Particular annexes for the Spanish jurisdiction in the documentation of the internal complaints system in force in the Rothschild & Co Group

Rothschildco Wealth Management Spain, A.V., S.A.

November 2024

Internal use

Document History

Version	*Changes made*	*Author*	*Date of completion*	*Date of approval*
V1	Creation of the Appendices	GAR	15/11/2024	09/12/2024

Table of Contents

1. Background

Rothschildco Wealth Management Spain, A.V., S.A. (the **" Company "**) is a Spanish company belonging to the Rothschild & Co Group, which has aninternal system for reporting breaches (*whistleblowing*).

Based on an analysis of the system's documentation[1] with respect to applicable Spanish legislation[2], different gaps were identified that the Company covers by means of annexes to the system's documentation that are specific to this jurisdiction.

The annexes to the above documents are listed below.

2. Annex to the document Group Policy on Reporting Concerns and irregularities (Whistleblowing) of March 2022

This Annex describes the specific features of the Group Policy on Reporting Concerns and irregularities (Whistleblowing) (the "Policy") to be considered in Spain, so that the Policy, together with the 'Procedure on Reporting Concerns and irregularities (Whistleblowing)' (the "Procedure") document the Internal Information System of the Company in accordance with Law 2/2023, of 20 February, regulating the protection of persons reporting infringements of regulations and the fight against corruption (the 'Law 2/2023') .

In this regard, in Spain:

1. Within the personal scope of application of the Policy (section 1.2), in Spain natural persons who have obtained information on infractions in an employment or professional context **, even if the relationship is completed, as well as volunteers, interns, employees in training periods regardless of whether they are paid or not, as well as those whose employment relationship has not yet begun, will be considered as** informants .[3][4]

   2. The protection provided for in Law 2/2023 for informants shall also extend to the legal representatives of working persons in the exercise of their functions of advising and supporting the informant and, where appropriate, to the natural persons who, within the framework of the Company, assist the informant in the process, to natural persons who are related to the informant and who may suffer reprisals, such as coworkers or relatives of the informant, and to legal persons, for whom they work or have any other kind of relationship in a working environment or in which the informant has a significant participation .[5]

   3. The foregoing shall be entitled to the protection provided for in Law 2/2023 provided that the following circumstances are met:

   (a) Make communications (or public disclosures) related to actions or omissions:

   i. *Which may constitute infringements of European Union law provided that*:

   - *They fall within the scope of the EU acts listed in the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting infringements of Union law, irrespective of their status under national law.*
   - *Affect the financial interests of the EU as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU).*
   - *They have an impact on 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 which infringe the rules of corporate tax or practises the purpose of which is to obtain a tax advantage which would undermine the object or purpose of the legislation applicable to corporate tax*.

   ii. Or which may constitute a serious or very serious offence or administrative offence in Spain.

   (b) Have reasonable grounds to believe that the information is true at the time of communication (or public disclosure), even if they do not provide conclusive evidence.

   (c) The communication (or public disclosure) was carried out in accordance with the requirements established in Law 2/2023.

   4. If the facts which are the subject of the information may constitute an offence, they must be brought to the attention of the Department of Public Prosecutions or the European Public Prosecutor's Office, as the case may be.

   5. The Company shall not (and shall ensure that its professionals do not adopt) any form of direct or indirect reprisals, including threats or attempted reprisals, against any person who has reported a

[1] *Group Policy on Reporting Concerns and irregularities (Whistleblowing), March 2022 and Procedure on Reporting Concerns and irregularities (Whistleblowing) , May 2022.*
[2] *Act 2/2023 of 20 February on the protection of persons reporting regulatory and anti-corruption offences.*
[3] *In any case, including: (A) persons who are public employees or employed persons; (B) the self employed; (C) shareholders, unitholders and persons belonging to the administrative, management or supervisory body of the undertaking, including non executive members; D) any person who works for or under the supervision and direction of contractors, subcontractors and suppliers.*
[4] *In cases where information on infringements has been obtained during the pre contractual selection or negotiation process.*
[5] *For this purpose, it is understood that the participation in the capital or in the voting rights corresponding to shares or units is significant when, by their proportion, it allows the person who owns it to have the capacity of influence in the investee company.*

possible breach in accordance with the above requirements.Retaliation is any act or omission prohibited by law, or which, directly or indirectly, results in unfavourable treatment that places the person who suffers it at a particular disadvantage compared to another in the employment or professional context, solely because of his or her status as a reporter (or because he or she made a public disclosure). Retaliation includes but is not limited to:

(a) Suspension of the contract of employment, dismissal or termination of the employment or statutory relationship; imposition of any disciplinary measure; downgrading or denial of promotion and any other substantial modification of working conditions; and non conversion of a temporary employment contract into an indefinite one, in the event that the person making the communication had legitimate expectations in that regard; unless such measures were carried out in the regular exercise of executive power under the labour legislation or regulating the status of the relevant public employee, due to circumstances, events or infringements established, and unrelated to the submission of the communication.

(b) Damages, including those of a reputational nature, or economic losses, coercion, intimidation, harassment or ostracism.

(c) Evaluation or negative references with respect to work or professional performance.

(d) Inclusion on blacklists or dissemination of information in a given sector, which makes it difficult or impossible for individuals to access employment or to contract works or services.

(e) Refusal or cancellation of a licence or permit.

(f) Refusal of training.

(g) Discrimination or treatment that is unfavourable or unfair

6. Act 2/2023 also provides for the following measures to support and protect the informant, to be provided, where appropriate, by the Independent Authority for the Protection of the informant or by another competent authority or body:

(a) Support measures:

i. Full, independent and free information and advice on available procedures and remedies, protection from retaliation and the rights of the person concerned.

ii. Effective assistance by competent authorities to any relevant authority involved in their protection from retaliation, including certification that they are eligible for protection under Law 2/2023.

iii. Legal assistance in cross border criminal and civil proceedings in accordance with Community law.

iv. Financial and psychological support, on an exceptional basis, if so decided by the Independent Reporting Authority, A.A.I. following an assessment of the circumstances arising from the submission of the communication.

(b) Protection measures:

i. The informant shall not be deemed to have violated any restriction on disclosure of information and shall not be held liable of any kind in connection with such disclosure or public disclosure, provided that he or she had reasonable grounds to believe that such disclosure was necessary to disclose a breach, in accordance with the definition included in Law 2/2023. This measure will not affect criminal responsibilities.

This extends to the communication of information by representatives of workers, even if they are subject to legal obligations of secrecy or not to disclose classified information. This is without prejudice to specific protection rules applicable under labour law.

ii. The informant shall not be liable for the acquisition of or access to the information communicated, provided that such acquisition or access does not constitute a crime.

iii. In proceedings before a court or other authority concerning the injury suffered by the informant, once it has reasonably demonstrated that it has made a communication and that it has suffered injury, the injury shall be presumed to have arisen as a reprisal for reporting. In such cases, it shall be up to the person who took the injurious measure to prove that that measure was based on duly justified reasons unrelated to the communication.

iv. In judicial proceedings, including those concerning defamation, infringement of copyright, breach of secrecy, infringement of data protection rules, disclosure of business secrets, or requests for compensation based on labour or statutory law, the informant and those persons to whom protection is legally extended to the informant shall not incur any liability whatsoever. The informant and those persons to whom the protection is legally extended to the informant shall have the right to plead in their dismissal and in the framework of the aforementioned judicial proceedings, to have reported, provided that they have reasonable grounds to believe that the communication was necessary to reveal an infringement under Law 2/2023.

7. Appropriate information on the use of the internal information channel, as well as on the essential principles of the management procedure, shall be

provided in a clear and easily accessible manner. In any case, this information must be recorded on the home page of the Socedad website, in a separate and easily identifiable section.

The governing body has appointed a Responsible consisting of three members as collegiate body of the Internal Information System. Ms. Noémie Criado and Ms. Rebeca García, members of the department of internal coordination and support of Regulatory Compliance, and by Mr. Lorenzo Gallardo, analyst, who will delegate to one of their members the powers of management of the IIS and processing of the investigation files.

The designation of the Responsible of the Internal Information System and its members shall be notified to the Independent Authority for the Protection of the Reporting Person.

The Responsible of the Internal Information System shall diligently assume, in the absence of any conflict of interest, the management of the information received, ensuring the proper application of the Procedure, without prejudice to the possible outsourcing of the receipt of information. It shall also keep a record of the information and communications received and the Research Records that have arisen, ensuring the confidentiality of such information and compliance with data protection regulations.

The Responsible of the Internal Information System has the material and personal resources necessary for the correct performance of his duties, which he performs independently and independently from the other bodies of the Company, and his actions must be governed by the general principles included in this Policy and in accordance with Law 2/2023.

This Policy, taken into consideration and approved by the Board of Directors of the Company, as responsible for the implementation of its Internal Information System, will be duly publicised within the Company.

3. Annex to the document Procedure on Reporting Concerns and irregularities (Whistleblowing) of May 2022

This Annex describes the specifics of the Procedure on Reporting Concerns and irregularities (Whistleblowing) to be considered in Spain, so that the Procedure, together with the Group Policy on Reporting Concerns and irregularities (Whistleblowing), document the Internal Information System of the Company in accordance with Law 2/2023, of 20 February, on the protection of persons reporting regulatory infringements and the fight against corruption (the **" Law 2/2023** ").

The Responsible of the Internal Information System (the "**IIS Responsible**") will be responsible for its diligent processing.

3.1 Internal Information System Channel

The Company will permanently keep available to its directors, executives, employees, shareholders, suppliers, as well as to other third parties indicated in the Appendix for Spain of the Policy, the Internal Whistleblowing Channel as an appropriate channel for the communication of possible breaches included in the scope of the Policy that relate to or affect the scope of its professional activity, without prejudice to the possibility that they may address their communications to the Independent Protection Authority of the informant or to any other competent authority or body.

This channel is the preferred channel for the communication of information regarding possible breaches.

The means established to channel information regarding potential breaches through the Internal Whistleblowing Channel are as follows:

(a) *Written communication, either by post addressed to the attention of Ms. Noémie raised at Paseo de la Castellana, 40 bis, 28046 Madrid, Spain; or in the space reserved on the website for this purpose, managed by a third party (Whistleblower Software by Formalize), in* Rothschild & Co Wealth Management Spain Communication System | Inicio *where communication is permitted without including personal data.*

i. *Verbal communication in the space reserved on the website for this purpose, managed by a third party (Whistleblower Software by Formalize), in Rothschild & Co Wealth Management Spain Communication System | Inicio where it is possible to record a distorted voice message; or directly with the* IIS Responsible *if you choose to report in person meetings, which will take place within the seven working days following the request.*
Verbal communications must be documented, with the consent of the informant, in any of the following ways: (I) by a recording of the conversation or II) by a complete transcript of the conversation which may be reviewed by the informant.
The informant may indicate in his communication a postal or e mail address for the purpose of receiving notices and may also expressly waive the receipt of any subsequent communication.
The communication may also be done anonymously at source by written communication by post without indicating the sender and other data that could identify the informant.
The confidentiality of the communication and the identity of the informant and any third party mentioned in the communication shall be protected by the provisions of this Procedure and additional information security measures based on the ISO 27001 standard.
The identity of the informant, if known, as well as of the third parties mentioned in the communication, may only be communicated, in addition to the third parties indicated in the privacy policy, to the Judicial Authority, the Public Prosecutor's Office or the competent administrative au-

thority in the context of a criminal, disciplinary or disciplinary investigation, after transfer to the informant or the third party concerned, provided that this circumstance does not jeopardise the ongoing investigation or judicial proceedings.

3.2 External channels

Without prejudice to the preferential channel of the Internal Information System channel, for the communication of possible breaches referred to in the Policy Annex, the informants may also access the channels established by the Public Authorities for this purpose, either directly or after communication through the Internal Whistleblowing Channel.

The external channels authorised for reporting breaches are as follows[6]:
(a) For breaches in Catalonia: www.antifrau.cat/es
(b) For breaches relating to the defence of competition: https://sede.cnmc.gob.es/tramites/competencia/denuncia-de-conducta-prohibida

3.3 Processing of Research Files

(a) General issues

The investigation file regulated in this section will be processed only if the Company does not have a specific procedure or protocol for investigating the file based on the content of the information (e.g. protocols established by law for the prevention and treatment of complaints of moral, sexual and/or gender based harassment).

The Research File is understood to be the set of actions carried out to verify and clarify the facts included in the communications of which IIS Responsible becomes aware.

The IIS Responsible will be responsible for documenting the different phases of the investigation and for guarding all the documentation generated during the processing in any type of support and must adopt the necessary measures to guarantee the confidentiality of the Research File and complying with the regulations on the protection of personal data.

This is understood to be without prejudice to the custody tasks that may be entrusted to those teams or persons that could support the Investigation File Instructor.

The notifications that must be sent to the informant, as well as to the members of the Company and other third parties related to the Research File, will be sent from an email address or, as the case may be, from a specific platform, which allows communication with these persons and obtaining their answers in a reserved and confidential manner, so that only the IIS Responsible or the Research File Instructor have access to the content of such communications, thus complying with the regulations on the protection of personal data.

(b) Receipt, acknowledgement of receipt and admission/entry for processing.

The IIS Responsible will initiate a Research File when he becomes aware of facts or circumstances that may constitute a breach, either ex officio or by virtue of a communication or information received through the channels authorised for this purpose, or by any other means.

The most common ways of learning about potential breaches are as follows:

i. Communications received through the channels authorised for this purpose.

ii. Press news.

iii. Judicial/Prosecution/Police injunctions.

iv. Findings in the framework of an internal control procedure.

In the event that any member of the Company, other than the IIS Responsible, receives a communication or information relating to a potential breach, it must be sent immediately to the IIS Responsible, maintaining the confidentiality of the communication and, where appropriate, the identity of the informant. IIS Responsible will enter such communication or information in the Internal Whistleblowing Channel and will proceed in accordance with the provisions of this procedure.

The manager of the IBS will ensure that he/she is informed of the previous reporting obligation, as well as the consequences of noncompliance, which will be subject to disciplinary measures.

All information and communications of which the IIS Responsible is aware shall be identified with a registration number.

In the event that the Investigative File begins upon receipt of a communication, the IIS Responsible shall send the informant, provided that he/she has not waived the right to receive notifications, or his/her anonymity is not compromised (if any), an acknowledgement of receipt within seven calendar days of receipt of the communication, unless this may jeopardise the confidentiality of the communication.

Once the communication has been received and registered, and the existence of a conflict of interest has been ruled out, the IIS Responsiblrmust rule on its admission or non admission. To that end, it shall verify whether the information concerns facts potentially constituting a breach as defined in this procedure.

If necessary in order to decide on admission or rejection, the IIS Responsible may request additional information from the informant regarding the facts that are

[6] Indicate the external channels authorised at the date of approval of this Procedure.

the object of the communication received, provided that the informant has not given up receiving notifications or his or her anonymity is not put at risk (if applicable).
In any event, the rejection of a communication must be based on at least one of the following reasons:

i. *The facts reported lack any likelihood.*

ii. *The facts reported do not constitute noncompliance as defined in this procedure.*

iii. *The communication is manifestly unfounded or, in the opinion of the IIS Responsible, there are reasonable indications that the information contained in the communication would have been obtained by committing an offence.*

iv. *The notice does not contain new and significant information on a noncompliance compared to an earlier communication in respect of which the relevant proceedings have been completed, unless new factual or legal circumstances exist which warrant a different follow up.*

If the information is admitted for processing, the IIS Responsible shall verify whether there is a specific procedure or protocol for investigating the investigation file (e.g. protocols established by law for the prevention and treatment of complaints of moral, sexual and/or gender based harassment). Where appropriate, once the specific procedure or protocol is completed, the results of this investigation shall be sent to the IIS Responsible for any other necessary measures in accordance with this Procedure.

In the event that the facts on which the information was received might constitute an offence, the European Public Prosecutor's Office or the European Public Prosecutor's Office should be notified, as appropriate.

The decision on admission or rejection of the communication received shall be taken within ***ten working days*** *from the date of registration and shall be notified to the informant within* ***five working days*** *of the decision being taken. In the event of non admission, the reasons shall be transferred to the informant. All of this, provided that the informant has not waived the right to receive notifications or his or her anonymity is not compromised (where applicable).*

(c) Investigation of the file

If the communication is accepted, the investigation shall commence, which shall include all the proceedings designed to verify the verisimilitude of the facts to which the information relates.
The time limit for carrying out the investigation shall not exceed ***three months*** *from the receipt of the communication or information except in cases of particular complexity requiring an extension of the time limit, in which case it may be extended to a maximum of* ***three additional months.***

All phases of the Research File must be documented, under the direction and supervision of the IBS Manager, in an appropriate and sufficient manner to ensure its traceability and allow its accreditation to a third party.

i. *Appointment of the Instructor*

The IIS Responsible will designate the person responsible for processing the Research File and coordinating the research actions carried out (the 'Instructor'), who may be himself, another member of the collegiate body or of the Company or a professional external to the Company.

In any case, the following guidelines shall be followed for the selection of the Instructor:

- *If the communication or information affects any member of the administrative body or the Chief Executive Officer, a person external to the Company shall be appointed as Instructor.*
- *In the event that communication or information affects the IIS Responsible or any of its members, the latter may not participate in the investigation file, and must refer the rest of the members of the body if it is a collegiate body in order to appoint a person external to the Company as an Instructor.*
- *Where the person concerned by the communication or information is a member of the Works Council, a staff delegate or a delegate of a trade union section, account must be taken of the specific formalities which apply to this condition, for which the person responsible for Human Resources of the Company must be informed.*

In the event that an internal Instructor other than the IIS Responsible is appointed, the IIS Responsible shall notify him of such appointment.

If an External Instructor is appointed, the relevant service provision contract shall be signed, including the Processor Agreement as required by the Personal Data Protection Regulations.

The Instructor shall ensure confidentiality and impartiality in the performance of his or her duties, which include but are not limited to the following:

- *Compilation of the background and relationship with the Company of the persons involved in the information received.*
- *Communication to persons potentially responsible for the facts that are the object of the communication or information received (the 'affected person') of the existence of the Investigation File.*
- *Decision on investigative actions deemed necessary to clarify the facts, in accordance with time bound planning.*
- *Determination, as the case may be, of the areas of activity of the Company that should be involved in the Research File.*

- *Identification of persons who can account for the facts and provide additional information.*
- *Determination of the documentation requirements to be submitted to any third party.*
- *Opening, if appropriate, of new lines of research in view of the evidence obtained.*
- *Evaluation of the relevant evidence obtained in the research*

The Instructor may require the assistance of external advisers or personnel belonging to internal bodies or departments of the Company. In the latter case, the existence of conflicts of interest must be ruled out in advance.

ii. Development of instruction

During the investigation, the necessary actions will be carried out to investigate and clarify the facts contained in the communication or information admitted for processing.

Respect for the presumption of innocence and the honour of the person concerned, as well as the protection of his or her personal data, shall be ensured at all times. He shall be informed of the initiation of the investigation and, succinctly, of the facts attributed to him, as well as of his right to be heard at any time and in such manner as is deemed appropriate to ensure the proper conduct of the investigation.

Where such information may lead to the concealment, destruction or alteration of evidence by the person concerned, it may be postponed until the time of the interview, stating the reasons for such decision in the Investigation File. Under no circumstances shall the person concerned be informed of the identity of the informant or given access to the communication.

Once the person concerned has been informed of the existence of the Investigative File, he/she may request the examination of the information and documentation contained therein, although the necessary measures must be taken to ensure that no type of information is disclosed that would make it possible to know the identity of the informant.

If the presence in the Company of the person concerned during the training period could jeopardise the successful completion of the Research Purpose, at the proposal of the Instructor, and in accordance with labour and data protection regulations at all times, he may be restricted from access to the Company's facilities, documentation/information and computer systems, and may suspend employment other than salary, in order to ensure that the necessary research activities are carried out without interference.

If necessary for the proper purpose of the Investigation File, the Instructor may request additional information from the informant regarding the facts that are the object of the communication sent, provided that the informant has not given up receiving notifications or his or her anonymity is not put at risk (if applicable).

Likewise, if as a result of the investigation carried out other events that might constitute new breaches were detected, the IIS Responsible - previously informed by the Instructor where applicable - shall agree to open a new investigation file, or if related to the investigation under way, to extend it.

If as a result of the investigation proceedings carried out during the investigation of the Investigation File, indications of the possible commission of an offence are identified, the European Public Prosecutor's Office or the European Public Prosecutor's Office, as the case may be, must be notified.

- *Specific issues: Collection and/or extraction of information and documentation in any medium.*

During the course of the investigation investigation investigation, all information and documentation that may contribute to the clarification of the facts investigated will be collected.

If necessary, the Instructor shall coordinate the e discovery work to be carried out on computer equipment and devices that may contain information relevant to the research, selecting the keywords that allow such information to be extracted. Access to computer devices will be made in the legally established terms.

The documentation and information gathered will form part of the Research File and may be used to defend the interests and rights of the Company.

The Instructor may rely, in compliance with the regulations on the protection of personal data, on a forensic investigation team to carry out the necessary technical tasks, and may opt for an internal or external team:

If the intervention of these forensic teams is necessary, they shall essentially carry out the following tasks:

- *E discovery: Consisting of the acquisition, processing and indexing of the information stored in the computer devices included in the research perimeter.*
- *Forensic accounting: Designed to analyse economic and financial corporate documentation.*
- *Corporate intelligence: Analysis of the corporate and equity structure and the personal, financial and equity links that the people affected may have.*
- *Data tracking: Analysis of information flows to identify possible obtainment or illicit use of information.*

Likewise, in carrying out these tasks, the forensic team will be in charge of guarding all documentation and information, in any format, that is acquired and generated during the development of the Investigation File. To this end, they shall establish the necessary technical guarantees to ensure confidentiality and the chain of custody.

- *Specific issues: Interviews*

In the development of the Research File, the Instructor may carry out all the interviews considered necessary for the verification and clarification of the facts.

The interviews shall be announced sufficiently in advance and shall be conducted by the Instructor in the presence of at least one other person, always respecting the rights to privacy, honour, defence and presumption of innocence of the interviewee. In addition, the following questions will be taken into account according to who the person interviewed is:

- *Affected per of the facts reported and to provide the documents or evidence he/she deems relevant to his/her defence, which shall be incorporated into the Investigation File. The person concerned shall be informed of all matters relating to the processing of personal data in compliance with the rules applicable for this purpose, unless the person concerned already has such information. He or she shall be invited to explain his or her version of the facts and may refuse to answer any or all of the questions put to him or her or to answer only such questions as he or she deems appropriate.*

- *Person other than the person affected: The interview will begin by informing the interviewee of the duty to maintain the utmost confidentiality in relation to the Research File in progress and their participation in it. You will be informed of everything related to the processing of personal data in compliance with the applicable regulations for this purpose, unless you already have this information. Likewise, you will be informed of your duty to collaborate in the development of the investigation, responding fairly and truthfully to the questions asked and providing any data at your disposal and that are required by you.*

In any event, interviews shall be conducted in a context that is fully respectful of the rights of the interviewees.

A written record containing the content of the interview shall be drawn up from the interview. The record shall be read to the interviewee to give his agreement to the content. In the case of discrepancies, such discrepancies shall be analysed and, where appropriate, the necessary amendments shall be made to the minutes or such discrepancies recorded. The record shall be signed at the end of the interview by both the Instructor and the interviewee. If the interviewee does not wish to sign the record, this will be recorded.

In addition, if the interviewee so authorises, instead of the written record, the interview may be recorded and incorporated into the file. In this case, an equally effective alternative procedure shall be provided and, if not previously provided, the processing of image and/or voice data shall be included in data protection information.

In the event that the affected person or any of the members of the Company, duly called to appear in the framework of the Investigation File, does not acknowledge receipt of the communications sent or does not confirm their participation in the investigation in the form requested, the Instructor will request this confirmation by phone or even through a personal contact - always ensuring the reserved nature of the communication - and will document the result of the management carried out.

If, after this communication, the person summoned does not appear in the process for which the appointment is made, the Investigative File will continue its course.

If third parties who do not have a contractual relationship with the Company do not come forward after the first written notice, they will be deemed to refuse to participate in the open investigation. Accordingly, no additional communication will be sent.

iii. Resolution of the Research File

Upon completion of all investigation proceedings, the Instructor shall issue a report containing at least the following information:

- *Identification code assigned to the communication or information that gave rise to the Research Purpose.*
- *Chronological description of the main milestones in the processing of the Research File.*
- *List of the investigation proceedings carried out to establish the verisimilitude of the facts to which the information relates, as well as the documentation provided.*
- *Assessment of the outcome of the investigation carried out and the conclusions reached.*
- *Motion for a resolution.*

Where the Instructor is a person other than the IIS Responsible, he/she shall forward the report together with the Research File to the IIS Responsible who, in accordance with the conclusions reached in that report, shall adopt one of the following resolutions:

- *Favourable decision: It will be adopted in cases where it is considered that no breach has been established, which will determine the conclusion of the investigation investigation file without the need to take any action. The decision shall be notified to*

the person concerned.

- *Non favourable resolution: It will be adopted when it is determined that the commission of any breach attributable to the person affected has been proven.*

  In this case, and when labour regulations apply, the appropriate measures will be taken in accordance with the applicable disciplinary regime, and specifically, with the provisions of the Collective Agreement applicable to the relevant relationship and the Workers' Statute.

  If the affected person's relationship with the Company does not permit the application of labour regulations in disciplinary matters, the corresponding legal or statutory provisions shall be observed.

The result of the investigation report shall be communicated to the informant, provided that he/she has not waived the right to receive notifications or that his/her anonymity (where applicable) is not put at risk, as well as the confidentiality of the information received

3.4 Registration

The manager of the Iic shall keep a record of the information and communications received and the Research Records that have arisen, ensuring the confidentiality of such information.

The register shall contain the following information for each communication or information received:

(a) Date of receipt

(b) Registration number

(c) Internal investigation procedure: YES/no

(d) Closing date

For the preservation of the information collected in the register, the regulations on the protection of personal data and Law 2/2023 shall be applied. In particular, personal data which, where appropriate, are entered in the register may be kept only for the period necessary to prove compliance with Law 2/2023.

3.5 Protection of personal data

The processing of personal data carried out in the framework of the IIS shall be carried out in full compliance with the general principles and obligations established in the regulations on the protection of personal data and in the Law on the protection of the informant

(a) Obligations of the IIS Responsible on data protection

Among other obligations, the IIS Responsible will ensure that:

i. The principle of transparency, the informant, the person concerned or any third party involved in the investigation must be provided with the information required in the field of personal data protection. To this end, the controller shall draw up a corresponding information clause to be made available to the data subjects.In particular, the informant shall be informed that his/her identity shall in any event be reserved and that he/she shall not be notified to the person concerned or to the third party except, where appropriate in accordance with the provisions of the Law on the Protection of the informant, the Judicial Authority, the Department of Public Prosecutions or the competent administrative authority in the context of a criminal, disciplinary or disciplinary investigation.

ii. The principle of minimisation, and no data must be collected other than those that are strictly necessary and indispensable for the correct functioning of the IBS, if more than strictly necessary data are collected by accident, will be eliminated as soon as possible.

iii. The principle of limitation of the purpose, and the personal data collected through the Iic must not be processed for any purpose other than managing the communication and processing of the Data Subject.

iv. The principle of limiting the retention period, and personal data must be processed only for the time necessary to decide whether to initiate an investigation into the facts reported by the informant.

v. In any case, once three months have elapsed since the receipt of the communication without having initiated the investigation, the personal data must be deleted, unless the purpose of the preservation is to provide evidence of the functioning of the system.

vi. Communications that have not been acted upon may only be retained in an anonymized manner, without applying the blocking obligation provided for in the personal data protection regulations.

vii. The principle of accuracy, and all personal data included in the information communicated that are not true must be deleted. All this, unless the absence of truthfulness may constitute a criminal offence, in which case the information shall be stored for the time necessary during the course of the judicial proceedings.

viii. The principle of integrity and confidentiality, ensuring the confidentiality of the informant and third parties as indicated in the Procedure. In addition, technical and organisational security measures shall be put in place as may be necessary to protect the information from unauthorised or unlawful processing and from loss, destruction or accidental damage

No personal data may be collected other than that which is necessary and essential for the proper management of the IMS.

(b) Limited access to IBS personal data

Personal data in the IIS shall only be accessible to third party service providers who are treated as data controllers and the Data Protection Officer.

It may also have access to the personal data contained in the IIS:

i. The human resources officer, who shall have access to personal data only and exclusively, when disciplinary measures may be taken against a worker.

ii. The person responsible for the legal services, who shall have sole and exclusive access to personal data if necessary the adoption of legal measures in relation to the facts reported in the communication.