Group

BANKINTER

Whistleblower Channel Policy

March 2025

Content

1. Aim of the Policy 3

2. Scope 3

3. Roles and responsibilities 3

3.1. Board of Directors 4
3.2. Audit Committee 4
3.3. Internal Audit Division 4
3.4. Regulatory Compliance division 4
3.5. Crime Prevention and Professional Ethics Committee 5
3.6. Employees 5
3.7. Third parties 5

4. Reporting non-compliance 5

4.1. The importance of reporting non-compliance 5
4.2. When to report 5
4.3. How to report 6
4.4. What information should be included in the complaint 7

5. Procedure for managing and investigating complaints 8

6. Measures for the protection of whistleblowers and persons involved in the investigation 9

7. Communication and awareness raising 10

8. Non-compliance with this Policy 11

Appendix I – External reporting channels 12

1. Aim of the Policy

At the BANKINTER Group[1] we foster an environment of transparency, in which we can all express ourselves openly and respectfully. To this end, we have set up a confidential *Whistleblower Channel* through which we encourage you to report your concerns or suspicions about possible breaches of the *Code of Professional Ethics* or any other irregular conduct.

This Policy forms part of our internal control and compliance framework and offers the necessary guidance for reporting any concerns regarding potential misconduct, both confidentially and without fear of retaliation.

This Policy has been prepared pursuant to the relevant regulations:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).
- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, also known as the Whistleblower Protection Directive or the Whistleblower Directive.
- Protected Disclosures Act 2014 (as amended)

2. Scope

This Policy applies to the following users:

- All BANKINTER Group employees.
- Third parties, persons or organisations: (suppliers, subcontractors, customers, consultants, agents, temporary employment agencies, candidates for positions at the company, interns, etc.).

With this in mind, the *Bankinter Group Whistleblower Channel* is available to both the company's employees and third parties.

3. Roles and responsibilities

To ensure an effective procedure is in place for reporting suspected breaches and investigating complaints, the roles and responsibilities of the people who form part of the Bankinter Group must be well defined. It is important that you understand your role and responsibilities.

[1] Constituted by Bankinter, S.A. and its subsidiaries.

3.1. Board of Directors

The *Board of Directors* at the BANKINTER Group is ultimately responsible for the internal control system and delegates the daily operational functions of the control system to the Audit Committee, which in turn entrusts the management of the Whistleblower Channel to the Internal Audit Division.

The functions and responsibilities of the Board of Directors include the following:

- Promote a business culture structured around the principle of the "absolute rejection" of the commission of unlawful acts and fraud and encourage all employees at the organisation to act pursuant to the company's ethical principles as reflected in our *Code of Professional Ethics*.
- Set out the functions of the Audit Committee as the party responsible for the management and investigation of complaints received via the *Whistleblower Channel*.

3.2. Audit Committee

The Audit Committee is a body that reports to the Board of Directors, which in turn delegates the management and supervision functions in relation to the Bankinter Whistleblower Channel to the Audit Division.

The functions and responsibilities of the Audit Committee are the following:

- Ensure that a business culture is pursued structured around the principle of the "absolute rejection" of the commission of unlawful acts and fraudulent situations.
- Supervise the confidential reporting procedure and ensure its effectiveness.
- Decide on how to proceed as regards particularly important complaints referred by the Internal Audit Division.
- Report annually to the Board of Directors on the activity of the Whistleblower Channel.

3.3. Internal Audit Division

The *Internal Audit Division* is a body that reports to the *Board of Directors* of the Bankinter Group and is responsible for managing the Whistleblower Channel. Its main functions are:

- Evaluate and analyse the complaints received and, where appropriate, inform the *Board of Directors*, via the Audit Committee, of any particularly important complaints.
- Coordinate the investigation of complaints received and suggest any measures deemed necessary, processing these accordingly.
- Provide advice on issues arising as part of the application of the organisation's codes and policies, pursuant to the applicable legislation in each case.
- Maintain an updated Record of complaints received and internal investigations undertaken, guaranteeing, in all cases, the confidentiality requirements provided for by law.
- Guarantee the confidentiality of the reports received, the whistle-blower's personal data, and the information provided.

3.4. Regulatory Compliance division

In the event that the complaint is in relation to the Internal Audit Division, the Regulatory Compliance Department will request its abstention and will assume the responsibilities of the Internal Audit Division when it comes to handling complaints. To this end, the Regulatory Compliance Division will designate the area(s) and person(s) to carry out the investigation of the reported facts, depending on the nature of the report, and the designated area(s) and person(s) will carry out their task under the exclusive direction and instructions of the head of Control and Compliance.

3.5. Crime Prevention and Professional Ethics Committee

If, once the investigation of the complaint has been performed, it is found that an employee or agent has participated in irregular conduct, the area in charge of the investigation will inform the Crime Prevention and Professional Ethics Committee, which will decide whether it is appropriate to take disciplinary measures against those involved or even inform the relevant authorities if necessary.

3.6. Employees

All BANKINTER Group employees must act in accordance with the organisation's ethical principles and, to this end, they are required to report any suspicious and/or irregular action or circumstance that may be in breach of the applicable legislation, the *Code of Professional Ethics* and the organisation's framework of rules and values.

3.7. Third parties

The BANKINTER Group is particularly committed to a culture of ethics and regulatory compliance. To this end, BANKINTER Group's *Whistleblower Channel* is available for third parties from outside the organisation to report potential breaches detected as part of their collaboration with Bankinter Group employees.

4. Reporting non-compliance

4.1. The importance of reporting non-compliance

At BANKINTER Group, we seek to instil trust in our employees and third parties by maintaining the highest ethical standards, acting with integrity in everything we do. Our reputation is critical to our success and capacity to operate both today and in the future.

We are prepared to respond appropriately to situations of potential non-compliance or irregular conduct, thus complying with the company's ethical values.

If you observe and/or are concerned about any suspicious conduct that may constitute a breach of our *Code of Professional Ethics*, you are required to report this via the *Whistleblower Channel*.

We encourage you to report in good faith any irregular conduct based on a reasonable suspicion.

Making false accusations in bad faith against other Bankinter Group employees or third parties will be considered a very serious breach and may lead to disciplinary measures.

4.2. When to report

We encourage our employees and third parties to report any non-compliance or suspicious conduct as soon as they become aware of it and, insofar as possible, before any damage occurs. To this end, workers and third parties must use one of the channels referred to in *Section 4.3 below (How to report)*.

A non-exhaustive list of potential suspicious and/or irregular conduct that can be reported using the *Whistleblower Channel* is as follows:

• Fraud. • Breaches of the Code of Professional Ethics.	• Data protection breaches. • Disclosure of confidential information.

• Non-compliance with laws and regulations (internal and external). • Anti-competitive practices. • Conflicts of interest. • Irregular payments. • Inappropriate use of the organisation's assets.	• Retaliation against anybody using the *Whistleblower Channel* in good faith. • Workplace Harassment • Sexual Harassment • Any type of discrimination, whether based on sexual orientation or any other reason • Health and safety • Damage to the environment

You may have other concerns or worries that cannot be reported using the *Whistleblower Channel* and that must be dealt with using other channels, in particular:

- Any issue involving collective bargaining or consultation of trade unions.
- Complaints from customers/users.
- Complaints related to the functioning of the Group's websites/apps.
- Complaints in relation to training and professional development.

In any case, to maintain an appropriate culture of compliance, at the BANKINTER Group, we encourage raising queries in relation to the company's internal control and compliance framework, as well as any concerns that our employees and third parties may have in relation to the *Code of Professional Ethics*. To this end, if you have any questions regarding the application of the internal regulatory framework, you can also use the channels provided to this end (*see Section 4.3 How to report*).

4.3. How to report

At BANKINTER Group, we have enabled the following reporting mechanisms that together make up the *Whistleblower Channel*. Reports may be made in writing or verbally, either by completing the questionnaire available via the Channel, by voice message or in the form of a face-to-face meeting.

If the complaint is made via voice message or in-person, the complaint will be documented, with the consent of the whistleblower, in the form of a report.

4.3.1. Digital whistleblower platform

The *Digital whistleblower platform* enabled by BANKINTER Group allows suspicious conduct to be communicated in writing, by filling in the corresponding form, as well as verbally in the form of a voice message that can be recorded and sent. In the latter case, the voice will be distorted in such a way that it will not be possible to determine the identity of whistleblowers who wish to remain anonymous, thus protecting their identity.

The *Digital whistleblower platform* has been designed in such a way to meet the highest standards as regards data protection and information confidentiality.

When making a report on the Digital Whistleblower Platform, the complainant has the option of providing their contact details or remaining anonymous. However, BANKINTER Group has a report management procedure in place to ensure that only the persons strictly necessary have access to the contents of reports.

The *Digital whistleblowing platform* can be accessed on the BANKINTER Group's website: *https://grupobankinter.integrityline.app/*

4.3.2. Verbal reports

The complainant has the option, if they so wish, to report the potential facts constituting irregular practices and/or non-compliance verbally by requesting a face-to-face meeting or over the phone with the Internal Audit Division. The Internal Audit Division must hold a face-to-face meeting or phone call within a maximum period of seven days from the complainant's request. If the complainant so wishes, they may contact BANKINTER Group by post at the following address: Avenida Bruselas 12, post code: 28108, Alcobendas, (Madrid). This email must be sent FAO the Internal Audit Division in general or the Regulatory Compliance Division, for complaints related to the Internal Audit Division.

In these cases, the content of the complaint, with the consent of the complainant, will be recorded in the form of a report.

4.3.3. External reporting channels

We encourage you to raise your concerns using BANKINTER Group's *Whistleblower Channel*. By reporting it internally, you offer us the opportunity to investigate the matter, take action if necessary and appropriately manage any potential repercussions.

However, if you prefer to use an external reporting mechanism, as an alternative to our *Whistleblower Channel*, you can contact the Independent Whistleblower Protection Authority or the corresponding authorities, regional bodies or organisations to inform them of any suspicions or irregular conduct you have witnessed[2].

4.4. What information should be included in the complaint

To adequately assess the complaint made, we encourage you to provide at least the following information:

- Any background information that helps us to obtain context in relation to the facts and circumstances reported
- The reasoning behind your decision to report.
- The details of the complaint (detailed explanation of the circumstances, dates, amounts, people and departments involved and any other information you consider relevant).
- If available, documentation that supports or corroborates the data provided.

If you wish, you can provide your contact information (name, phone number and e-mail address) or remain anonymous. In any case, our whistleblower platform allows for information to be exchanged and communications with the whistleblower to be maintained. We therefore ask that the whistleblower remain alert to any communication that they may receive after filing the complaint to clarify any matter that the manager of the whistleblower channel or the investigation team may require.

When filing a complaint, generally speaking, we will process complaints that:

- Contain congruent and consistent facts or actions.
- Offer objective or reasonably verifiable data that could be obtained as part of an investigation.

All personal information will be processed confidentially and consistent with the prevailing legislation on personal data protection, pursuant to the legal information provided in this policy.

For the sake of clarity, the following cases cannot be handled via this Confidential Whistleblower Channel, as stipulated in the corresponding law:

a. Information related to claims on interpersonal conflicts, unless they constitute a breach of any employment provision in the Code of Ethics.
b. Information that is already fully available to the public or that is mere rumour.
c. When the facts reported lack credibility or are manifestly unfounded or there are reasons to believe that they were obtained through the commission of a crime.

[2] See Appendix I.

d. Where the communication does not contain new and significant information concerning breaches compared to a previous communication for which the relevant procedures have been concluded, unless new factual or legal circumstances arise which justify a different approach.

5. Procedure for managing and investigating complaints

At BANKINTER Group, we take all reports of possible suspicions and/or irregular conduct very seriously. We have procedures in place for managing and investigating complaints that aim to provide transparency in how we assess, analyse and investigate communications received via the *Whistleblower Channel*.

Terms

If you report a possible suspicion and/or irregular conduct via our *Whistleblower Channel*, within the following seven (7) calendar days, you will receive confirmation of receipt of your report, unless this may compromise its confidentiality.

We will conduct a preliminary assessment of the complaint and, if necessary, an internal investigation. The deadline for performing investigations is three (3) months, although, in the case of particularly complex investigations, this deadline may be extended by a further three (3) months.

If you did not receive acknowledgement of receipt, the three-month period will begin from the end of the seven-day period once the report was filed.

Preliminary assessment

Upon receipt of the complaint, BANKINTER Group may contact you and request additional information. In any case, the presumption of innocence and the honour of the persons affected will be respected.

BANKINTER Group will analyse the report received to determine whether:

- The suspicion consists of irregular conduct that must be reviewed in depth and, if appropriate, investigated; or
- The reported facts are not subject to this Policy.

Internal investigation

The Internal Audit Division is the unit responsible for performing internal investigations into reported incidents. If a member of the Internal Audit Division is named in the reported incident, they will be removed from the case to ensure objectivity. If all members of the Internal Audit Division are named in the reported incident, the complaint will be assessed and managed by the Regulatory Compliance Division and the investigation may be outsourced to an external third party.

The investigation will entail an objective analysis of the complaint and will be conducted in a strictly confidential manner. If necessary, we may involve external experts such as specialist investigators, legal advisors, etc., to support the investigation. Details of the case, your identity and the identity of any other person mentioned will remain confidential during and after the investigation.

The identity of the complainant may only be communicated to the court authority, the Public Prosecutor's Office or the competent administrative authority within the framework of a criminal, disciplinary or sanctioning investigation, in full compliance with the legal provisions in this area.

To this end, BANKINTER Group guarantees the protection of those who report irregular practices provided that the following requirements are met:

- There are reasonable grounds to believe that the information provided is true, despite the lack of conclusive evidence.
- The report has been made pursuant to the provisions of the current regulations.

The person named in the report has the right to be informed of the actions or omissions attributed to them and to provide a response before the case is resolved. They shall be informed at the time and in the manner considered appropriate to ensure the successful completion of the investigation.

If you are involved in or are aware of an internal investigation, you must keep the matter confidential; otherwise you may interfere in its investigation. Disclosing information relating to internal investigations will be considered a very serious offence and may lead to disciplinary measures.

Decision making

The Internal Audit Division will take one of the following decisions in relation to the complaint received:

- If it is identified that irregular conduct has indeed occurred , the Crime Prevention and Professional Ethics Committee will be informed, which will decide whether disciplinary measures should be taken against those involved or even inform the relevant authorities if necessary.
- If, having assessed and/or investigated the complaint, it is concluded that there has been no breach or irregular conduct and/or there is insufficient information, the case will be closed and the decision will be documented.

Reports to the Audit Committee and Board of Directors

The Internal Audit Division must regularly inform the *Audit Committee* and the *Board of Directors* at the Bankinter Group about the number and status of communications received, as well as their resolutions, including possible action plans.

6. Measures for the protection of whistleblowers and persons involved in the investigation

BANKINTER Group wants all its employees and third parties to feel confident in reporting any potential non-compliance or irregular conduct witnessed.

To this end, the whistleblower channels enabled by BANKINTER Group have been designed and implemented following specific measures to protect the identity of complainants and any other third party mentioned in the communication made, as well as the actions performed as part of the management and processing of complaints, with special attention paid to confidentiality and data protection, preventing access by unauthorised personnel.

The main characteristics and general principles of operation of the *Whistleblower Channel* at BANKINTER Group are:

Confidentiality

It guarantees the confidentiality of the data included in complaints, with a particular focus on those relating to the identity of the complainant and any other third party mentioned in the communication.

To this end, the person named in the complaint will not be able to access the details of the complainant, or any other person who could be involved in the notifications. The right of access is therefore limited to their own personal data.

However, the person named in the report may know the identity of the whistleblower in the cases provided for by law or when the latter expressly consents to this if needed as part of the internal investigation.

In turn, the complainant has the duty to provide the data and documents available to them in relation to the incident reported and the duty not to communicate the identity of the person named in the report by any means other than those provided for by law.

Absence of retaliation

It guarantees that there is no retaliation or any type of negative consequences for the whistleblower, provided that they act in good faith.

In this regard, whistleblowers will be protected against any type of extortion, discrimination or penalisation for the complaints made, notwithstanding the adoption of disciplinary measures deemed appropriate in the event of false complaints or complaints made in bad faith.

It should be noted that complaints made in bad faith may give rise to disciplinary measures and/or sanctions that may be applicable against the complainant.

Proportionality

All notifications received are treated rigorously and equally, regardless of who sent them or those named in the complaint.

Decision making

Decisions regarding how to conduct an investigation or when to dismiss notifications are made in a planned and traceable (documented) manner as provided in the legislation and internal procedures for handling and investigating complaints.

Terms

There is a protocol that guarantees compliance with the deadlines established in the applicable legislation, depending on the different scopes of communication.

BANKINTER Group has a maximum of three months[3] from receipt of the complaint to respond to the investigation actions. If the complainant did not receive acknowledgement of receipt, the three-month period will begin from the end of the seven-day period once the report was filed.

Data protection

The personal data included in notifications are processed pursuant to the data protection clause signed at the time of filing the complaint.

Rights of the complainant, the defendant and third parties mentioned in notifications

There are protocols in place to ensure that the rights of the whistleblower and the defendant are respected at all times.

In cases where the defendant or other persons known to have been involved in irregular actions, Bankinter must allow them to provide a defence before taking any disciplinary action.

In addition, on a regular basis, Bankinter Group will review the functioning of the whistleblower channels with the aim, where appropriate, of identifying potential areas for improvement in their operating and management mechanisms.

7. Communication and awareness raising

[3] This period may be extended by three (3) months in the case of particularly complex investigations (See *Section 5. Procedure for managing and investigating complaints*).

BANKINTER Group is responsible for communicating and disseminating the contents of this *Policy* with the aim of creating a culture of total transparency in which potential users are not afraid to report any type of possible suspicious conduct, as well as ensuring that appropriate measures and processes are implemented to ensure compliance.

To ensure the maximum effectiveness of the whistleblowing channel, it is the duty of the Communication, Brand and Sustainability department, on the request of the Internal Audit division, to give it sufficient publicity on Bankinter Group's intranet

8. Non-compliance with this Policy

Any non-compliance with this *Policy* will be investigated and may result in disciplinary action being taken.

Appendix I – External reporting channels

The whistleblower may use the following external reporting channels to report suspicious and/or unusual conduct:

- Irish Office of the Protected Disclosures Commission (OPDC)

  https://www.opdc.ie/en/

- The Central Bank of Ireland (CBI)

  https://www.centralbank.ie/regulation/protected-disclosures-whistleblowing

- Irish data Protection Commission (DPC)

  https://www.dataprotection.ie/en/who-we-are/corporate-governance/making-protected-disclosure-dpc

- Irish Competition and Consumer Protection Commission (CCPC)

  https://www.ccpc.ie/business/about/governance/protected-disclosures-annual-reports/#:~:text=In%20order%20to%20make%20a,relevant%20wrongdoing%20relates%20to%20matters

- Irish The Companies Registration Office (CRO)

  https://www.cro.ie/

- The Intellectual Property Office of Ireland (IPOI)

  https://www.ipoi.gov.ie/en/about-us/protected-disclosures-act-2014/

- The Irish Auditing and Accounting Supervisory Authority

  https://iaasa.ie/wp-content/uploads/2022/11/Protected-Disclosures-External-Policy-December-2016.pdf

- The Irish Takeover Panel

  http://irishtakeoverpanel.ie/

- The National Standards Authority of Ireland

  https://www.nsai.ie/

- Irish Office of the Comptroller and Auditor General

  https://www.audit.gov.ie/en/disclosures/protected-disclosures.html

- Irish Office of the Revenue Commissioners

  https://www.revenue.ie/en/corporate/statutory-obligations/protected-disclosures/index.aspx

- Irish Commission for Communications Regulation (ComReg)

  https://www.comreg.ie/about/foi-aie-info/protected-disclosures/

VERSION HISTORY

Version	Date	Prepared/modified by:	Approval
1.0	24th March 2025	Internal Audit	Audit Committee