTECTION RISK ANALYSIS.

The processing of personal data carried out through the Internal Information System requires an analysis of the threats to which you may be exposed in terms of data protection, through a data protection impact assessment

7. SANCTION REGIME

The performance of any conduct that goes against or does not comply with the provisions of this Procedure may have disciplinary consequences in accordance with the provisions of both the applicable collective agreement.

8. RECORDS

It is the responsibility of the following Individuals, during the time indicated, to control and archive the records of this document:

TITLE	RESPONSIBLE	RETENTION	LOCATION	CODE
Wisthelblowing Channel Procedure	Compliance Officer	5 años	Red	CMP.PO.01

The method of archiving quality system records is covered by procedure PG01 "Checking documented information".

9. ANNEXES

N/A