

FAQ INTERNAL INFORMATION SYSTEM

WHISTLEBLOWING CHANNEL



What is the Whistleblowing Channel?

Telefónica's Whistleblowing Channel is integrated into the Telefónica Group's Internal Information System and constitutes the preferred mechanism for reporting matters related to or affecting the Group's activities or the performance of professional duties, referring to indications of irregularities, whether by action or omission, that could constitute:

- ✓ A criminal offense.
- ✓ A serious or very serious administrative infringement.
- ✓ A breach of the obligations established in the **Responsible Business Principles**.

The channel also allows the reporting of potential breaches of European Union law in connection with activities subject to that legal framework.



Who is responsible for the Whistleblowing Channel?

The Chief Compliance Officer is responsible for Telefónica's Internal Information System, which includes the Whistleblowing Channel.



Which regulations govern the Internal Information System?

The Internal Information System is governed by the Internal Information System Management Policy and its implementing regulations.

Additionally, some Group companies and jurisdictions have specific protocols (for example, regarding harassment) that regulate the handling of these investigations.



Who can use the Whistleblowing Channel?

The Whistleblowing Channel may be used by:

- Employees and former employees of Group companies
- Any third party maintaining a commercial and/or contractual relationship with Group companies
- Directors and officers of Group companies
- Suppliers and contractors
- Shareholders
- Volunteers
- Interns and trainees

What types of situations can be reported through the Whistleblowing Channel?



Workplace Harassment: systematic and recurring conduct that undermines an employee's dignity, creates a hostile environment, or seeks to damage their professional position. Occasional interpersonal conflicts are excluded.



Sexual Harassment: unwanted conduct of a sexual nature that creates an intimidating, hostile, or offensive work environment.



Discrimination: unfair treatment based on race, gender, religion, nationality, sexual orientation, disability, age, or other personal characteristics.



Inappropriate Conduct and Workplace Conflicts: abuse of power or mistreatment among employees, regardless of hierarchical relationship.



Working Conditions: situations that may pose a workplace risk to employees (for example, safety-related issues).



Information Confidentiality: improper use of company information or information belonging to its stakeholders for personal gain or the benefit of third parties.



Favoritism: granting unjustified advantages to certain individuals without a legitimate basis, thereby undermining equal treatment.



Conflict of Interest: situations in which personal interests influence or may influence professional decisions, including breaches of internal regulations.



Corruption of Public Officials: offering or providing benefits to public officials in order to obtain advantages.

What types of situations can be reported through the Whistleblowing Channel?



Private Sector Corruption: offering or accepting improper incentives in private business relationships.



Internal or External Fraud: a deliberate act against the company committed by employees, contractors, or suppliers, aimed at depriving it of property or money through deception or other dishonest means.



Internal Control over Financial Reporting: accounting irregularities or audit-related matters.



Legal or Regulatory Non-Compliance: any other breach of applicable laws or regulatory requirements.



Breach of Internal Regulations: failure to comply with internal rules or procedures of Group companies.



Failure to Meet Commitments to Customers: failure to fulfill obligations towards customers or engagement in improper practices.



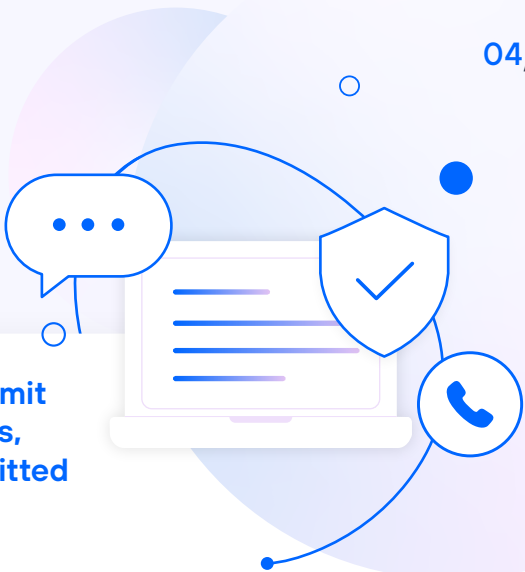
Competition Law Violations: anti-competitive agreements or abuse of a dominant market position.



Content-Related Conduct: breaches of responsible communication principles (for example, integrity or legality).



Other: cases that do not fall within any of the above categories.



Can I use the Whistleblowing Channel to submit commercial complaints (billing, service issues, customer service, etc.) or report fraud committed against customers by third parties (phishing, scams, etc.)?

NO. The Whistleblowing Channel is not the appropriate means for submitting commercial complaints or service-related issues (for example, billing or customer service matters), which should be addressed through customer service and commercial complaint channels.

It is also not the appropriate means for reporting crimes committed against customers by third parties (fraud, scams, identity theft, etc.), which must be reported through customer service channels.



How can I submit a report through the Whistleblowing Channel?

You can access the Whistleblowing Channel through any of the following means, all designed to ensure confidentiality and information security:



Web form available on [Telefónica's website](#) and on the intranet of any Group company.



Toll-free telephone lines ; in these cases, reports will be recorded and retained in accordance with applicable legislation (you may consult the telephone numbers in [Annex 1](#) of the Internal Information System Management Policy. For calls made from Spain, the designated number is [900107689](#))



Dedicated email addresses (you may consult the specific mailboxes listed in [Annex 1](#) of the Internal Information System Management Policy or write to canaldenuncias@telefonica.com).

If you wish, you may also submit information during an in-person meeting to be held within a maximum period of seven (7) calendar days from the date of the request, which may be made through any of the above-mentioned access channels.



Without prejudice to the use of the internal Whistleblowing Channel, you also have the right to report to any competent authority or body and, in particular, to the [Independent Authority for Whistleblower Protection](#) when the matter concerns a Spanish company.



Can I submit a report anonymously through the Whistleblowing Channel?

YES. The Whistleblowing Channel allows anonymous reports to be submitted.



What information should a report include?

There is no mandatory format for submitting a report. However, it is recommended that the communication include sufficient and detailed information to enable a proper assessment and investigation of the case:



Detailed description of the facts



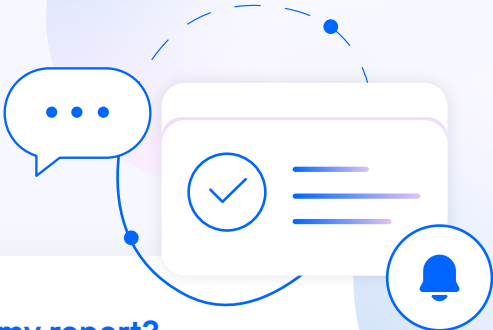
Individuals involved



Dates, locations, and context



Evidence or supporting documentation



Will I receive an acknowledgment of receipt for my report?

YES. An acknowledgment of receipt will be provided to the reporting person within a maximum of seven (7) calendar days. The system is currently configured to automatically provide the acknowledgment through the same channel used to submit the report:



Web form: a confirmation message will be displayed in the browser



Telephone: a recorded message will confirm successful registration



Email: the system will send an acknowledgment email



In-person report: the preferred means for receiving the acknowledgment will be requested



What happens after I submit a report through the Whistleblowing Channel?

The team responsible for managing reports will review the information provided. If the information is insufficient, clarifications may be requested from the reporting person, including in cases of anonymous reports.

A decision will then be made regarding whether the report will be accepted for review.



a) Rejection

A report may be rejected for any of the following reasons:

- The reported facts are clearly unfounded
- The report does not meet the required criteria or does not relate to internal regulations or applicable law
- The report does not contain new and significant information compared with a previous report for which the relevant procedures have already been completed, unless new circumstances justify a different approach.

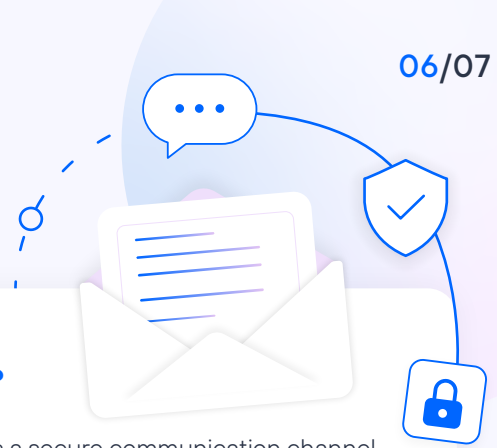


b) Acceptance

If the report is accepted for review:

- An Investigator will be appointed.
- An internal investigation will be initiated.
- The confidentiality and rights of all parties involved will be respected.

The report will be handled in accordance with Telefónica's internal policies and protocols, as well as the legislation applicable in each case. In Spain, investigations must be completed within a maximum period of three (3) months from the registration of the report, which may be extended by a further three (3) months in particularly complex cases. Compliance with data protection regulations is guaranteed throughout the process.



Can I follow up on the case, communicate with the investigation team, or provide additional information?

YES. Once a report is registered, the Channel automatically enables a secure communication channel that guarantees:

- The anonymity of the reporting person, if desired.
- The confidentiality of all shared information.
- The ability to track the status of the case.

Together with the acknowledgment of receipt, and through the same communication channel, you will receive an ID and password to access the secure platform. Please make sure to keep these credentials safe, as you will be required to change the password the first time you log in.



Am I required to report possible irregularities that I become aware of?

YES. Everyone working within the Telefónica Group has a duty to cooperate in preventing any person within the Group from acting improperly or lacking integrity, actively promoting the reporting of potential irregularities or non-compliance.



Are reports submitted through the Whistleblowing Channel confidential?

YES. The Internal Information System establishes specific measures to ensure the confidentiality of the identity of the reporting person and any third party mentioned in the report, as well as the confidentiality of all actions taken in processing and handling the report.

Reports are managed through secure channels to prevent unauthorized access, ensuring that only expressly authorized personnel may access the report and investigation information.

Furthermore, investigations are conducted while safeguarding the privacy and reputation of all individuals involved.



Am I protected against retaliation if I submit a report through the Whistleblowing Channel?

YES. Group companies, in accordance with applicable legislation, will not take nor tolerate any form of retaliation against individuals who report concerns in good faith.



What happens if I submit a false report?

The Whistleblowing Channel must be used responsibly and in good faith.

Telefónica may take disciplinary action against any employee who intentionally and in bad faith submits a false accusation or report for the purpose of harming another person.



What safeguards does the procedure provide?

The Internal Information System guarantees:

- Confidentiality and, where applicable, anonymity of reports.
- Protection against any form of retaliation.
- Appropriate handling and protection of personal data.
- Access to information regarding the status and progress of the case.
- Resolution within legally established timeframes.

Disclaimer

The Whistleblowing Channel is not an emergency service.

It should not be used to report situations that pose an imminent risk to life or property.

Communications submitted through this channel will not receive an immediate response.



Secure and Confidential Channel



Those who can use the whistleblowing channel



- Employees
- Former Employees
- Suppliers
- Shareholders
- Third Parties

Reporting Channels



Web



Intranet



Telephone



Email

Reportable Matters



Harassment



Discrimination



Fraud



Conflict of Interest



Corruption / Bribery



Accounting and Financial Information



Other Misconduct

How does the process work?

Follow-up

Acknowledgement of Receipt
Secure Channel

Resolution

Diligent Investigation
Legal Timeframes
Final Feedback



Confidentiality



Data Protection



No Retaliation

We are here to listen

