Procedure for Managing the Internal Information System

INDEX

1. PURPOSE

This "Procedure for Managing the Internal Information System" (hereinafter, the "Procedure") regulates the management and handling of reports submitted through RESA[1]'s Internal Information System (hereinafter, the "Internal Information System" or the "System", interchangeably).

This Procedure develops the "Corporate Policy on the Internal Information System" (hereinafter, the "Policy") with regard to establishing the guidelines, principles, guarantees and actions to be followed for managing the information received through the Internal Information System.

2. SCOPE OF APPLICATION

The scope of application of RESA's Internal Information System is set out in the "Corporate Policy on the Internal Information System".

3. PERSON RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM

RESA's Management Body has appointed the Compliance Committee as the person responsible for the Internal Information System (hereinafter, the "System Manager"), which assumes the management and handling of investigation files.

The System Manager shall act autonomously and independently from the rest of RESA's bodies, committees or commissions, without interference or instructions of any kind during the performance of its duties.

Likewise, it must have the personal and material resources necessary for the proper performance of its duties.

The powers and responsibilities assigned to this role are set out below:

- It shall ensure the confidential nature of the identity of the person using the System ("reporting person") who freely chooses to identify themself. Thus, it shall ensure that the identity of the reporting person is not disclosed to third parties—especially the reported person—without their consent, unless legally required (for example, by formal request from a Court or Tribunal).

[1] For the purposes of this Procedure, RESA means the Organization made up of the following companies:

Residencias de Estudiantes S.L.
Siresa Campus, S.L.
Sociedad Invensora en Residencias para Estudiantes Euskadi, S.A.
Siresa Salmantina, S.L.
Dibea Itg, S.A.
Hereinafter, "RESA" or the "Group", interchangeably.

- It shall seek to maintain a secure and confidential communication channel with the reporting person, using the Reporting Channel tool or any other means that may be enabled for this purpose depending on the circumstances.
- It shall ensure that the processing, investigation and resolution of the communications received are carried out in accordance with the legislation, principles and guarantees of the "Corporate Policy on the Internal Information System" and the other applicable internal rules, acting with full independence and impartiality.
- It shall report periodically to the Management Body, at least annually and whenever necessary, all information required concerning the System's activity, preserving in all cases the confidentiality and security of the information, as well as the other guarantees and rights of users established in the "Corporate Policy on the Internal Information System".

Finally, the System Manager shall keep the Register Book updated with the information on the communications received.

4. CHANNELS FOR REPORTING COMPLAINTS

The reporting channels available at RESA are set out in the "Corporate Policy on the Internal Information System".

5. PROCEDURE FOR HANDLING REPORTS

5.1 Receipt, acknowledgement of receipt and registration of reports

The System Manager shall be responsible for receiving reports submitted through the various channels of the Internal Information System.

Submission of a report shall generate an acknowledgement of receipt to the reporting person within seven (7) calendar days following receipt of the report.

If the report is submitted through a tool, the acknowledgement of receipt shall be generated automatically.

Special features of verbal reports

Where the report is received verbally, the System Manager shall offer the reporting person the possibility to submit, ratify, expand on or clarify the report in an in-person or remote meeting within a maximum period of seven (7) days from receipt.

If the reporting person agrees to hold such meeting, the System Manager shall document the report by recording it (if the reporting person gives authorization) or by means of a complete and accurate

transcript of the conversation. At this meeting:

- The reporting person may be accompanied, if they wish, by a lawyer or by an employee representative.
- To guarantee due confidentiality of the information and facts communicated, as well as of the different participants, those attending the meeting shall be informed in writing of their duty of secrecy and confidentiality, as well as of all legal information on data protection matters.
- If a transcript is used, it must be signed by those present at the meeting. If, for any reason, the reporting person or any of those present do not wish to sign the record, this shall be stated and the investigation shall continue.

Finally, the System Manager shall attach the recording or transcript of the conversation to the file and continue the investigation procedure in accordance with this Procedure.

Special features of reports submitted through other channels

If any information is received through a channel other than those mentioned above, the reporting person shall be informed of the channels (or, where appropriate, it may be channelled ex officio through the Reporting Channel), and this procedure shall apply in cases where the report falls within the scope of application.

If a person other than the System Manager receives, by any means, a communication relating to an irregularity or infringement covered by the objective scope of this Procedure, they must immediately transfer it to the Manager through the System.

In all cases, the person who has received such communication has a duty of confidentiality regarding all the information communicated, especially with respect to the identity of the reporting person and other affected persons.

Breach of this duty, especially regarding confidentiality, is considered a very serious infringement and may entail the application of the relevant disciplinary and legal consequences.

All reports received shall be assigned an identification code for proper traceability and follow-up and shall be recorded in the Register Book of reports.

5.2 Decision on admission or non-admission for processing

Once the report has been registered, the System Manager shall carry out a preliminary analysis of its scope and content, deciding on its admission or non-admission for processing according to the indications of infringement and the evidence provided.

Accordingly, the System Manager shall adopt one of the following decisions:

- **Admission for processing**: admission shall be agreed when the facts reported fall within the

objective scope of application of the System and it is considered that there are sufficient elements giving credibility to the report.

- **Non-admission for processing**: otherwise, the Manager shall decide not to admit it for processing.

Without prejudice to the foregoing, in order to ensure the proper functioning of the System, if the System Manager considers that the report has a remediable defect (whether formal or substantive), before deciding on its admission or non-admission for processing, it shall inform the reporting person so that the defect may be remedied as soon as possible.

Likewise, if the Manager considers that the information provided is not sufficient to initiate an investigation, it shall also indicate this to the reporting person so that, where appropriate, they may provide further detail or additional information.

5.2.1 Communication to the affected parties

- Communication to the reporting person: in the event that the report is admitted for processing, the decision shall be communicated to the reporting person, unless that person has expressly or tacitly waived the right to receive notifications.
- Communication to the reported person: in accordance with the applicable legislation, the reported person has the right to be informed succinctly of the actions or omissions attributed to them, and to be heard at any time during the investigation. However, it shall be necessary to assess, on an individual basis, whether informing them at that time could compromise the proper development and successful outcome of the investigation.

5.3 Investigation of the report

5.3.1 Opening of the file and appointment of the Investigating Officer

Once the communication has been admitted for processing, the System Manager shall appoint, depending on the nature of the facts reported, the Investigating Officer for the investigation file. In all cases, the Investigating Officer must have access to all documentation and information related to the facts under investigation.

In all cases, the System Manager shall supervise the handling and investigation of reports conducted by the appointed Investigating Officer and shall provide support, assistance and advice at all times.

5.3.2 Investigation of the reported facts

i. Time limits for the investigation

The investigation may not exceed a maximum period of three (3) months from receipt of the report. In particularly complex cases requiring an extension, this period may be extended by up to an additional

three (3) months.

ii. General principles of the investigation

Throughout the investigation file, compliance with the principles and guarantees set out in the "Corporate Policy on the Internal Information System" shall be ensured.

iii. Investigation

The Investigating Officer shall carry out all actions and inquiries deemed necessary to ascertain the accuracy and truthfulness of the information received, as well as to clarify the facts. These include, among others:

- Documentary analysis. The Investigating Officer shall analyse in detail the information and/or documentation provided by the reporting person, affected person, witnesses and other persons connected with the investigation procedure. Likewise, they may request any additional professional information and/or documentation deemed necessary, always observing criteria of proportionality and reasonableness.
- Witness interviews. The Investigating Officer shall hear the persons linked to the investigation of the facts, including in all cases the reporting person, the affected person and witnesses. All of them must be aware of the rights, guarantees and duties assisting the parties.
- The interviews held must be duly documented, either by recording (subject to request and authorization of the interested party) or by means of minutes of the meeting held. In the latter case, the record of having read out the rights, guarantees and duties of the parties, signed by all attendees, shall be attached.
- Technical or expert opinions or reports. At any time during the investigation phase, the Investigating Officer may request a technical opinion or report, either from other RESA professionals or from external experts in the matter. Such external opinions or reports must be attached to the Investigation Report.

5.3.3 Issuance of the internal investigation report

Once all actions have been concluded, the Investigating Officer shall issue a Report of the procedures carried out, which shall be delivered to the System Manager, unless the latter has assumed the investigation of the file, and it shall contain at least the following:

- Facts or conduct subject to investigation.
- Detailed analysis of the investigation (participants, affected departments, etc.).
- Investigative steps carried out during the handling of the file.
- Result of the investigative steps carried out.

- Assessment of the facts reported.
- Conclusions.
- Where appropriate, measures adopted.

If the Investigating Officer is the System Manager, the internal investigation report may contain the Proposed Resolution referred to in the following section.

5.3.4 Resolution of the file

In light of the Report resulting from the investigation, the System Manager shall prepare a Proposed Resolution including:

a. Closure of the file, when, after the appropriate investigation, it is considered that the reported facts have not been sufficiently proven, or that they do not constitute an infringement included within the objective scope of the System.

b. The proposal of disciplinary and/or sanctioning measures to be adopted, when the reported facts have been sufficiently proven and, in addition, constitute an infringement included within the objective scope of the System.

If the facts appear to constitute a criminal offence, the System Manager shall send the information to the Public Prosecutor's Office.

5.3.5 Communication of the resolution

Finally, the final decision adopted shall be communicated to the reporting person and to the reported person. To safeguard the rights and guarantees of all parties, under no circumstances shall the investigation report or the resolution be provided to the reporting person, the reported person or other persons unrelated to the Investigating Officer and the System Manager.

6. MANAGEMENT OF CONFLICTS OF INTEREST

A conflict of interest exists where the objectivity of the person who must make decisions regarding a report is compromised by their relationship with the reporting person, the reported person, or the facts reported. The conflict of interest may be:

- Direct, where the person is the subject of the report.
- Indirect, where, without being the reported person, objectivity may be at risk for other reasons, such as:
    - the existence of a relationship of affection or kinship with the reported person;
    - manifest friendship or enmity with the reporting person or the reported person or, if

there are several, with any of them;

- a connection by marriage or analogous relationship of affection or kinship with the reporting person or the reported person or, if there are several, with any of them;
- the presence of personal interests (e.g. economic or professional development) that may be affected by the investigation of the reported facts;
- the existence of indirect responsibility (e.g. by omission) in relation to the reported facts;
- a direct team relationship between the reporting person and the reported person.

Measures to avoid conflicts of interest

- If the report is directed against any of the members of the body responsible for the System, or if any conflict of interest exists with them, that person must abstain from intervening in the handling of the file (except insofar as may be appropriate in their capacity as affected person).
- The investigation shall be assumed by another of the members responsible for the System or, where necessary, may be entrusted, totally or partially, to an independent third party.
- If the report concerns a member of the Management Body, the Manager may decide to seek the help and cooperation of an independent third party for the investigation, in whole or in part.
- If the report concerns a member of Senior Management, the Manager may decide to seek the help and cooperation of an independent third party for the investigation, in whole or in part.

7. PROTECTION OF REPORTING PERSONS

Acts constituting retaliation are expressly prohibited, including threats of retaliation and attempted retaliation against persons who submit a communication in accordance with this Procedure.

However, the prohibition of retaliation shall not prevent the adoption of the relevant disciplinary measures when the internal investigation determines that the report is false and that the person who made it was aware of its falsity, thus acting in bad faith.

The conditions, measures and time limits for the protection of reporting persons against retaliation are regulated in the “Protocol Prohibiting Retaliation” (Annex II).

8. DATA PROTECTION

When designing and reviewing this System, RESA shall ensure full and strict compliance with the applicable data protection regulations; in particular, 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, Organic Law 3/2018, of 5 December, on Data Protection, and the implementing regulations.

In this regard, as basic information, it is stated that the personal information collected shall be processed by "Residencias de Estudiantes S.L.", as the legally responsible entity, to try to prevent the commission of possible unlawful activities, as well as to comply with the legal obligations deriving from Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and combating corruption, as the main purposes.

Likewise, and among other matters, RESA shall adopt the technical and organizational measures necessary to guarantee data security and prevent their alteration, loss, unauthorized processing or access, taking into account the state of the art and the provisions of the legislation in force on the matter.

Persons referred to in the communications submitted, as well as those participating in the investigation procedure and other persons to whom the Law grants legal protection, may exercise their rights of access, objection, rectification, erasure, restriction of processing and portability, where legally applicable.

To know in due detail all legal information on Data Protection, you may consult our "Privacy Policy", also accessible on RESA's website.

9. APPROVAL, PUBLICATION AND ENTRY INTO FORCE

RESA's Management Body promotes and approves this Procedure, thereby fulfilling its role of establishing the necessary foundations for adequate and efficient management of the Internal Information System and promoting compliance with the principles and guarantees set out in the applicable Policy and this Procedure.

This Procedure shall be reviewed, updated, approved and disseminated periodically and whenever it is necessary to make any modifications.

Annex I - CATALOGUE OF INFRINGEMENTS CONTEMPLATED IN DIRECTIVE (EU) 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 and 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 network and information systems;

b) Infringements affecting the financial interests of the Union as referred to in Article 325 TFEU and as further specified in the relevant Union measures;

c) Infringements relating to the internal market as referred to in Article 26(2) TFEU, including infringements of Union competition rules and State aid rules, as well as infringements relating to the internal market in connection with acts infringing the rules on corporate tax or practices aimed at obtaining a tax advantage that defeats the object or purpose of the applicable corporate tax law.

Annex II – PROTOCOL PROHIBITING RETALIATION

1. PURPOSE

This "Protocol Prohibiting Retaliation" (hereinafter, the "Protocol") has as its main objective the protection of reporting persons who submit a communication through the channels included in RESA's Internal Information System (hereinafter, the "Internal System" or the "System", interchangeably) against possible retaliation, including threats of retaliation and attempted retaliation.

Likewise, the Protocol aims to establish a protection framework capable of effectively addressing risk situations and protecting persons who report in good faith from such retaliation.

2. CONCEPT OF RETALIATION

For the purposes of this Protocol, "retaliation" means any act or omission prohibited by law, or which, directly or indirectly, involves unfavourable treatment placing the persons who suffer it at a particular disadvantage compared with another person in the employment or professional context, solely because of their status as reporting persons, or because they have made a public disclosure, provided that such acts or omissions occur while the investigation procedure is ongoing or within the two years following its termination or the date on which the public disclosure took place. The exception is where such action or omission can be objectively justified by a legitimate purpose and where the means to achieve that purpose are necessary and appropriate.

The following, among others, shall be considered retaliation:

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 once the probationary period has been completed, or early termination or cancellation of contracts for goods or services, imposition of any disciplinary measure, demotion or denial of promotion and any other substantial modification of working conditions, and the non-conversion of a temporary employment contract into an indefinite one, where the worker had legitimate expectations that an indefinite job would be offered; unless such measures were adopted within the regular exercise of management powers under employment legislation or the rules governing the status of the relevant public employee, due to circumstances, facts or proven infringements unrelated to the submission of the communication.

b) Harm, including reputational harm, or economic losses, coercion, intimidation, harassment or ostracism.

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

d) Inclusion on blacklists or dissemination of information in a given sector, making access to employment or procurement of works or services more difficult or impossible.

e) Revocation of a licence or permit.

f) Refusal of training.

g) Discrimination, or unfavourable or unfair treatment.

3. CONDITIONS FOR PROTECTION

The persons included within the subjective scope of the Procedure for Managing the Internal Information System and Protecting the Reporting Person (hereinafter, the "Procedure") who report infringements included within the objective scope of the Procedure (exclusively those considered in section 2.2.A) shall be subject to the protection regime set out in this Protocol, provided that the following conditions are met:

a) The communication or report has been submitted in compliance with the requirements set out in the Procedure;

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

By contrast, the following persons are expressly excluded from protection if they report:

a) Information already fully available to the public;

b) Reports that are not admitted for processing;

c) Information related to interpersonal conflicts, or affecting only the reporting person and the reported person;

d) Mere rumours;

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

4. MEASURES FOR PROTECTION AGAINST RETALIATION

In order to protect reporting persons, the System Manager shall ensure the application of any protection measures that may be appropriate. In particular, by way of example and not limitation:

- **Anonymity and confidentiality**: the reporting person may, at their sole discretion, identify themselves or submit their report anonymously. In all cases, it is guaranteed that all reports received shall be handled confidentially and in accordance with the data protection regulations in force, protecting both the identity of the reporting person who chooses to identify themselves and that of the facts, data and information provided concerning natural and legal persons.

  As a measure to guarantee confidentiality of the identity of the reporting person who decides to identify themselves, RESA expressly states that their identifying data are not included within the scope of the right of access that may be exercised by the reported person. Therefore, as a general rule, the reported person shall not know the identity of the reporting person.

Likewise, all persons who, by reason of the duties they perform, become aware of communications that are submitted are obliged to maintain professional secrecy regarding the identity of the reporting person and all information or data to which they have access, and breach of this duty constitutes a very serious infringement.

- **Prohibition on adopting retaliation against the reporting person acting in good faith**, such as dismissal, non-renewal, early termination of the employment relationship, reputational or economic harm, performance evaluations not consistent with the work performed, among others.
- **Development of training and communication actions** on protection measures against retaliation directed at RESA personnel and third parties with whom the Group has dealings.
- **Periodic monitoring of the reporting person's situation**: the System Manager shall carry out periodic monitoring to prevent retaliation.
    - **RESA Personnel**: the System Manager shall monitor the working conditions of reporting persons. To that end, it shall hold periodic meetings with them to learn first-hand about their employment situation, requesting, where appropriate, any documentation deemed necessary during the handling of the report and, especially, after its closure, in order to verify that there has been no condition or behaviour that could amount to retaliation.

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

      If it is established that retaliation has in fact been adopted against the reporting person or other persons involved, in addition to adopting the appropriate disciplinary measures against the perpetrators of such retaliation, the necessary and available measures shall be adopted to restore the reporting person to the situation prior to the harm suffered (e.g. reinstatement of the employee to their original job/salary/responsibilities; access to internal promotion/training/benefits and rights denied; apologies; compensation for damages; etc.).

      For the implementation of the aforementioned actions, the System Manager shall also have the support of the Human Resources Department.

    - **Third parties external to RESA**: to the extent applicable, the System Manager shall monitor the commercial relationship with the business partner who has submitted the report in order to guarantee the absence of retaliation, such as early termination or cancellation of contracts.

Any of the persons who, being included within the scope of this Protocol, suffer retaliation, threats of retaliation or attempted retaliation as a consequence of reporting through the Internal Information System, shall be entitled to seek protection from the competent authority, in addition to RESA's protection.

The System Manager shall record the actions carried out in the framework of its periodic monitoring function, as well as the results obtained.

5. SUPPORT MEASURES

Although Law 2/2023, of 20 February only obliges the Independent Whistleblower Protection Authority (A.A.I.) to provide support measures, RESA shall ensure that, to the extent possible, a series of support measures are provided to the reporting person, where necessary and always subject to assessment of the circumstances arising from the report and the System Manager's criteria:

- Information on the procedures and resources available for protection against retaliation offered by the competent authorities, as well as information on external reporting channels.
- Psychological support.
- Legal assistance in judicial proceedings in which the reporting person may be affected.

The support measures provided to the reporting person shall respond to the circumstances and needs of each case and, in any event, other protection measures and/or additional support may be applied in addition to those set out above and in this section, in order to guarantee and ensure rapid and effective protection.

6. BREACHES OF THE PROTOCOL PROHIBITING RETALIATION

In the event of suffering retaliation or having suspicions or knowledge of retaliation being adopted against another person, the matter must be reported immediately to the System Manager through the Internal Information System so that the case may be analysed and the appropriate measures adopted to prevent or, where appropriate, remedy it. All this is without prejudice to any other disciplinary or legal actions that may apply.

If retaliation is confirmed, those responsible shall be investigated and, where appropriate, subject to disciplinary sanctions in accordance with the established procedures, or the legal actions available under law shall be applied.

Annex III – PRIVACY POLICY OF THE INTERNAL INFORMATION SYSTEM

1. Introduction and purpose

This policy develops the legal obligations required in accordance with Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and combating corruption (hereinafter, the "Whistleblower Protection Law" or "Whistleblowing Law"), pursuant to which RESIDENCIAS DE ESTUDIANTES S.L. (hereinafter, RESA) has a Reporting Channel that makes it possible to bring to its attention any irregularity detected within its organisation.

The purpose of this policy is to declare the organization's commitment, and especially that of its Governing Bodies and Senior Management, to the compliance function and, specifically, to the Whistleblower Protection Law.

RESA's internal information system (hereinafter, the "Reporting Channel") is made available to the reporting person through the following channels:

- In writing, through the corporate website www.resa.ethic-channel.com or by post at Calle Serrano no. 41, 4th floor, 28001 Madrid, for the attention of the Ethics Committee.
- In person, at the reporting person's request.

2. Material and personal scope of application

2.1.1. Personal scope - — Who may report through the Reporting Channel?

Through RESA's Reporting Channel, the following reporting persons may report any infringement of which they become aware in a work or professional context and which is subject to the objective scope developed in this policy:

a) persons who are employees, salaried workers or self-employed workers;
b) shareholders, stakeholders and persons belonging to RESA's management, governing or supervisory body, including non-executive members;
c) any person who works for or under the supervision and direction of contractors, subcontractors and suppliers;
d) volunteers, interns, workers in a training period, regardless of whether or not they receive remuneration;
e) job candidates whose employment relationship with RESA has not yet begun, but who become aware of infringements during the selection process or pre-contractual negotiations;
f) workers whose employment relationship has already ended;
g) RESA's clients and suppliers.

In addition, whistleblower protection measures shall apply equally to the following groups:

a) legal representatives of employees in the exercise of their advisory and support functions for the reporting person;
b) natural persons who, within the organisation in which the reporting person provides services, assist them in the process;
c) natural persons related to the reporting person and who may suffer retaliation, such as co-workers or family members of the reporting person; and
d) legal entities for which the reporting person works or with which they maintain any other type of relationship in an employment context or in which they hold a significant shareholding. For these purposes, a shareholding in the capital or voting rights corresponding to shares or participations is deemed significant where, by its proportion, it allows the person holding it to have the capacity to influence the legal entity in which they participate.

2.1.2. Material scope — What can be reported through the Reporting Channel?

Anyone having well-founded knowledge of any kind of act or omission that may constitute an unlawful act or one contrary to current regulations, or that may contravene the principles and values of RESA's Code of Ethics, must report it through the Reporting Channel enabled for that purpose.

The objective scope of the Reporting Channel extends to the following breaches or irregularities:

a) **Any acts or omissions that may constitute infringements of European Union law provided that they:**
    1. fall within the scope of the acts of the European Union 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 who report breaches of Union law, regardless of how they are classified under domestic law;
    2. affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU); or
    3. affect the internal market, as referred to in Article 26(2) TFEU, including infringements of European Union competition rules and State aid rules, as well as infringements relating to the internal market in connection with acts infringing the rules on corporate tax or with practices aimed at obtaining a tax advantage that defeats the object or purpose of the legislation applicable to corporate tax.

b) **Acts or omissions that may constitute a criminal offence or a serious or very serious administrative infringement**. In all cases, all serious or very serious criminal or administrative

infringements involving economic loss to the Public Treasury and Social Security shall be deemed included.

c) **Acts or omissions that may contravene the principles and values of RESA's Code of Ethics**.

In this regard, the following categories of irregularities have, a priori, been defined as reportable through the Channel:

- Competition
- Public Procurement
- Financial interests of the Union
- Prevention of money laundering
- Environmental protection
- Consumer protection
- Protection of personal data and privacy
- Public health
- Security of networks and information systems
- Food safety
- Product safety
- Harassment, aggression and/or violence

3. Rights and guarantees of the reporting person and the reported person

Throughout the entire life cycle of the communication, RESA shall guarantee the following rights to the reporting person and the reported person:

a) **Confidentiality**: RESA shall provide due protection to all persons who submit a report, and the identity of the complainant/reporting person shall remain confidential at all stages of the investigation and resolution process.

b) **Anonymity**: RESA's reporting channel has been designed so that the reporting person who wishes to remain anonymous may do so with sufficient guarantees to preserve their identity and ensure the confidentiality of the data mentioned in the information provided.

c) **Good faith**: reports must always be submitted in good faith and be based on real facts, or reasonable grounds to believe that the information on the infringements is true, and must not be based on assumptions or unfounded facts.

d) **Prohibition of retaliation**: under no circumstances shall RESA retaliate against the reporting

person, including threats and attempted retaliation against persons who submit a report in good faith. This protection extends to any natural or legal person related to the reporting person with whom they are linked in one way or another in a work or professional context. However, in the event of any knowingly false, malicious or abusive report, RESA may take appropriate action against the reporting person.

e) **Right to receive a response within a reasonable time**: the reporting person shall receive an acknowledgement of receipt within a maximum period of seven calendar days from receipt by RESA, except where the reporting person expressly requests otherwise or where the body in charge of the investigation considers that such acknowledgement may compromise protection of the reporting person's identity.

f) **Right to receive information**: once a preliminary analysis of the report has been carried out, after RESA has verified the sufficiency and plausibility of the information, as well as whether the facts reported may constitute irregularities or acts contrary to ethics and legality, the reporting person shall be informed in writing.

In addition, during the processing of the file, the persons affected by the communication shall have the right to the presumption of innocence, the right of defence and the right of access to the file in the terms regulated by the Whistleblower Protection Law.

4. Data protection

The processing of personal data derived from the reporting channel shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights, and Organic Law 7/2021, of 26 May, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offences and execution of criminal penalties.

RESA has a Privacy Policy informing about the processing of personal data collected through the reporting channel, which may be consulted at www.resa.ethic-channel.com.

5. Operation of the reporting channel

The reporting person must complete the report form available on the website that RESA has established for this purpose.

Communication shall also be permitted, at the reporting person's request, through an in-person meeting.

Upon receipt of the information, RESA shall send an acknowledgement of receipt of the communication to the reporting person within no more than 7 calendar days from the day following its receipt, unless this could endanger the confidentiality of the communication.

The System shall assign the communication a relative identification code that will allow the reporting person to know at all times the processing status of their request, while guaranteeing throughout the process the confidentiality of the identity of the parties involved.

The reporting person must provide sufficient detail about the facts, conduct or suspicious activities so that the System Manager may assess and decide whether the communication sets out facts or conduct that do or do not fall within the scope of application set out in section 2.1.2 of this policy, and shall carry out a preliminary analysis of the content, determining whether the facts referred to in the communication are admitted or not admitted for processing.

If the communication is admitted for processing, the investigation shall begin, during which all actions aimed at verifying the plausibility of the facts described shall be carried out and, once the evidence has been gathered and analysed by the System Manager, the investigation phase shall conclude and a decision shall be made as to whether or not the communication made by the reporting person involves the commission of an unlawful act.

Before the expiry of the period of three months from receipt of the report, which may be extended by a further three months due to the special complexity of the case, RESA undertakes to provide a response regarding the investigation actions relating to the report.

6. Publicity

This policy shall be communicated to all Professionals and interested parties related to RESA and shall be published on RESA's corporate website and intranet.

7. Entry into force

This Policy was approved by RESA's Ethics Committee on 18 September 2023 and enters into force on the same day; it shall be reviewed periodically and any update must be approved by the Ethics Committee.

Version control

Versión	Fecha	Autor	Cambios producidos
02	March 2026	Person Responsible for the Internal Information System	Initial version. Adoption of the Internal Information System Procedure in accordance with the requirements of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and combating corruption.

Related documentos

Nombre	Última versión
Internal Information System Policy	March 2026