PROCEDURE FOR THE MANAGEMENT OF THE INTERNAL INFORMATION SYSTEM AND DEFENCE OF THE WHISTLEBLOWER

ARESBANK S.A.

HISTORY OF REVISIONS CARRIED OUT

VERSION	DATE	ELABORATE	APPROVED	REVISION
V.1	21/03/2019	Legal Counsel & Compliance	OCI	Approval of the Procedure.
V.2	08/11/2022	Compliance	Board of Directors	Any labour sanction imposed by Aresbank that is motivated by or related to a previous complaint by the employee or manager is null and void. The minimum content of the information to be reported is included. The recipients of the complaints are modified, depending on the subject. The confidentiality measures applied are included.
V.3	19/09/2023	Global Risk Management. Regulatory Compliance Area	Board of Directors	Adaptation of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory and anti-corruption infringements.
V.4	24/05/2024	Global Risk Management. Regulatory Compliance Area	Board of Directors	Revision of the Internal Information System Management Procedure

INDEX

I. INTRODUCTION 3
II. SUBJECTIVE SCOPE 3
III. OBJETIVE SCOPE OF APPLICATION 4
IV. MEANS FOR THE PRESENTATION OF COMMUNICATIONS 4
V. COMPETENCIES AND RESPONSABILITIES 6
VI. PROCESSING OF COMPLAINTS 8
5.1. Reception and Registration 8
5.2. Admission to processing 9
5.2.1. Preliminary analysis. Admission or inadmissibility for processing 9
5.2.2. Information to affected parties 9
5.3. Investigation of the facts denounced 10
VII. CONFLICT OF INTEREST MANAGEMNET 13
VIII. CONFIDENTIALITY AND PROTECTION OF `PERSONAL DATA 14
IX. APPROVAL, REVIEW AND UPDATE OF THE PROCEDURE 16
ANNEX I. CATALOGUE OF INFRINGEMENTS REFERRED TO IN DIRECTIVE (UE) 2019/1937 17
ANNEX II: MAIN EXTERNAL CHANNELS FOR COMMUNICATIONS SET OUT IN ARTICLE 2 OF LAW 2/2023 18
ANNEX III. PROTOCOL PROHIBITING RETALIATION 19

I. INTRODUCTION

Article 9 of Law 2/2023, of February 20, 2023, regulating the protection of persons who report regulatory and anti-corruption breaches, establishes the duty of entities to approve an Information Management Procedure.

Thus, the Board of Directors approves this Procedure for the management of the Internal Information System and the defence of the Whistleblower (hereinafter, the "**Procedure**"), which establishes the necessary provisions for the management and processing of communications received through the Internal Information System of Aresbank, S.A. (hereinafter, "Aresbank"), as a mechanism for communication and reporting of irregularities.

II. SUBJECTIVE SCOPE

The people who can carry out communications through the Internal Information System are those who fall within the following groups:

- Employees.
- Managers.
- Shareholders.
- Members of Aresbank's administrative, management and supervisory bodies.
- Interns.
- Staff in training.
- Temporary employment agency workers.
- Candidates who are in a selection process.
- Legal representative of workers.

All of them, hereinafter, the "**Staff**" of Aresbank. In any case, it is recalled that it is mandatory to report in case of detecting possible risks and non-compliances.

The following may also make communications:

- Contractors, subcontractors and suppliers.
- Any person working for or under the supervision and direction of contractors, subcontractors, and suppliers.
- Former employees.
- Any other person who has been in the process of belonging to any of the above groups or has belonged to them in the past.

Hereinafter, all of them, "**Third Parties**".

III. OBJETIVE SCOPE OF APPLICATION

In accordance with the Policy of the Internal Information System and the Defense of the Whistleblower (hereinafter, the "**Policy**" or "**Policy of the Internal Information System**"), Personnel and Third Parties may report knowledge or motivated suspicion of irregular conduct related to the following matters:

- Any infringement of the principles set out in the Code of Conduct;
- Breaches Aresbank's Criminal Risk Prevention Model or any internal standard on ethics and compliance;
- Infringements of European Union law included in the material scope of application of 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, and the Spanish Law transposing it (see details in Annex I);
- Facts or Conducts that may have criminal significance;
- Serious or very serious administrative offences;
- Infringements of labour law in the field of occupational safety and health.

Annex II of this Policy includes some examples of events that can be reported through the Internal Information System.

❖ For guidance purposes and not limitation, you should NOT communicate through the Whistleblowing Channel:

- General information related to the company;
- Issues for which there is a specific channel (transparency, customer service, etc.).);
- Information that is already fully available to the public or that is mere rumor;
- Matters relating to interpersonal matters that do not involve infringement and/or that are part of the strictly personal and private sphere between individuals.

IV. MEANS FOR THE PRESENTATION OF COMMUNICATIONS

At Aresbank we have multiple channels of communication with Staff and Third Parties to foster a culture of dialogue as a basic element of our Internal Information System.

The following is a description of the channels available to Aresbank for reporting complaints and/or queries:

- **Whistleblowing Channel:** Online platform provided by a specialized technology company and accessible through the website https://aresbank.es/es/cumplimiento.html in the Compliance section,

separate and easily accessible. The platform has measures in place to preserve the security and integrity of information and the processing of personal data. The Whistleblowing Channel allows communications to be made orally or in writing, even anonymously. Communications relating to sexual and/or gender-based harassment may be reported through the Whistleblowing Channel.

- **Face-to-face meeting:** Through the Whistleblowing Channel, the Whistleblower may request a face-to-face meeting to verbally communicate the facts to be reported. In these cases, the communication will be recorded and you will be informed of the processing of your data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
- **Mail**: by post to Paseo de la Castellana, 257, 28046 MADRID (Spain) to the attention of the Chief Risk and Compliance Officer as Head of the Internal Information System (hereinafter, "**System Manager**") of the entity.

Likewise, information will be provided on the Aresbank website, in a clear and accessible way, on the external channels for reporting to the competent authorities and, where appropriate, to the institutions, bodies or agencies of the European Union.

The Customer Service or the Complaints Service of Aresbank's Supervisors do not constitute channels for reporting irregularities. In the event of receiving any communication that is included in the objective scope of the Whistleblowing Channel, the reporting person will be redirected to the Whistleblowing Channel.

The filing of the complaint must comply with the following formal requirements:

- Identity of the informant and email address, all this in the event that the complaint is not anonymous.
- Reason for the complaint: Detailed description of the facts or circumstances that, in the opinion of the informant, constitute a breach or irregularity.
- Possible people involved (if known): name and surname, as well as any other information that is known and considered relevant for the identification of the alleged offender.
- If applicable, concrete evidence to support the complaint: all documents available that support the belief that the irregularity described in the reason for the complaint has been committed.
- Place and date.
- Acceptance of the Principles and Guarantees of the Aresbank Whistleblowing Channel.

Likewise, the following material requirements must be met:

- Be carried out in good faith and deal with true facts, without prejudice to the inaccuracy or omission that may be committed involuntarily by the informant.

- Dealing with facts included within the scope of application of the Whistleblowing Channel.
- Be presented by Staff and/or Third Parties.

V. COMPETENCIES AND RESPONSABILITIES

Board of Directors

Aresbank's Board of Directors is responsible for **approving and supervising** all policies that include the general administration of the entity and the risk management inherent to the activity carried out by Aresbank. In this way, it is also responsible for **ensuring the correct implementation and management of the Internal Information System.**

In this regard, the Board of Directors, at the proposal of the Compliance Committee, is responsible **for approving the Internal Information System Policy**, as well as monitoring **and promoting** actions aimed at resolving the deficiencies detected.

In the same way, the Board of Directors is also responsible for appointing **the person responsible for the management of the Internal Information System**, as well as for his or her dismissal or dismissal, and for providing him with the personnel and material resources necessary for the proper performance of his or her duties.

The Board of Directors, through the Compliance Committee, will be **periodically informed of the activity carried out in the Internal Information System**, as well as of any possible deficiencies found in its operation.

Responsible for the Internal Information System

The Board of Directors has appointed the person who holds the position of **Chief Risk and Compliance Officer** of Aresbank as Head of the Internal Information System (hereinafter, "*System Manager*"), insofar as this position is a managerial position that exercises its functions independently and autonomously with respect to the rest of the entity's bodies and does not receive instructions of any kind in its exercise.

On the other hand, the Head of the Internal Information System is equipped with all the personal and material resources to carry out his/her functions in an appropriate manner.

The powers and responsibilities attributed to this figure are detailed below:

- It is the responsibility of the Head of the Internal Information System **ensure the confidentiality of the identity of the person** who makes use of the Whistleblowing Channel and chooses to identify himself. The identity of the identified Informant will not be disclosed to the Respondent without his or her consent, without prejudice to the provisions of the previous section.

- The System Manager will try to maintain **a secure channel of communication with the Informant**, using the tool of the Whistleblowing Channel or any other means that may be enabled for this purpose according to the circumstances.
- The System Manager shall ensure that the **processing, investigation and resolution** of communications is carried out in accordance with the legislation and principles of the Policy, acting with full independence and impartiality.
- The System Manager **shall periodically report to the Board of Directors**, at least annually and whenever necessary, as much information as may be required on the activity of the System, preserving in any case the confidentiality and security of the information, as well as the other guarantees and rights of users established in the Policy.
- The System Manager will keep the **Record Book updated** with the information of the communications received.
- Act as **an interlocutor**, on behalf of Aresbank, with the Independent Whistleblower Protection Authority.
- **Adopt the decision to outsource part of the management process to external experts** when reasons of complexity, objectivity and the preservation of confidentiality and anonymity so advise.

Both the appointment and the dismissal of the Head of the Internal Information System must be notified to the Independent Authority for the Protection of Whistleblowers, in accordance with the legally established procedure, specifying, in the case of their dismissal, the reasons that have justified it.

Regulatory Compliance Function

The Regulatory Compliance function, within the Global Risk Control Department, is responsible for coordinating the management of the Internal Information System, reporting in all cases to the System Manager.

In the performance of this function, Regulatory Compliance may require the collaboration of other key persons in the organization when the nature of the communication makes it advisable for operational or specialization reasons.

In addition, the Regulatory Compliance function will be responsible for the performance of the following functions:

- **Periodically review the Internal Information System Procedure and Policy.**
- **Assist the System Manager in the processing, instruction and resolution** of communications received through the Internal Information System.
- **Publication, promotion and awareness-raising** within the organization of the Internal Information System.

- **Resolution of doubts and queries** that may arise within the framework of the Internal Information System.
- **Periodically report to the Compliance Committee** on the activity carried out in the Internal Information System.

Internal Audit

The Internal Audit Department is responsible for the periodic review, on a triennial basis, of the proper functioning and management of the Internal Information System.

Legal Department

In cases in which the analysis carried out concludes that there are facts that show indications of constituting a crime, the Legal Department will be responsible for immediately forwarding the information to the Public Prosecutor's Office or the European Public Prosecutor's Office, in the event that the facts affect the financial interests of the European Union.

Employees

All Aresbank employees, including members of the General Management and the Board of Directors, are obliged to report through the Internal Information System any alleged action or omission that is within the scope of this Policy.

VI. PROCESSING OF COMPLAINTS

5.1. Reception and Registration

Once the communication has been received, regardless of the means used, it will be registered in the Whistleblowing Channel, in such a way that the communication will be recorded in the tool in a secure way and with restricted access to the people authorized to do so. The tool will record and update all reports received, date of receipt, identification code, status and measures taken.

Within a maximum of **seven calendar days** following receipt of the communication, Aresbank shall send acknowledgement of receipt to the Informant, unless this could jeopardize the confidentiality of the communication. Without prejudice to the foregoing, the Informant may waive, if he/she so wishes, his/her right to receive notifications in the framework of the processing.

In the event that any information is received by means other than those established in the Internal Information System, Aresbank will guarantee confidentiality and, as far as possible, that its treatment is in accordance with the provisions of this Procedure.

Specialities of verbal complaints

Aresbank offers the Informant the possibility of formulating, ratifying, expanding or clarifying the complaint in a face-to-face meeting within a maximum period of seven (7) days from the receipt of their communication.

If the Respondent agrees to hold such a face-to-face meeting, the System Officer shall document the report by recording it (if the Reporting Party gives its consent)

or by means of a complete and accurate transcript of the conversation. At this meeting:

- The Informant may be accompanied, if he so wishes, by a lawyer or a workers' representative.
- In order to ensure the proper confidentiality of the investigation, those who attend this meeting will be informed by the System Manager, in writing, of their duty of secrecy and confidentiality, as well as of all legal information on data protection.
- The transcript will be signed by those present at the meeting. If, for any reason, the Informant or any of those present do not wish to sign the report, it will be recorded as such and the investigation will continue.

Finally, the System Manager will attach the recording or transcript of the conversation to the Whistleblowing Channel application and will continue the investigation file in accordance with the provisions of the following sections.

5.2. Admission to processing

5.2.1. Preliminary analysis. Admission or inadmissibility for processing

Once the communication has been received, the Regulatory Compliance function will carry out a preliminary analysis to verify that it is a communication relating to conduct within the scope of application of Law 2/2023 and the formal requirements of the complaint.

In the event that the complaint does not meet the minimum requirements for processing, the Regulatory Compliance function will transmit its conclusions to the System Manager so that he or she can authorise, where appropriate, the inadmissibility of the communication. The file of the communication will be duly registered by Regulatory Compliance in the Complaints Channel.

In the event that a communication has been made that must be processed by another means, for example, a customer complaint or claim, the Informant will be redirected to the appropriate channel to carry out the communication received.

In the case of admission, if additional information is necessary to carry out the investigation, it will be requested prior to the start of the investigation. In this regard, efforts will be made to ensure that communications are based on documentary or witness evidence.

5.2.2. Information to affected parties

- **Communication to the Informant**: In the event that the complaint is admitted for processing, the decision will be communicated to the Reporting Person who identifies himself and provides some means of communication (email, telephone number, etc.) or through the Whistleblowing Channel tool within seven (7) calendar days, provided that it does not compromise the investigation itself. All this, unless the person has waived the right to receive notifications.

- **Communication to the accused:** A person affected by an internal investigation procedure originating from a communication received through

the Internal Information System shall be informed, as soon as possible, of the acts or omissions attributed to him or her and shall have the right to be heard at any time, except in cases where such communication would pose an obvious and significant risk to the investigation. and such communication must then be postponed until the danger disappears.

In any case, the above communication will be made in the time and manner considered appropriate to ensure the successful completion of the investigation. This exception shall be applied restrictively, on a case-by-case basis, and the broader interests at stake shall be taken into account.

In any case, the period for informing the reported person shall not exceed one (1) month from the date on which the complaint has been received, with the possibility of extending this period to a maximum of three (3) months if there are justified reasons for doing so.

This information will be sent in terms that protect the confidentiality of the Informant, so neither their identity, nor the area or department of the bank from which the communication comes, nor any other information that could facilitate the identification of the Informant will be included.

In any case, the affected party will be informed of the following points:

- Reception of the communication
- Acts imputed to him
- Processing of personal data

5.3. Investigation of the facts denounced

5.3.1. Opening of the file and designation of the instructor

As a general rule, the System Manager will be the **Investigator** of the investigation file. For the exercise of this function, the System Manager will have the support of the Regulatory Compliance function. Notwithstanding the foregoing, the System Manager may request the collaboration of other areas of the bank when the nature of the communication makes it advisable for operational or specialization reasons, and thus form an Investigation Committee.
In view of the specificity of the case in question, the System Manager may also request the collaboration of an external advisor when reasons of complexity, objectivity and the preservation of confidentiality and anonymity so advise.

5.3.2. Deadlines for the instruction

The duration of the investigation proceedings may not exceed **three months** from the receipt of the communication or, if an acknowledgement of receipt has not been sent to the Informant, three months from the expiry of the period of seven days after the communication is made. In cases of particular complexity, the System Manager may decide in a reasoned manner to extend the period up to a maximum of **three additional months**.

5.3.3. General Principles of instruction

In any case, during the investigation process, the guarantees and principles established in Aresbank's Internal Information System Policy will be respected. In particular:

- The person affected shall have the right to be informed of the acts or omissions (offences) attributed to him or her by means of a succinct communication of the facts and to be heard at any time. The accused may present the facts that he considers relevant and provide all the evidence that proves his innocence as far as the information is concerned, that is, he will be able to defend himself against the facts that are imputed to him and refute the evidence against him.
- Their presumption of innocence and their right to honour and right of defence shall be respected.
- Strict confidentiality will be maintained with respect to communications.

The investigation process shall be adequately documented, indicating in any case the facts, evidence analysed and the conclusions reached in the analysis.

5.3.3. Instruction

The Instructing Officer shall carry out all those actions and consultations deemed necessary to verify the accuracy and veracity of the information received, as well as to clarify the facts. Among others:

- **Document analysis**. The Instructor will analyze in detail the information and/or documentation provided by the Informant, affected person or witnesses. Likewise, it may request as much additional information and/or documentation of a professional nature as may be necessary, always taking into account criteria of proportionality and reasonableness.
- **Witness proceedings**. The Investigator shall give a hearing to the persons concerned, including in all cases the Informant, the affected person and witnesses. All of them must be aware of the rights, guarantees and duties of the parties.
  The interviews held must be duly documented, either by recording (upon request and authorization by the interested party) or by minutes of the meeting held. In the latter case, the minutes of the reading of the rights, guarantees and duties of the parties, signed by all those present, will be attached.
- **Technical or expert opinions or reports**. At any time during the instruction phase, the instructor may obtain an opinion or technical report, both from other Aresbank professionals and from external experts in the field. Such external opinions or reports should be attached to the Research Report.

5.3.4. Conclusions

Once the relevant evidence has been collected, and analysed together with all the information available from the beginning of the communication, the investigation phase itself is closed and the System Manager or, where appropriate, the Investigation Committee, will decide on compliance/non-compliance with the regulations with respect to the facts/conducts that are the subject of the communication. and this will be communicated to the parties involved as quickly as possible.

The System Manager will proceed to issue a Report of the procedures carried out, which will include:

- Facts reported in the complaint.
- Steps taken in the investigation of the case.
- Results of the proceedings carried out.
- Allegations of the accused.
- Assessment of the reported facts.

The System Manager, in view of the Report derived from the investigation, will prepare a Resolution Proposal of the complaint made, in which he will pronounce on:

- **Filing the complaint**: The System Manager will agree to file the complaint and the actions taken when, after the appropriate investigation, it considers that the facts reported have not been sufficiently proven, or they do not constitute an infringement included in the objective scope of the Whistleblowing Channel.

- **Proposal of disciplinary measures to be adopted**: When the facts reported have been sufficiently proven and, in addition, constitute an infringement included in the objective scope of the Whistleblowing Channel, the System Manager

    - It shall formulate in writing a proposal for a resolution, duly justified, of the possible disciplinary measures to be adopted and/or the seriousness of the facts.
    - It will propose to send the complaint, the documented results of the investigation and the proposal for a sanction and/or the assessment of the facts, to the Department of Administration and Human Resources and the General Directorate so that they can assess, within 10 working days, the applicable sanction according to the applicable rules.

- **Whistleblower Protection Measures**. When, having proven the facts denounced, they constitute any of the infractions included in the objective scope of the Whistleblowing Channel, the System Manager may assess the maintenance of the whistleblower protection measures deployed during the process of processing the complaint, taking into account the circumstances of each specific case.

Conclusions should be set out in a clear and concise manner, and always in relation to the evidence and analysis obtained during the investigation. Any

conclusion that is based on the knowledge and experience of the research team must be accompanied by a warning to that effect.

If there has also been any limitation in the course of the investigation, or it has not been possible to obtain any of the requested evidence, it must also be reflected in the report.

In the event of inappropriate conduct on the part of an employee, the System Manager will forward the file to the Human Resources function and the General Management. If the report contains a proposal for other measures, the file shall be forwarded to the Directorate-General. In any case, the Compliance Committee will be informed of the measures taken.

In the event that it is found that the facts may constitute a criminal offence, the Legal Counsel function will be informed so that, immediately, it can forward the information to the Public Prosecutor's Office or the European Public Prosecutor's Office, in the event that the facts affect the financial interests of the European Union.

The maximum period for responding to the investigation proceedings may not exceed three (3) months from the receipt of the communication or, if no acknowledgement of receipt was issued to the informant, three months from the expiry of the period of seven days after the communication was made, except in cases of particular complexity that require an extension of the deadline. in which case, it may be extended up to a maximum of three additional months.

VII. CONFLICT OF INTEREST MANAGEMNET

A conflict of interest exists when the objectivity of the person who has to make decisions about a communication is compromised by his or her relationship with the Informant, with the respondent, or with the facts communicated. Conflict of interest can be:

- Direct, when the complaint is the subject of the complaint.
- Indirect, when, without being the accused, objectivity is at risk of being compromised for other reasons, such as:
  - The existence of an affective or kinship relationship with the defendant:
  - Friendship or open enmity with the Informant or the respondent or, if there are several, with any of them.
  - Relationship by reason of marriage or similar relationship of effectiveness or kinship with the Informant or the accused or, if there are several, with any of them.
  - The presence of personal interests (e.g., economic or professional development) that may be compromised by the investigation of the facts reported.

- The existence of vicarious liability (e.g., for inaction) in relation to the facts complained of.

- The direct team relationship between the Whistleblower and the Respondent.

If any of the persons participating in the investigation is involved in the facts denounced, or if there is a conflict of interest, they will abstain from processing the file (unless they proceed in their capacity as the accused) and must inform the System Manager.

If the complaint is directed against the System Manager or there is a conflict of interest, the latter will refrain from intervening in the processing of the file (except as appropriate in his or her capacity as the respondent) and must inform the Compliance Committee. Thus, the Compliance Committee will be responsible for deciding who will oversee processing the complaint.

VIII. CONFIDENTIALITY AND PROTECTION OF `PERSONAL DATA

Aresbank will adopt the necessary measures to preserve the identity and guarantee the confidentiality of the data corresponding to the persons affected by the communications received.

In particular, the processing of personal data arising from the application of this Procedure will be governed by the provisions of Regulation (EU) 2016/679, Organic Law 3/2018 and the provisions of Title IV of Law 2/2023.

Thus, the processing of personal data subject to this Procedure will be governed by the following principles:

- **Respect for the principle of proportionality and limitation of purpose:**

The data collected as a result of a communication will only be those that are necessary to manage the information received.

In this sense, personal data that is not necessary for the knowledge and investigation of communications that fall within the scope of application of Law 2/2023 will be immediately deleted. Likewise, all personal data that may have been communicated and that refer to conduct not included in the scope of application of the aforementioned law 2/2023 will be deleted.

Finally, if the information received contains personal data included within the special categories of data. They will be immediately deleted, without being registered or processed, unless, following a risk analysis and, where appropriate, a data protection impact assessment, their processing is strictly necessary for reasons of essential public interest in accordance with article 30.5 of Law 2/2023

- **Information for interested parties:**

When personal data is obtained directly from the data subjects, they will be provided with the information referred to in Articles 13 and 14 of Regulation (EU) 2016/679 and 11 of Organic Law 3/2018.

In the case of the Informant, he/she will also be expressly informed that his/her identity will be reserved in any case and that it will not be communicated to the persons to whom the facts reported refer or to third parties.

You will also be informed that data subjects may exercise the rights referred to in Articles 15 to 22 of Regulation (EU) 2016/679: access, rectification, erasure, restriction, portability, opposition and not to be subject to a decision based solely on automated processing. To this end, Aresbank has enabled email derechoslopd@aresbank.es.

In the event that the person to whom the facts related in the communication refer exercises their right to object, it will be indicated that (i) the processing of the data is carried out in compliance with legal obligations applicable to Aresbank and (ii) for those uses of data that could be based on a legitimate interest, It will be presumed that, in the absence of proof to the contrary, there are compelling legitimate grounds that legitimise the processing of your personal data.

Aresbank has also appointed a Data Protection Officer who is responsible for enforcing compliance with the GDPR. To contact the Data Protection Officer, the interested party can send a communication to the following email address: dpd.aresbank@aresbank.es.

- **Limitation of access to information:**

Access to the data contained in the Internal Information System shall be limited, within the scope of its powers and functions, exclusively to:

- The System Manager, the Regulatory Compliance function and those who, in accordance with the provisions of section III. (iii) this procedure could include the committee of inquiry into a particular communication.
- The Head of Human Resources, only when disciplinary measures could be taken against an employee.
- The Head of Legal Counsel, if appropriate to adopt legal measures in relation to the facts reported in the communication.
- The Data Protection Officer, for the purpose of advising and supervising compliance with data protection regulations.

Likewise, it will be lawful for the data to be processed by other people, or even communicated to third parties, when it is necessary for the adoption of corrective measures in the entity or the processing of sanctioning or criminal proceedings that, where appropriate, may be appropriate.

- **Preservation of the identity of the Whistleblower and the persons concerned**

Anyone submitting a communication has the right not to have their identity disclosed to third parties.

Aresbank has put in place the appropriate technical and organisational measures to preserve the identity and guarantee the confidentiality of the data corresponding to the persons concerned and to any third party mentioned in the information

provided, the identity of the Informant, when the communication is not anonymous.

The identity of the Informant may only be communicated to the judicial authority, the Public Prosecutor's Office, or the competent administrative authority in the context of a criminal, disciplinary or punitive investigation. In such cases, the Informant will be informed before revealing his or her identity, unless such information could jeopardize the investigation or legal proceedings.

- **Data retention and deletion:**

The data will be kept only for the time necessary to decide on the admissibility of initiating an investigation into the facts denounced.

If it is proven that the information provided or part of it is not true, it will be immediately deleted as soon as this circumstance becomes known, unless such lack of veracity may constitute a criminal offence, in which case the information will be kept for the necessary time during which the legal proceedings are being conducted.

In any case, if three months have elapsed since receipt of the communication without any investigation proceedings having been initiated, it must be deleted, unless the purpose of the preservation is to provide evidence of the operation of the System.

Communications that have not been processed may only be recorded in anonymised form, without the blocking obligation provided for in article 32 of Organic Law 3/2018, of 5 December, being applicable.

Personal data relating to the information received and internal investigations will only be kept for the period necessary and provided for the purposes of complying with Law 2/2023. Under no circumstances may the data be kept for a period exceeding ten years.

IX. APPROVAL, REVIEW AND UPDATE OF THE PROCEDURE

The Regulatory Compliance function is responsible for the periodic review of this document.

This Procedure shall be reviewed and submitted to the Board of Directors for approval, where appropriate, at least every three years.

Apart from this triennial periodicity, Aresbank's Regulatory Compliance function will also review the content of the report and submit it to the Board of Directors for approval, after review by the Compliance Committee, whenever any of the following circumstances occur:

- Changes in the applicable regulation.
- Deficiencies detected in internal or external audits and other possible control processes.
- Approvals or modifications of internal policies and procedures that affect the content of this policy.

- Significant organizational changes affecting this Procedure.

ANNEX I. CATALOGUE OF INFRINGEMENTS REFERRED TO IN DIRECTIVE (UE) 2019/1937

a) Infringements falling within the scope of the Union acts listed in the Annex relating to the following areas:

   i. Public procurement,

   ii. Financial Services, Products and Markets, and prevention of money laundering and terrorist financing,

   iii. Product Safety & Compliance,

   iv. Transport Safety,

   v. Environmental protection,

   vi. Radiation protection and nuclear safety,

   vii. Food and feed safety, animal health and animal welfare,

   viii. public health,

   ix. Consumer protection,

   x. protection of privacy and personal data, and security of networks and information systems;

b) Infringements affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU);

c) Infringements relating to the internal market as referred to in Article 26(2) TFEU, including infringements of EU competition rules and State aid, as well as infringements relating to the internal market in relation to acts infringing corporate income tax rules or practices aimed at obtaining a tax advantage which distorts the object or purpose of the Applicable Corporate Income Tax Legislation.

ANNEX II: MAIN EXTERNAL CHANNELS FOR COMMUNICATIONS SET OUT IN ARTICLE 2 OF LAW 2/2023

Public Authority	Access web address
Independent Whistleblower Protection Authority	In the process of creation
Bank of Spain	www.bde.es/wbe/es/para-ciudadano/gestiones/canal-de-denuncias-del-banco-de-espana/
Spanish Data Protection Agency	sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/tramitesCiudadano.jsf
National Securities Market Commission	www.cnmv.es/portal/whistleblowing/presentacion.aspx
Tax Agency	sede.agenciatributaria.gob.es/Sede/colaborar-agencia-tributaria/denuncias/denuncias-no-tributarias.html
Madrid	Municipal Anti-Fraud and Corruption Office (https://www.madrid.es/portales/munimadrid/es/Inicio/El-Ayuntamiento/Denuncias)
Catalonia	Anti-Fraud Office of Catalonia (Anonymous Complaints Mailbox | Anti-Fraud Office of Catalonia)
Basque Country	In the process of creation

ANNEX III. PROTOCOL PROHIBITING RETALIATION

I. Object

The main objective of this Protocol on the Prohibition of Retaliation (hereinafter, the "**Protocol**") is the protection of Informants who submit a communication through the channels included in the Internal Information System (hereinafter, "**Internal System**" or "**System**"), of Aresbank, with respect to possible reprisals, including threats of retaliation and attempts at retaliation. The Protocol also aims to establish a protection framework that can effectively address situations of risk and protect persons who report such retaliation in good faith.

II. Scope of application

This Protocol applies to all personnel subject to Aresbank's Policy.

In addition, the protective measures provided for in this Protocol shall also apply:

- To those individuals who assist the informant in the process.
- To their co-workers and family members (ascendants and descendants, spouses or common-law partners, and siblings).
- To those natural persons who, due to their close relationship with them, may influence or condition the informant when it comes to filing a complaint and providing information and possible means of proof.
- To legal entities for which the informant works or with which he or she has any other type of relationship in an employment context or in which he or she holds a significant stake. For these purposes, it is understood that the participation in the capital or in the voting rights corresponding to shares or participations is significant when, due to its proportion, it allows the person who holds it to have the capacity to influence the investee legal person.

III. Concept of retaliation

For the purposes of this Protocol, “retaliation” means any act or omission that is prohibited by law, or that, directly or indirectly, involves unfavorable treatment that places the persons who suffer it at a particular disadvantage with respect to another in the employment or professional context, solely because of their status as Whistleblowers, and provided that such acts or omissions occur during the duration of the investigation procedure or within two years following the termination of the investigation procedure. An exception is made in cases where such action or omission can be objectively justified in the light of a legitimate aim and the means of achieving that aim are necessary and appropriate.

Retaliation shall be considered to be reprisals in the form of:

a) Suspension of the employment contract; dismissal or termination of the employment or statutory relationship, including non-renewal or early

termination of a temporary employment contract after the probationary period has passed, or early termination or annulment of contracts for goods or services; imposition of any disciplinary measure, demotion or denial of promotions and any other substantial modification of working conditions and the non-conversion of a temporary employment contract into an indefinite one. All this in the event that the worker had legitimate expectations that he or she would be offered an indefinite job; unless these measures were carried out within the regular exercise of the power of management under labour law, due to proven circumstances, facts or infractions, and unrelated to the presentation of the communication.

b) Damages, including reputational damages, or financial loss, coercion, intimidation, harassment or ostracism.

c) Negative evaluation or references regarding work or professional performance.

d) Blacklisting or dissemination of information in a certain sectoral area, which hinders or prevents access to employment or the contracting of works or services.

e) Cancellation of a license or permit.

f) Denial of training.

g) Discrimination, or unfavorable or unfair treatment.

IV. Measures to protect against retaliation

In order to protect the Informants, the System Manager will ensure that the appropriate protection measures are applied. In particular, by way of example and not limitation:

- **Anonymity and confidentiality**: the Informant may, at his/her free choice, identify himself or herself or submit his/her communication anonymously. In any case, it is guaranteed that all communications received will be treated confidentially and in accordance with the data protection regulations in force, protecting both the identity of the Informant who wishes to identify themselves and that of the facts, data and information provided relating to natural and legal persons.

  As a measure to guarantee the confidentiality of the identity of the Informant who decides to identify himself, Aresbank expressly states that the identification data of the Informant is not included in the scope of the right of access that may be exercised by the Informant. Therefore, and as a general rule, the Informant will not know the identity of the Informant.

  Likewise, all persons who, by reason of the functions they perform, have knowledge of the communications that are made, are obliged to maintain professional secrecy regarding the identity of the Informant and any information or data they have access to, the breach of this duty being a very serious infringement.

- **No Retaliation Against the Bona Fide Whistleblower**, such as dismissal, non-renewal, early termination of the employment relationship, reputational or economic damage, performance evaluations that are not in accordance with the work performed, among others.
- **Development of training and communication actions on measures to protect** against retaliation aimed at Aresbank Personnel and Third Parties.
- **Periodic monitoring of the Whistleblower's situation**: the System Manager will carry out periodic monitoring to prevent the adoption of retaliation:
  - **Personal:** The System Manager will monitor the working conditions of the Informants. To this end, it may hold regular meetings with them to find out first-hand their employment situation, requesting from them, where appropriate, the documentation it deems necessary – for example, but not limited to, periodic performance evaluations, internal promotions, job assignments, etc. – during the processing of the complaint and, especially, after it has been filed, in order to verify that there has not been any condition or behaviour that could entail retaliation.

    Where appropriate, the possibility of adopting measures, temporary or permanent, aimed at protecting the professional who has made the communication will be assessed (e.g. physical change of workplace or location, change of area/department or change of job, change of supervisor or manager, change of reporting line, etc.).

    If it is found that retaliation has indeed been taken against the Whistleblower or other persons involved, in addition to taking appropriate corrective action against the perpetrators of such retaliation, the Whistleblower will be restored to the situation prior to the injury suffered (e.g.: reinstatement of the employee to his or her original job/salary/responsibilities; access to internal promotion/training/benefits and rights denied; offer of apology; compensation damages; etc.).

    For the development of the aforementioned actions, the System Manager will have the support of Aresbank's Administration and Human Resources Department.
  - **Third parties external to Aresbank**: to the extent applicable, the System Manager shall monitor the business relationship with the reporting business partner in order to ensure that there is no retaliation, such as early termination or cancellation of contracts.

Any of the subjects who, being included in the scope of application of this Protocol, suffer reprisals, threats of retaliation or attempted reprisals, as a result of communication through the Internal Information System, will be entitled to request the protection of the competent authority, in addition to the protection of Aresbank.

The System Manager will record the actions carried out within the framework of its periodic monitoring function, as well as the results obtained, in the application of the Whistleblowing Channel.

V. Support measures

Although Law 2/2023, of February 20, 2023, only obliges the Independent Authority for the Protection of Whistleblowers (A.A.I.) to provide support measures, Aresbank will ensure that, as far as possible, a series of support measures are provided to the Informant, if necessary and always taking into account the assessment of the circumstances arising from the communication and the criteria of the System Manager:

- Information on the procedures and remedies available for protection from retaliation provided by competent authorities, as well as information on external reporting channels.
- Psychological and/or financial support.
- Legal assistance in legal proceedings in which the informant may be affected.

The support measures provided to the Informant will respond to the casuistry and needs of each case and, in any case, other protection measures and/or support may be applied in addition to those set out in the previous section and in this section, in order to guarantee and ensure rapid and effective protection.

VI. Conditions for protection

Persons falling within the scope of this Protocol (paragraph 2) who report infringements shall be subject to the protection regime provided for in this Procedure, provided that:

a) The communication or complaint has been submitted in compliance with the requirements set forth in the Internal Information System Management Procedure.

b) The reporting person has reasonable grounds to believe that the reported information is true at the time the report was filed, even if the reporting person was unable to provide conclusive evidence.

On the other hand, those subjects who report the following are expressly excluded from protection:

a) Information that is already fully available to the public;

b) Complaints that are inadmissible;

c) Information related to interpersonal conflicts, or affecting only the respondent and the respondent;

d) Mere rumours;

e) Information related to infringements not included in the objective scope of the Whistleblowing Channel.

VII. Periods of protection

Any person within the scope of this Protocol who is subject to reprisals, threats of retaliation or attempted retaliation as a result of the communication of information or a complaint through Aresbank's Internal System shall be entitled to request the protection of the competent authority within a period of two years.

To this end, the Informant's follow-up will be carried out by Aresbank's System Manager for at least a period of two years, unless the circumstances imply a longer monitoring period.

VIII. Violations of the Protocol on the Prohibition of Retaliation

In the event of suffering retaliation or having suspicions or knowledge of its adoption with respect to another person, the Head of the System must be immediately informed through the application of the Whistleblowing Channel, face-to-face meeting or by post, so that he can analyse the case and adopt the appropriate measures to prevent it or, where appropriate, correct them. All this, without prejudice to any other disciplinary or legal actions that may be applicable.

If retaliation is confirmed, the perpetrators will be subject to investigation and, where appropriate, disciplinary action in accordance with established procedures or any other legal action that may be applicable.