



# Internal Information System Protocol



# Contents

- I. Objective
- II. System Characteristics
- III. Material Scope of Application
- IV. Subjective Scope of Application
- V. System Manager
- VI. Internal Information Channel
- VII. Action Procedure
  - VII-I. Information Receipt and Registration Procedure
  - VII-II. Admission Procedure
  - VII- III. Investigation Procedure
  - VII- IV. Closure of Proceedings
- VIII. External Reporting Channel
- IX. Public Disclosure
- X. Protective Measures
  - X-I. Whistleblower Protection
  - X-II. Protection of Affected Persons
- XI. Personal Data Protection
- XII. Review and Update

## I. Objective

---

With the entry into force of Law 2/2023 of 20 February, governing the protection of persons who report regulatory infringements and the fight against corruption (hereinafter, the Whistleblower Protection Law), Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October on the protection of persons who report breaches of Union law (known as the Whistleblowing Directive) has been transposed into Spanish law. This represents a further step in fostering a culture of transparency and corporate compliance to prevent and detect threats to the public interest.

The new law regulates both the protection of individuals who, in a professional or work-related context, report irregular practices by public or private entities, and the requirements and safeguards that effective reporting mechanisms (whistleblowing channels) must meet.

TESET CAPITAL SGEIC, S.A. (hereinafter, "TESET CAPITAL" or "TESET") is committed to preventing legal breaches and has approved a Whistleblower Protection Policy and implemented this Internal Information System Protocol, in accordance with applicable regulations.

This Protocol provides individuals who act as whistleblowers within TESET CAPITAL with an internal channel to report irregular practices of which they become aware, ensuring at all times the protection of their rights and the safeguards established by law.

## II. System Characteristics

---

TESET CAPITAL adheres to the general principles relating to internal reporting systems and whistleblower protection as established in the Whistleblower Protection Law and has made the necessary provisions to ensure the following requirements are met:

- Establish a procedure for managing received reports.
- Allow whistleblowers to report information through secure and easily accessible channels.
- Guarantee the confidentiality of the identity of the whistleblower, any third parties named, and any proceedings carried out in connection with the report.
- Safeguard the rights of the person concerned, including the right to be informed of the allegations, the right to be heard at any time, the presumption of innocence, and the right to honour.
- Allow reports to be submitted in writing (via email or postal mail) or in person.
- Permit anonymous reporting.
- Provide information on external reporting channels to competent authorities and, where appropriate, to EU institutions, bodies, or agencies.

- Appoint a System Manager.
- Establish safeguards to protect whistleblowers.
- Immediately refer reports to the Public Prosecutor or the European Public Prosecutor's Office if they may constitute a criminal offence.
- Process personal data in accordance with applicable data protection regulations.

### III. Material Scope of Application

---

Any type of infringement may be reported through the Internal Information System, including:

- Acts or omissions that may constitute a breach of European Union law, specifically:
  - Those falling within the scope of the Union acts listed in the Annex to Directive (EU) 2019/1937, regardless of how such acts are classified under national law, including:
    - Public procurement.
    - Financial services, products and markets, and the prevention of money laundering and terrorist financing.
    - Product safety and compliance.
    - Transport safety.
    - Environmental protection.
    - Radiation protection and nuclear safety.
    - Food and feed safety, animal health and animal welfare.
    - Public health.
    - Consumer protection.
    - Protection of privacy and personal data, and security of networks and information systems.
  - Affect the financial interests of the European Union, as set out in Article 325 of the Treaty on the Functioning of the European Union (TFEU).
  - Impact the internal market, as provided in Article 26(2) of the TFEU, including breaches of European Union rules on competition and state aid, as well as infringements related to the internal market concerning acts that violate corporate tax rules or practices aimed at gaining a tax advantage that undermines the purpose or intent of the applicable corporate tax legislation.
- Serious or very serious criminal and administrative offences (including those causing harm to the Tax Authority and Social Security).
- Labour-related infringements concerning health and safety at work.

The following are expressly excluded from the scope of protection of this Protocol:

- Irregularities governed by their specific regulations under sectoral laws (including those falling within the scope of Part II of the Annex to Directive (EU) 2019/1937).

- Information that affects classified or secret data.
- Information related to complaints about interpersonal conflicts.
- Information obtained or accessed through the commission of a criminal offence.
- Information involving breaches of legal or medical professional secrecy.
- Information concerning the confidentiality of judicial deliberations.
- Information subject to confidentiality within the armed forces or law enforcement bodies.
- Information relating to irregularities in public procurement procedures.
- Disclosures concerning information already publicly available or mere rumours.

Additionally, TESET CAPITAL may use the Internal Information System to receive any other communications or information that could constitute a breach of applicable law, even if outside the scope of the Whistleblower Protection Law. However, in such cases, these communications and their senders will not be covered by the legal protections granted under that Law.

## IV. Subjective Scope of Application

---

This Protocol applies to all individuals who report to TESET CAPITAL information regarding infringements obtained in a work-related or professional context, specifically:

- Employees of TESET CAPITAL (including individuals whose professional relationship has ended, interns, trainees, scholarship holders, and volunteers).
- Individuals participating in recruitment processes or contractual negotiations with TESET CAPITAL.
- Self-employed individuals working for or under the supervision of TESET CAPITAL.
- Shareholders, partners, and members of the administrative, management, or supervisory bodies of TESET CAPITAL (including non-executive members).
- Any other person working for or under the direction and supervision of contractors, subcontractors, or suppliers of TESET CAPITAL.

Likewise, the internal information system and the protective measures provided therein extend to:

- Natural persons who, within the organisation where the whistleblower works, assist them in the reporting process.
- Natural persons related to the whistleblower who may suffer retaliation, such as colleagues or family members.
- Legal entities for which the whistleblower works, has any kind of professional relationship with, or in which they hold a significant interest.

## V. System Managers

---

TESET CAPITAL's Board of Directors has appointed Javier Zabala as the System Manager, responsible for ensuring the proper functioning of the internal information system. He shall carry out his duties independently and autonomously.

In the event that the System Manager is the subject of the reported information, and to avoid any potential conflict of interest, the report may be addressed to Ángel Escudero, who will assume the responsibilities of the System Manager solely for the purposes of handling that specific case.

The System Manager may be supported by various delegates within TESET CAPITAL in conducting investigations, all of whom shall also be bound to uphold the rights and protections afforded to whistleblowers.

## VI. Internal Information Channel

---

Information regarding the internal reporting channels is clearly and easily accessible on the TESET CAPITAL website ([www.tesetcapital.com](http://www.tesetcapital.com)).

The internal channels for receiving disclosures fully comply with the legal guarantees for whistleblower protection.

TESET CAPITAL has enabled the following internal reporting channels:

- By email sent to [canaletico@tesetcapital.com](mailto:canaletico@tesetcapital.com), which shall be the preferred channel for receiving disclosures.
- By postal mail, addressed to the attention of the System Manager, at TESET CAPITAL's offices located at C/ Monte Esquinza 35, 1st floor, 28010 Madrid.
- By in-person appearance before the System Manager, to be held within a maximum of seven days following a prior request for a face-to-face meeting, submitted via email or postal mail.

Such meetings shall be documented either through an audio recording, provided the whistleblower gives prior consent, or by means of a full written transcript, which the whistleblower may review and formally accept by signing.

Reports may be submitted either with identification or anonymously, and should include, as far as possible, the following information:

- Full name(s) of the individual(s) allegedly involved in the irregular conduct.
- Date of the events.
- Description of the irregular conduct being reported and/or any relevant information available.
- Documents or other forms of evidence supporting the reported misconduct.

When submitting the report, the whistleblower may indicate an address, email, or secure location for receiving notifications. If no such contact information is provided, or if the whistleblower explicitly waives this right, no follow-up communication will be made.

The maximum time frame for responding to the whistleblower regarding the outcome of the investigation is three months from the date of receipt of the report. In especially complex cases, this period may be extended by an additional three months, for a total maximum of six months.

## VII. Action Procedure

---

### VII-I. Information Receipt and Registration Procedure

Once the report has been received, and within no more than seven calendar days from the date of submission, an acknowledgment of receipt will be issued to the whistleblower—provided they have indicated a postal address, email address, or secure location for receiving communications.

If the report has been submitted anonymously, or if the whistleblower has explicitly waived the right to receive communications regarding the actions taken, no acknowledgment of receipt will be issued. Likewise, acknowledgment will not be provided if the System Manager reasonably considers that doing so could compromise the whistleblower's identity.

Along with the acknowledgment of receipt, the whistleblower will also be informed of their rights and the guarantees available to them during the course of the investigation.

Once the report is received, it will be recorded in a secure logbook, with access restricted to personnel designated by the System Manager, and assigned a unique identification code. The following details will be entered into the log:

- Date of receipt
- Identification code
- Whistleblower's contact details (if applicable)
- Reported facts
- Actions undertaken
- Measures adopted
- Date of closure

The data recorded in the log will not be made public and will be treated as confidential. However, access to the log may be granted to the competent judicial authority upon formal and reasoned request.

## VII-II. Admission Procedure

Once the information has been recorded, the System Manager will carry out a preliminary assessment to determine whether the content of the report falls within the scope of the Internal Information System.

To that end, the System Manager may contact the whistleblower to request clarifications or additional information or documentation.

Following the necessary checks, and within no more than ten days from the date of receipt, the System Manager will decide whether to reject the report, admit it for processing, or forward the information to the relevant public authority.

- Rejection of the report.

A report will be rejected if any of the following circumstances apply:

- The reported facts are entirely implausible.
- The reported facts do not constitute an infringement within the scope of the Internal Information System.
- The report is clearly unfounded or, in the opinion of the System Manager, there are reasonable indications that the information was obtained through the commission of a criminal offence. In this latter case, in addition to rejecting the report, a detailed account of the potentially criminal facts will be forwarded to the Public Prosecutor's Office.
- The report does not contain new and significant information compared to a previous report on which proceedings have already been concluded, unless there are new factual or legal circumstances justifying a different course of action. In such cases, the System Manager will notify the whistleblower of the decision with appropriate reasoning.

The decision to reject the report will be communicated to the whistleblower, unless the report was submitted anonymously or the whistleblower waived the right to receive communications.

- Admission of the report.

If the report is admitted for processing, this decision will also be communicated to the whistleblower, unless the report was anonymous or the whistleblower waived the right to receive updates.

- Referral to the Public Prosecutor's Office.

If the reported facts may reasonably be considered to constitute a criminal offence, the report will be forwarded immediately to the Public Prosecutor's Office or to the European Public Prosecutor's Office (if the case affects the financial interests of the European Union).

- Referral to the competent authority.

The report may also be forwarded to the relevant authority, body, or institution deemed competent to handle the matter.

## VIII. External Reporting Channel

---

In addition to TESET CAPITAL's internal reporting channel, any natural person may also use external reporting channels, either directly or after first submitting a report through the internal channel, to report irregularities to the Independent Whistleblower Protection Authority (A.A.I.), or to the relevant regional authorities or agencies:

- National Anti-Fraud Coordination Service  
<https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/Paginas/inicio.aspx>
- Public Prosecutor's Office against Corruption and Organised Crime  
<https://www.fiscal.es/>
- National Police  
[https://www.policia.es/\\_es/denuncias.php](https://www.policia.es/_es/denuncias.php)
- Spanish Court of Auditors  
<https://www.tcu.es/es>
- Ombudsman  
<https://www.defensordelpueblo.es/>
- European Court of Auditors  
[https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-court-auditors-eca\\_es](https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-court-auditors-eca_es)
- European Anti-Fraud Office (OLAF)  
[https://anti-fraud.ec.europa.eu/about-us/what-we-do\\_es](https://anti-fraud.ec.europa.eu/about-us/what-we-do_es)

As of the date of approval of this Protocol, the Independent Whistleblower Protection Authority (A.A.I.) has not yet been established. The Spanish Government has one year from the entry into force of the Whistleblower Protection Law to approve its statutes.

## IX. Public Disclosure

---

Public disclosure is understood as any act of making information about irregularities available to the public that falls within the scope of protection established by this Protocol and the Whistleblower Protection Law.

A person who makes a public disclosure is entitled to the same protections as those who report through internal or external reporting channels, provided that one of the following conditions is met:

- The individual previously reported the information through internal and external channels, or directly through external channels, and no appropriate measures were taken within the prescribed timeframe.
- The individual had reasonable grounds to believe that the infringement could constitute an imminent or manifest danger to the public interest—particularly in emergency situations or when there is a risk of irreversible damage, including danger to a person’s physical integrity—or, in the case of reporting through an external channel, that there was a risk of retaliation or little likelihood of the information being effectively addressed, due to particular circumstances of the case (such as concealment or destruction of evidence, collusion between authorities and the perpetrator, or the authority being involved in the wrongdoing).
- When the information has been disclosed directly to the press, based on the exercise of the constitutionally recognised right to freedom of expression and the right to receive truthful information, the above conditions for protection shall not be required.

## X. Protective Measures

---

### X-I. Protection of the Whistleblower

Individuals who report or disclose information that may be considered an infringement shall be entitled to protection, provided that:

- They had reasonable grounds to believe that the information reported or disclosed was true at the time of the communication or disclosure, even if they did not provide conclusive evidence, and that the information falls within the scope of this Protocol and the Whistleblower Protection Law.
- The communication or disclosure was made in accordance with the requirements set out in this Protocol and the Whistleblower Protection Law.

The same protection shall also apply to:

- Individuals who communicated or publicly disclosed information on actions or omissions anonymously but were later identified.
- Individuals who report breaches falling within the scope of Directive 2019/1937 to the relevant institutions, bodies, or agencies of the European Union.

Conversely, the following individuals are expressly excluded from protection:

- Those who submit or disclose information that has been rejected through any internal reporting channel for reasons including:
  - The reported facts are wholly implausible.
  - The facts do not constitute a breach within the scope of the Whistleblower Protection Law.

- The report is clearly unfounded or, in the opinion of the System Manager, shows signs of having been obtained through the commission of a crime.
- The report lacks new and relevant information compared to a previous case for which proceedings have concluded, unless there are new factual or legal circumstances justifying a different approach.
  - Individuals reporting interpersonal conflicts or information that only concerns the whistleblower and the persons named in the communication or disclosure.
  - Information already publicly available or which merely constitutes rumours.
  - Information relating to actions or omissions that fall outside the scope of this Protocol and the Whistleblower Protection Law.

### **Prohibition of Retaliation**

Retaliation is understood to mean any act or omission that is prohibited by law or that, directly or indirectly, results in unfavourable treatment placing the individual at a specific disadvantage in their professional or working environment, solely because they acted as a whistleblower or made a public disclosure.

TESET CAPITAL will adopt the necessary measures to expressly prohibit all acts of retaliation, including threats and attempts of retaliation, against individuals who submit a report—within two years from the conclusion of the investigation.

For the purposes of this Protocol, and by way of example, the following shall be considered acts of retaliation:

- Suspension of the employment contract, dismissal, or termination of the professional or statutory relationship, including the non-renewal or early termination of a temporary employment contract after the probation period, or the early termination or annulment of service or supply contracts.
- Imposition of any disciplinary action, demotion, denial of promotion, or any other substantial modification of working conditions.
- Failure to convert a temporary contract into a permanent one, where the employee had a legitimate expectation of such conversion—except where such measures are taken in the normal exercise of managerial authority under applicable labour or public service law, based on verified circumstances, facts, or violations unrelated to the whistleblower report.
- Damages, including reputational harm, financial loss, coercion, intimidation, harassment, or social isolation.
- Negative performance evaluations or professional references.
- Blacklisting or dissemination of information within a particular sector that hinders or prevents access to employment or contract opportunities.

- Denial or cancellation of a licence or permit.
- Denial of training opportunities.
- Discrimination, or unfair or unfavourable treatment.

Any person whose rights have been harmed as a result of their report or disclosure may, after the two-year protection period has elapsed, request protection from the competent authority, which may, exceptionally and with proper justification, extend the protection period.

Any acts that:

- Are intended to prevent or obstruct the submission of reports or disclosures, or
- Constitute retaliation or result in discrimination following such submissions, shall be deemed null and void by law and may lead to corrective disciplinary or liability measures, including compensation for any damages suffered by the affected party.

### **Support Measures**

Individuals who report or disclose information may have access to support measures provided by the Independent Whistleblower Protection Authority (A.A.I.) (or the relevant competent body), including:

- Full and independent information and advice, easily accessible to the public and free of charge, on the procedures and remedies available, protection against retaliation, and the rights of the affected person.
- Effective assistance from competent authorities in ensuring protection against retaliation.
- Legal assistance in criminal proceedings and in cross-border civil proceedings, in accordance with EU regulations.
- Financial and psychological support, on an exceptional basis, if so decided by the Independent Whistleblower Protection Authority (A.A.I.).

Likewise, individuals who report or disclose information may access free legal aid for representation and defence in legal proceedings arising from the submission of a report or public disclosure.

### **Protective Measures Against Retaliation**

TESET CAPITAL is committed to adopting the necessary measures to ensure whistleblowers are protected against retaliation:

- Individuals who report information or make a public disclosure shall not be considered to have breached any information disclosure restrictions, nor shall they incur any liability in relation to such communication or disclosure, provided they had reasonable grounds to believe that disclosure was necessary to reveal an irregularity.
- Whistleblowers shall not be held liable for acquiring or accessing the information that is reported or publicly disclosed, as long as such acquisition or access does not constitute a criminal offence.
- Any other potential liability arising from acts or omissions unrelated to the report or public disclosure, or not necessary to expose an infringement, shall remain subject to applicable law.
- In judicial or administrative proceedings concerning harm suffered by whistleblowers, once the whistleblower has reasonably demonstrated that they submitted a report or made a public disclosure and suffered harm as a result, it shall be presumed that the harm was caused as a form of retaliation. In such cases, the burden of proof shall lie with the person who took the harmful measure to demonstrate that it was based on duly justified grounds unrelated to the report or disclosure.
- In legal proceedings, including those involving defamation, copyright infringement, breach of secrecy, violation of data protection laws, disclosure of trade secrets, or compensation claims under labour or statutory law, whistleblowers shall not be held liable in any way as a result of protected reports or public disclosures. These individuals shall have the right to defend themselves by claiming, within the scope of such proceedings, that the communication or public disclosure was made with reasonable grounds and was necessary to expose a breach.

## **X-II. Protection of the Affected Person**

TESET CAPITAL guarantees the following protective measures for individuals affected by a report:

- The right to the preservation of their identity and the confidentiality of the facts and data involved in the proceedings.
- The right to be informed of the irregularities attributed to them.
- The right to the presumption of innocence.
- The right to be heard at any time.
- The right to defence, including the ability to submit statements and to be assisted by legal counsel.
- The right of access to the case file.
- The right to have their personal data processed in accordance with data protection regulations.

## XI. Personal Data Protection

---

The processing of personal data shall be governed by the provisions of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (hereinafter, GDPR), as well as the corresponding national regulations.

Any person submitting a report or making a public disclosure has the right to have their identity kept confidential. The identity of the whistleblower may only be disclosed to the judicial authority, the Public Prosecutor's Office, or the competent administrative authority in the context of a criminal, disciplinary, or sanctioning investigation.

Under no circumstances shall the identity of the whistleblower or of the person making a public disclosure be communicated to the person implicated in the reported facts.

Personal data that is not necessary for the understanding of the irregularities shall not be processed, and if such data is provided, it shall be deleted.

Personal data that is not clearly relevant for the processing of a specific report shall not be collected. If such data is collected accidentally, it must be deleted without undue delay.

Any data subject may exercise their rights of access, rectification, erasure, objection, restriction of processing, and/or data portability regarding their personal data by writing to the address of TESET CAPITAL, or by sending an email to [info@tesetcapital.com](mailto:info@tesetcapital.com). Likewise, they may file a complaint with the Spanish Data Protection Agency ([www.aepd.es](http://www.aepd.es)).

If the individual mentioned in the report or public disclosure exercises their right to object, it shall be presumed—unless proven otherwise—that there are compelling legitimate grounds justifying the processing of their personal data.

The legal bases for the processing of personal data are as follows:

- Internal reporting channel:
- Pursuant to Article 6.1(c) of the GDPR, when the internal reporting channel is mandatory (processing necessary for compliance with a legal obligation).
- Pursuant to Article 6.1(e) of the GDPR, when the internal reporting channel is not mandatory (processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority).
- External reporting channel: Pursuant to Article 6.1(e) of the GDPR.
- Public disclosure: Pursuant to Article 6.1(e) of the GDPR, when the internal reporting channel is not mandatory.

- Processing of Special Categories of Personal Data: Pursuant to Article 9.2(g) of the GDPR, the processing of special categories of personal data is lawful when it is necessary for reasons of substantial public interest, on the basis of Union or Member State law, provided that it is proportionate to the objective pursued, respects the essence of the right to data protection, and includes appropriate and specific measures to safeguard the data subject's fundamental rights and interests.

Personal data shall be retained only for the time strictly necessary to determine whether to initiate an investigation into the reported facts.

In any case, if no investigative actions are initiated within three months of receiving the report, the data must be deleted—unless its retention is necessary to maintain evidence of the system's proper functioning. Reports that are not pursued may only be stored in anonymised form.

If it is confirmed that the information provided—either in whole or in part—is false, it must be immediately deleted as soon as this is known, unless the inaccuracy may constitute a criminal offence, in which case the information shall be retained for the duration of the relevant legal proceedings.

In all cases, access to personal data contained in the internal reporting system will be strictly limited to those within the scope of their roles and responsibilities, specifically:

- The System Manager and any individuals directly responsible for managing the system.
- The Human Resources Manager or designated competent body, only where disciplinary measures may be applicable against an employee.
- The entity's legal services, where legal action may be appropriate in relation to the facts reported.
- Any data processors that may be formally designated.
- Where necessary to implement corrective measures within the organisation, or to process applicable disciplinary or criminal proceedings, it is lawful for the data to be accessed by other individuals or even disclosed to third parties.

## XII. Review and Update

---

This Protocol was approved by the Board of Directors of TESET CAPITAL at its meeting held on 30 September 2024 and entered into force on the same date.

The Protocol shall be reviewed, updated, approved, and disseminated on a regular basis and whenever it is deemed necessary to introduce any modifications.