VALORIZA

MANAGEMENT PROCEDURE OF THE INTERNAL INFORMATION SYSTEM

CONTENTS

I. INTRODUCTION

Article 31 bis point 5, section 4 of the Criminal Code, in addition to including the obligation to implement, inter alia, an Organisation and Management Model for the Prevention of Crimes, establishes that legal entities must impose *"the obligation to report possible risks and breaches to the body in charge of monitoring the operation and observance of the prevention model".*

On the other hand, Law 2/2023, of 20 February, regulating the protection of persons who report regulatory and anti-corruption infractions ("Law 2/2023") establishes the obligation to implement an internal communications channel with the aim of providing a means through which to report irregular or suspicious conduct.

Those who report possible breaches will be protected by the safeguards set out in Law 2/2023 as long as the requirements established in terms of material and personal scope are met.

Accordingly, Valoriza Servicios Medioambientales, S.A., ("Valoriza" or "Organisation") within the framework of its Corporate Governance System and, in particular, of the VALORIZA Group's Regulatory Compliance, Crime Prevention and Antitrust Model (hereinafter, the Compliance Management System), has an Internal Information System that includes a Communications Channel (hereinafter, "the Channel"), with the aim of providing a means through which to report irregular or suspicious conduct or make inquiries in relation to the operation of the Compliance Management System.

The Internal Information System, in general, and the Channel, in particular, are an indispensable part of the Organisation's culture of compliance, information and integrity infrastructures, with the aim of preventing or detecting threats to the public interest.

The use of the Channel will be encouraged, guaranteeing interested parties that the information they provide will be treated confidentially within the company itself and without risk of reprisals.

The Internal Information System will be the preferred channel for reporting actions or omissions that fall within its scope, provided that the violation can be effectively dealt with and if the informant considers that there is no risk of retaliation.

The Internal Information System must also foster ideal results for the correct implementation of the Compliance Management System in the organisation, seeking to:

a) encourage and facilitate the reporting of irregularities;
b) support and protect informants and other persons involved;
c) ensure that reports of irregularities are handled in a proper and timely manner;
d) improve the organisational culture, governance and the prevention of irregularities.

Potential benefits to the organisation include:

a) it allows the organisation to identify and address irregularities as soon as possible;
b) it assists in preventing or minimising the loss of assets and in the recovery of lost assets;

c) it ensures compliance with the organisation's policies, procedures, and legal and social obligations;
d) it attracts and retains staff committed to the organisation's values and culture; and
e) it demonstrates to society, markets, regulators, owners, and other stakeholders sound and ethical governance practices.

An effective Internal Information System will build trust in the organisation by:

a) demonstrating the leadership's commitment to preventing and addressing wrongdoing;
b) encouraging individuals to submit early reports of irregularities;
c) reducing and preventing harmful treatment of informants and other persons involved; and
d) fostering a culture of openness, transparency and accountability.

II. PURPOSE OF THE PROCEDURE

The purpose of this Procedure is to be the guide for action in the event of communication through the channels provided and its subsequent management.

In this way, it sets out how to manage the information received, what decisions need to be made and what investigation process to follow, both in the preliminary phase of evaluating the information received, in the pre-procedural action if an investigation is initiated and taking into account the possibility of criminal proceedings.

The regulating of the reaction to the communication of possible breaches or irregularities is an important part of the regulatory compliance policies, in an organisation that has imposed on itself high ethical standards and a clear mission to create a "Culture of Compliance" within it.

All members of the Organisation have a duty to cooperate in any investigation processes that are initiated.

The Internal Information System Policy is available at: www.valorizasm.com.

III. INTERNAL INFORMATION CHANNEL.

The Internal Information System includes an internal channel to enable the submission of information regarding the infractions provided for in the defined scope and must allow communications to be made in writing or verbally, or both.

In this regard, the means determined by the Organisation to receive and manage communications is in writing:

- Either through the Channel enabled on the Valoriza website: www.valorizasm.com; or
- By postal communication addressed to the Valoriza Regulatory Compliance Unit, with address at C/ Condesa de Venadito, 5. 28027, Madrid.

In addition, at the informant's request, the communication may also be presented orally through a face-to-face meeting after the written request through the channels indicated above.

Oral communications made through a face-to-face meeting must be documented in one of the following ways, with the informant's prior consent:

- By recording the conversation in a secure, durable, and accessible format.

- Through a complete and accurate transcription of the conversation made by the staff responsible for dealing with it.

The data subject shall be informed about the processing of their data in accordance with data protection regulations and will be given the opportunity to check, make any corrections and accept the transcript of the conversation by signing it.

The submission and subsequent processing of **anonymous communications** will be accepted.

Finally, those who make the communication through this medium will be informed, in a clear and accessible way, about the external channels of information to the competent authorities and, where appropriate, to the institutions, bodies or agencies of the European Union.

IV. INTERNAL INFORMATION SYSTEM MANAGER.

The Board of Directors of Valoriza has the power to appoint an individual who will be responsible for the management of said system or Internal Information System Manager ("Internal System Manager"), and to remove or dismiss him/her; it may be decided that the Internal System Manager is a collegiate body, which must then delegate to one of its members the powers of management of the Internal Information System and the processing of the Internal Information System investigation files.

Both the appointment and the dismissal of the Internal System Manager must be reported to the Independent Authority for the Protection of informants, A.A.I. (in its initials in Spanish), or, where appropriate, to the competent authorities or bodies of the Autonomous Communities, within the scope of their respective competences, within the following ten working days, specifying, if the said person has been dismissed, the reasons for doing so.

The Internal System Manager must carry out his/her functions independently and autonomously from the rest of the organisation's bodies, may not receive instructions of any kind in the performance of his/her duties, and must have all the personal and material resources necessary to carry them out.

In entities or bodies in which there is already a person responsible for the function of regulatory compliance or integrity policies, whatever they may be called, this may be the person appointed as the Internal System Manager, provided that they meet the requirements established in this law.

As the Organisation is in the private sector, the Internal System Manager may be a director of the entity, who will perform his or her duties independently of the administrative or governing body thereof.

When the nature or scale of the entity's activities does not justify or permit the existence of a manager responsible for the system, it will be possible to ordinarily perform the functions of the position or post with those of the person responsible for the system, striving in all cases to avoid possible situations of conflict of interest

Under these premises, the Organisation has determined that the role of Head of the Internal Information System will be taken on by the Regulatory Compliance Unit.

V. MATERIAL SCOPE OF THE INTERNAL INFORMATION SYSTEM.

Communications relating to the following may be passed on and managed in accordance with the Internal Information System:

a) Actions or omissions that may constitute infringements of European Union Law whenever they:
   1. Fall within the scope of the acts of the European Union listed in the Annex to Directive (EU) 2019/1937[1];
   2. Affect the financial interests of the EU as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU);
   3. Affect the internal market, as referred to in Article 26(2) TFEU, including infringements of the European Union's rules on competition and funding granted by States, as well as infringements relating to the internal market in relation to acts infringing the corporate tax rules or with practices intended to obtain a tax advantage which distorts the object or purpose of the Purpose of the legislation applicable to Corporate Income Tax.

b) Acts or omissions that may constitute a criminal offence or a serious or very serious administrative infringement. In any case, it will be understood to include all serious or very serious criminal or administrative offences that involve pecuniary loss for the Public Treasury and Social Security Agency.

c) Actions or omissions of internal rules, policies or procedures that must be complied with by the members of the Organisation and whose non-observance may cause serious damage to the entity and may result in disciplinary action in the workplace.

Persons who report conduct related to the above or that does not constitute serious or very serious infringements will not legally enjoy the protection granted to informants by Law 2/2023.

However, the Organisation, as a gesture of its commitment and in a proactive manner, will recognise the right to protection of informants from actions or omissions of mandatory internal rules, policies or procedures, and also undertakes not to take reprisals against such persons.

As a guideline, irregularities or non-compliance may be reported in the following areas:

- Public procurement.
- Financial services, products and markets.

[1] **https://www.boe.es/doue/2019/305/L00017-00056.pdf**

- Environmental protection.
- Public health.
- Protection of privacy and personal data, and security of networks and information systems.
- Infringements affecting the financial interests of the European Union.
- Infringements relating to the internal market in the field of competition and funding granted by States, as well as infringements relating to internal market infringements in relation to acts infringing the rules on corporation tax.

VI. PERSONAL SPHERE

The people who may use the channel are those who have obtained information about infringements in a work or professional context, including:

a) Persons who have the status of employees;

b) The self-employed;

c) Shareholders, unitholders and persons belonging to the administrative, management or supervisory body, including non-executive members;

d) Any person working for or under the supervision and direction of contractors, subcontractors, and suppliers;

e) Third parties or business partners such as Customers, Suppliers, Collaborators and any related third parties.

VII. MINIMUM CONTENT OF COMMUNICATIONS.

The communication shall contain, as far as possible, the following points:

- Description of the allegedly irregular conduct, contrary to the law or the provisions of Valoriza's internal rules.
- The people possibly involved.
- Approximate dates of commission of the acts.
- Means through which the behaviours were carried out.
- Affected business areas.
- Relevant processes affected (e.g. procurement, accounting, treasury, etc.).
- Documents or evidence of the facts.

In any case, it is recommended that the communication be as descriptive and detailed as possible, thus making it easier for the recipient to identify the person(s) or department(s) involved.

In order to decide on its admissibility for processing, the informant may be asked to clarify or supplement the facts, providing any documentation or data that may be necessary to prove the existence of the irregular conduct.

VIII. PROTECTION CONDITIONS.

The protection of those who make a communication in good faith and honestly is guaranteed.

Thus, those persons who, having reasonable grounds to believe, in light of the circumstances and the information available to them at the time of communication, that the facts they communicate or report are true, will be protected.

This protection will not be lost even if the informant communicates inaccurate information due to a mistake made in good faith.

The personal motivation that the informant may have when making the communication will not be taken into account to grant this protection.

In particular, those who report through this channel due to their work activities related to the Organisation are protected against the risk of labour retaliation, for example, for breaching the obligation of confidentiality or loyalty.

This protection will apply not only to the person who has the status of full-time 'worker', but also to part-time workers and those on fixed-term contracts or with an employment contract or employment relationship with a temporary employment agency.

Likewise, this protection will apply in the following cases:

a) People who, even if they have not yet been hired, participate in selection processes, people who have ended an employment relationship, or personnel such as interns, volunteers, workers in training periods, i.e. people who may suffer reprisals, for example, in the form of negative job references, blacklisting or boycott of their business activity.

b) Legal representatives of the workers in performing their role of advising the informant.

c) Individuals who, within the framework of the organisation in which the informant works, assist the informant in the process.

d) Individuals who are related to the informant and who may suffer retaliation, such as co-workers or family members of the informant.

e) Legal entities for which the informant works or with whom he or she has any other type of relationship in a work context or in which the informant has a significant stake.

IX. SUPPORT MEASURES.

Law 2/2023 recognises that persons who report or disclose breaches will be able to avail of the following support measures:

a) Comprehensive and independent information and advice, easily accessible and free of charge, on available procedures and remedies, protection from retaliation and rights of the person concerned.

b) Effective assistance by the competent authorities to any relevant authority involved in their protection against reprisals, including certification that they are eligible for protection under this Act.

c) Legal assistance in criminal proceedings and cross-border civil proceedings in accordance with EU law.

d) Financial and psychological support, on an exceptional basis, if so decided by the Independent Authority for the Protection of informants, A.A.I. after assessing the circumstances arising from the submission of the communication.

All of the above is regardless of the assistance that may apply under Law 1/1996, of 10 January, on free legal aid, for representation and defence in legal proceedings arising from the presentation of the communication or public disclosure.

These support measures must be provided by the competent authorities

X. PROTECTION MEASURES AGAINST REPRISALS.

The protection recognised in Law 2/2023 includes:

a) Not to deem that the informant violates restrictions on the disclosure made or to deem that he or she shall be held liable whenever he or she has reasonable grounds to believe that it is necessary to bring a breach or omission of the regulations to the attention of the organisation.

b) Not to be held liable with respect to the acquisition of or access to information that is publicly communicated or disclosed, provided that such acquisition or access does not constitute a crime.

Persons who report maliciously, frivolously or abusively, or who deliberately and knowingly report incorrect or misleading information, as well as those who report information that is in the public domain, or unconfirmed rumours and gossip, shall be excluded from all protection.

This measure shall not affect responsibilities of a criminal nature.

This protection extends to the communication of information made by workers' representatives, even if they are subject to legal obligations of secrecy or not to reveal confidential information.

All of this is without prejudice to the specific protection rules applicable in accordance with labour regulations.

Special situations:

- In proceedings before a court or other authority concerning harm or loss suffered by informants, once the reporting person has reasonably demonstrated that he or she has communicated or made a public disclosure in accordance with the law and that he or

she has suffered harm or loss, the harm or loss shall be presumed to have occurred as a result of the harm or loss caused by the reporting person.

- In such cases, it shall be up to the person who took the prejudicial measure to prove that the action was based on duly justified grounds unrelated to the public communication or disclosure.
- In legal proceedings, including those relating to defamation, copyright infringement, breach of secrecy, infringement of data protection rules, disclosure of trade secrets, or claims for compensation based on employment or statutory law, informants shall not be liable as a result of communications or public disclosures protected by the Statute.
- Such persons shall have the right to claim, in their defence and in the context of the aforementioned legal proceedings, that they have communicated or made a public disclosure, provided that they have reasonable grounds to believe that the communication or public disclosure was necessary to reveal an infringement.

XI. PROHIBITION OF REPRISALS.

Informants are protected against any form of retaliation, including attempted retaliation or any form of threat, whether direct or indirect, carried out, encouraged or tolerated by co-workers or managers themselves.

Those who carry out, encourage or tolerate retaliation against an informant may be disciplined under the disciplinary provisions established in Valoriza's internal regulations or other applicable legislation, such as the applicable Collective Bargaining Agreement or the Workers' Statute.

Retaliation, whether consummated, attempted or threatened, is understood to mean the following actions:

a) suspension, dismissal, removal, termination, or equivalent measures of the employment and/or statutory relationship,
b) demotion or denial of promotions,
c) alteration of working conditions: change of position, location of the workplace, reduction of pay or change of working hours,
d) denial of training.
e) negative evaluation or references regarding their work and professional outcomes,
f) imposition of any disciplinary measure, reprimand or other penalty, including financial penalties,
g) coercion, intimidation, harassment or ostracism,
h) discrimination, or unfavourable or unfair treatment,
i) non-conversion of a temporary employment contract into an indefinite one, where the worker had a legitimate expectation that he or she would be offered an indefinite position;
j) non-renewal or early termination of a temporary employment contract,
k) harm, including to their reputation, especially on social media, or financial loss, including loss of business and revenue,

l) blacklisting on the basis of a sectoral agreement, informal or formal, which may mean that the person will not be employed in that sector in the future;
m) early termination or cancellation of contracts for goods or services,
n) revocation of a licence or permit.

XII. MEASURES FOR THE PROTECTION OF AFFECTED PERSONS.

The persons affected by the communication must also be guaranteed certain rights throughout the process, in particular:

a) The right to the presumption of innocence and to honour.

b) The right to be heard or in respect of the actions or omissions attributed to them, within a suitable period of time so as not to prejudice the investigation.

c) The right to defend themselves.

d) Access to the case file with the restrictions established by law.
e) The confidentiality of their personal data and preservation of their identity.
f) Confidentiality of the facts and the procedure.
g) Certain cases of exemption and mitigation of the penalty that may apply to the affected persons are recognised if the information is proven to be true.

Cases where exemption applies.

When a person who participated in the commission of the infringement that is the subject matter of the information is the one who reports its existence before being notified of the initiation of the investigation or disciplinary procedure, he or she may be exempt from the relevant administrative penalty provided that he or she meets the following conditions:

a) He or she has ceased to commit the offence at the time of submission of the communication or disclosure and identified, where appropriate, the rest of the persons who have participated in or contributed to it.
b) He or she has cooperated fully, continuously and diligently throughout the entire investigation procedure.
c) He or she has provided truthful and relevant information, means of proof or significant data as evidence of the facts investigated, has not destroyed them or concealed them, or revealed their content to third parties, directly or indirectly.
d) He or she has made reparation for the damage caused that is attributable to him/her

Attenuating circumstances.

When these requirements are not fully met, including partial reparation of the damage, it will be at the discretion of the competent authority, after assessing the degree of contribution to the resolution of the case, to mitigate the penalty that would have applied to the infringement committed, provided that the informant of the disclosure has not previously been disciplined for acts of the same nature that gave rise to the initiation of the procedure.

The mitigation of the penalty may be extended to the rest of the participants in committing the offence, depending on the degree of active collaboration in the clarification of the facts,

identification of other participants and reparation or reduction of the damage caused, assessed by the ruling body.

This will not apply to the infringements set out in Law 15/2007, of 3 July, on the Defence of Competition

XIII. INFORMATION PROCEDURE AND MANAGEMENT.

The administrative body or governing body of the Organisation is responsible for approving this information management procedure. The appointed Internal System Manager will be responsible for its diligent processing.

The life cycle of each communication must be regulated and documented, from its initial communication to its resolution or shelving.

A. Preliminary phase and guiding principles.

1. Identification of internal information channels and those associated with them.

This management procedure applies to information communicated within the framework of the Internal Channel accessible through: www.valorizasm.com.

2. Information on external channels of information to the relevant authorities and, where appropriate, to the institutions, bodies, offices or agencies of the European Union.

- ✓ Information channel on fraud or irregularities affecting European funds of the National Anti-Fraud Coordination Service (SNCA). Ministry of Finance and Civil Service of the Government of Spain.
- ✓ European Anti-Fraud Office (OLAF)
- ✓ Andalusian Office Against Fraud and Corruption
- ✓ Anti-Fraud Office of Catalonia (OAC)
- ✓ Barcelona City Council's Ethics and Good Governance Mailbox;
- ✓ Madrid City Council Municipal Office against Fraud and Corruption.
- ✓ Office for Preventing and Combatting Corruption in the Balearic Islands

3. Guiding principles of the procedure.

Taking into account the possible criminal consequences of the facts that may be communicated through the channel, its management will be aligned with the guiding principles of judicial procedures:

- Documentation: Regardless of the channel, the investigation procedure must be duly documented in writing, without prejudice to certain actions that may be of an oral nature (e.g. interviews with witnesses or the informant him/herself).
- Who drives the investigation: once a communication of facts that indicate a breach or infringement is received, the investigation will depend on the will of the organisation, thus preventing the complainant from misusing the channel.

- Right of challenge: during the investigation, the accused must be allowed at all times to exercise his/her rights of defence.

4. Sending an acknowledgement of receipt of the communication to the informant

Within seven calendar days of receipt of the communication, unless this may jeopardise the confidentiality of the communication or the communication has been made anonymously, an acknowledgement of receipt will be sent to the informant.

5. Communication with the informant.

If necessary, communication may be maintained with the informant (if he/she identifies him/herself) and additional information may be requested.

6. Rights of the affected person.

Any person affected by the information received has the right to be informed of the acts or omissions attributed to him/her, and to be heard at any time. Such communication shall take place in the time and manner deemed appropriate to ensure the successful completion of the investigation.

Furthermore, respect for the presumption of innocence and the honour of the persons concerned and their rights regarding the protection of personal data is guaranteed.

7. Confidentiality.

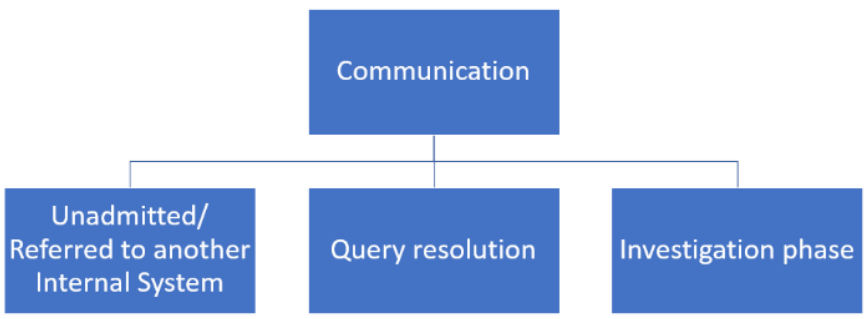
Confidentiality is guaranteed at all times when the communication is sent through reporting channels other than those established or to members of staff not responsible for its processing, who will have been trained in this matter and warned of the classification as a very serious infringement if it is breached and, likewise, of the obligation of the recipient of the communication to send it immediately to the System Manager.

8. Determination of the maximum period for responding to investigation actions.

The time limit for replying to the informant may not exceed three months from receipt of the communication or, if no acknowledgement of receipt has been sent to the informant, three months from the expiry of the seven-day period after the communication has been made, except in particularly complex cases requiring an extension of the period. in which case it may be extended up to a maximum of three additional months.

9. Classification.

The Internal System Manager will analyse and classify the information, identifying several scenarios:



10. Admission, rejection and transfer to other channels.

A communication may be inadmissible on the grounds that it is not relevant, that it is inadmissible or not related to the matters to be communicated through the channel, and therefore the following are grounds for inadmissibility:

a) When the facts reported are not credible.

b) When they do not constitute an infringement of the legal system.

c) When the communication is unfounded.

d) When the information does not contain new and significant information from a previous communication that has already been concluded.

In this case, this will be communicated with a rationale to the informant and the communication will be shelved; additionally and if necessary, the informant may be redirected to the appropriate channel in the event that his/her information does have a place in other spheres of action.

Furthermore, information that may be of interest to the management of the quality system due to reporting possible non-conformities with its procedures and processes may be referred to the relevant department, without prejudice to its transfer to the relevant department of Valoriza.

In the event that the complaint is considered relevant, a communication will be sent to the informant confirming that the case will be investigated.

In both cases, as proof of this due diligence, both in admission and inadmissibility, the reasons that led to the decision will be duly documented.

11. Communication to the accused.

Unless it jeopardises the course of the investigation (given that the complaint has been transferred to the Public Prosecutor's Office or investigation proceedings have been initiated), the accused shall be informed of the communication received, informing him/her of the basic content of the information received, as well as informing him/her of his/her rights.

In the event of a decision not to inform the defendant at the outset, this decision will be documented in writing, stating the reasons for which this decision has been made.

12. Referral to the Public Prosecutor's Office.

The information received shall be immediately forwarded to the Public Prosecutor's Office when the facts may constitute an offence.

In the event that the facts affect the financial interests of the European Union, it will be referred to the European Public Prosecutor's Office.

If it is not clear from the outset, this decision may be postponed until the conclusions of the internal investigation are reached.

B. Investigation phase. Handling the case before a criminal proceeding has been instigated.

The guidelines set out below shall apply to those cases in which, in the absence of open judicial proceedings, an event that may constitute a crime has come to light.

1. Opening of the investigation case.

When it is determined that the facts are sufficient evidence to indicate a possible breach, the relevant internal investigation will be conducted.

The Internal System Manager will in principle be in charge of carrying out the investigation, unless a situation of conflict of interest is detected, in which case the rest of the members of the Compliance Unit will be informed and will make the decision to appoint an alternative person to head the investigation, which may be internal or external.

All departments of the organisation are obliged to provide the necessary collaboration so that the Internal System Manager can carry it out with all the resources he deems appropriate.

The Internal System Manager will open the relevant case, which will include all the incidents that occur in conducting it; it shall be confidential and governed by the provisions of the regulations on the Protection of Personal Data and implementing regulations.

An Investigation Report will be issued with the following minimum content so that it can serve as a starting point for the investigation:

- Details of the communication, including date of receipt.
- Data provided in the communication, including any documentation that may have been provided.
- A first assessment of the content of the communication and the reliability of the informant (if identified).
- Prior analysis of the information, pointing out the most probable hypotheses and those with the highest risk.
- Precautionary measures that are proposed or have been carried out urgently, in the event that the Internal System Manager has considered them necessary to carry out his/her actions and the proper progress of the internal investigation, to prevent any negative consequences or to protect employees (for example, the suspension of employment and pay of the person involved).

In the event that the facts are considered to be of a certain seriousness and urgent reaction or containment measures are necessary, the Investigation Report will be forwarded to senior management so that they are aware of this information and, if appropriate, can take a decision regarding the proposed measures.

Likewise, a prior analysis of the evidence provided will be made available to the accused of the facts so that he/she can claim what he/she deems appropriate in his/her defence, unless at this first instance it is determined that the communication is not appropriate so as not to hinder the investigation or prevent the destruction of evidence.

2. The internal investigation.

The investigation may be carried out by those persons who are determined by the Internal System Manager based on the specific circumstances of each case.

The Regulatory Compliance Unit, with the support of the Board of Directors, will ensure that the investigation has all the necessary resources and that it has access to all the information and documentation, as well as the people who may be related to the case.

Consideration may be given to outsourcing the investigation to external experts in the event that Senior Management, the Compliance Unit or members of the Board of Directors or other relevant positions are affected by the facts under investigation or when from the outset it is evident that the investigation is technically complex.

This decision will be taken by the Internal System Manager, informing the Board of Directors, Senior Management or other relevant positions of this need along with the reasons for said decision.

If the investigation is outsourced, it will be essential for the external expert to report at all times on the progress of the investigation to the Regulatory Compliance Unit, so that it has the necessary information at all times to track its progress.

External experts must in all cases guarantee their compliance with data protection regulations, confidentiality and secrecy of communications. This external party must enter into a data processing contract in accordance with Article 28 of the GDPR.

All legally valid means may be used, including, among others, interviews, the examination of documentation of any kind and in any medium that is understood to be useful for the investigation, retrieval and analysis of the information contained in computer media through the use of software and hardware tools that preserve the integrity of the evidence and the possibility of providing it as a means of evidence in a criminal proceeding.

Only the Regulatory Compliance Unit will be empowered to authorise or decide on the collaboration of external expert advisors or collaborators in the investigation or in the sessions held by the body itself, for which it will weigh the seriousness of the alleged facts or other reasons, such as the appropriateness of greater objectivity and impartiality of the investigation when the action of the Regulatory Compliance Unit has its origin in the announcement of the submission of a lawsuit or complaint.

The Regulatory Compliance Unit will also have the power to authorise the attendance of notaries when deemed appropriate to ensure the validity of the evidence to be obtained as part of the internal investigation.

3. Conclusions.

Once the internal investigation has been completed within the established deadlines, Resolution Minutes will be drawn up with reasoned proposals for action.

In the event that the investigation has been carried out by an external expert, it will be their responsibility to prepare the Resolution Minutes and submit them to the Internal System Manager and the Regulatory Compliance Unit.

The Resolution Minutes must contain at least the following content, so that the investigation is duly documented and is the basis for subsequent decision-making:

- Technical aspects: Title, author, date, purpose, origin, level of confidentiality.
- Background and context of the case and persons or departments under investigation.
- Alternatively, a detailed list of facts, if relevant facts have been detected, the actions taken in order to clarify the facts and the assessment of the evidence carried out and the indications obtained.
- Scope of the investigation and its purpose.
- Actions and aspects analysed, stating the relevant facts investigated and detected.
- List of all the documentation analysed and used.
- Circumstances that may have constrained the conduct of the investigation.
- Conclusions.
- Proposal of measures to be adopted.
- If disciplinary measures are proposed, the infractions will be graded, in accordance with labour law and the collective agreement in force.

4. Adoption of decisions and decision-making based on the conclusions.

In order to demonstrate the impartiality and independence of the investigation process, the final decision on the measures proposed in the Resolution Act will be taken:

(i) By the Director of Human Resources or the competent Governing Bodies, when the final decision or proposed measures affect employees who do not have managerial responsibilities.

(ii) By the Board of Directors when the final decision or proposed measures affect those with the highest levels of responsibility in the organisation or, regardless of the level of responsibility, the facts are likely to affect or have affected to Valoriza's reputation.

In this way, there will also be evidence of their participation and commitment to the process.

If a possible conflict of interest is detected in the members of the decision-making body, due to it affecting their area of responsibility or due to any circumstance that may jeopardise their objectivity or impartiality, they must refrain from participating in the decision-making process, bringing this to the attention of the Regulatory Compliance Unit so that an alternative can be found.

Among the decisions that can be taken are disciplinary action against the implicated employees, which will be established according to the seriousness of the facts and applying the graduation and consequences set out in the Collective Agreement or Workers' Statute. When disciplinary consequences are determined, they must be supervised by the persons with the relevant authority, in particular the HR Department.

In the event that the person under investigation is a third party, such as a supplier, customer or business partner, the measures will be limited to the commercial sphere, for example, the limitation of actions, enhanced diligence or, in serious cases, the unilateral termination of the contractual relationship by the organisation.

5. Incentives.

On the other hand, in contrast to the need to penalise those conducts that involve a breach or a risk of non-compliance or infringement, in order to promote the culture of Compliance in the organisation, senior management may set up a system in order to recognise their contribution with respect to the people who have reported or assisted in the clarification of the facts. In any case, these will consist on cash awards.

6. Follow-up of decisions taken.

After the investigation process is complete and once the decisions deemed appropriate have been made, the Internal System Manager will follow up to ensure that the decisions taken are duly carried out.

The purpose of this follow-up is to check that the measures adopted are being implemented, thus contributing to the continuous improvement of the organisation's management model, and to reinforcing the culture of Compliance.

C. Litigation.

The guidelines set out below shall apply in those cases in which the organisation is or is imminent to be investigated in a criminal proceeding.

In cases where there is a court decision that takes action against the Organisation before notice is formally served in the company's registered office in accordance with the procedure established in arts. 119 and 120 LECrim., the Regulatory Compliance Unit must convene the Senior Management or Governing Bodies as a matter of urgency.

Unless there is a conflict of interest, the Regulatory Compliance Unit will be the body in charge of managing the basic lines of the strategy in the case, as well as all corporate strategies for responding to the criminal proceeding.

Once the criminal proceeding has come to its attention, the Regulatory Compliance Unit will carry out the guidelines defined in the previous section relating to the Internal Investigation.

In any case, the actions carried out will be guided by the principle of compliance with the law in accordance with the requirements that the criminal legal system imposes on legal persons, with the organisation and all its staff collaborating at all times with the relevant authorities in order to better clarify the facts and determine possible criminal responsibilities. This is without prejudice to the disciplinary decisions provided for.

D. Appointment of legal counsel.

The organisation, in accordance with the provisions of arts. 119 and 120 of the Code of Criminal Procedure, shall appoint in due course, as its legal representative in the proceedings, the person who it considers to have the best knowledge in the sphere of crime prevention.

It will also appoint the entity's defence counsel and *procurador* (its representative to the court in the Spanish legal system).

Defence counsel may be allowed to participate in the sessions of the Regulatory Compliance Unit, with the right to speak, but without the right to vote.

Depending on how the criminal procedure develops, the Organisation may change the person acting as its procedural representative, if this is the most appropriate option.

A person who may have procedural conflicts of interest with the entity may never be appointed as the Organisation representative in a legal proceeding, either because he or she is already under investigation in the same proceeding or because there is a possibility that he or she may be investigated in the future or if they turn out to be the legal representative in the proceeding of the natural person(s) allegedly involved in the facts.

XIV. RESOLUTION OF QUERIES.

The Channel may also be used as an internal source for receiving queries regarding regulatory compliance.

The resolution of queries of a general nature raised shall be resolved within a period not exceeding one month.

In the event that an important or significant incident is detected in terms of the volume of queries on a specific topic, the System Manager, or where appropriate the Regulatory Compliance Unit, may recommend awareness-raising or training actions to refresh knowledge of the criminal risks that affect the activity in general.

The Internal System Manager will maintain a repository of frequently asked questions to enrich its system in terms of criminal compliance.

XV. PUBLICITY AND RECORDING OF INFORMATION.

A. Information.

Interested parties shall be provided with adequate information, in a clear and easily accessible manner, on the Internal Information System and the use of the channel, as well as on the essential principles of this management procedure, included for this purpose in the Internal Information System Policy.

As it has a website, this information will appear on the home page, in a separate and easily identifiable section.

B. Recording of Information.

The Organisation has a book of records to compile the information received and the details of the internal investigations to which they have given rise, guaranteeing, in any case, the requirements of confidentiality and protection of personal data.

This book of records shall not be public and only at the reasoned request of the relevant judicial authority, by means of an order, and as part of a legal proceeding and under its supervision, may the contents of the aforementioned book of records be accessed in whole or in part.

Personal data related to the information received and internal investigations will only be kept for the period that is necessary and proportionate and under no circumstances may the data be kept for a period greater than ten years.

The Internal System Manager will be in charge of keeping the record book and its custody. It will be filed together with the open investigation files, implementing high-level security measures, with a key both in the cabinets and on the access door in the case of a physical file and with an access password in the case of a digital file.

The case files will be filed in chronological order, by date of entry.

XVI. REPORTS TO THE BOARD OF DIRECTORS.

In a quarterly basis, the Regulatory Compliance Unit will present a Compliance Report to the Board of Directors, which will contain an analysis of the files processed to date through the Internal Information System, as well as any other issues that the Regulatory Compliance Unit itself considers relevant for knowledge by the Board of Directors.

In this regard, any fact, situation, file, action regarding which there is indication or certainty of affecting the reputation of Valoriza, will be immediately brought to the attention of the President of the Board as well as to the Board of Directors for the appropriate purposes.

In the case the President of the Board or any members of the Board of Directors are involved, the Regulatory Compliance Unit will inform, firstly to the President of the Remuneration, Appointments and Sustainability Committee and, secondly, to the President of the Audit and Risks Committee.

In particular, they will be communicated when the Regulatory Compliance Unit knows, suspects or has reasonable grounds to suspect that these facts, situations, files or actions are related to any crime or misdemeanor classified in the Penal Code or regulations applicable in other jurisdictions.

XVII. DOCUMENTATION AND FILING SYSTEM OF THE ACTION TAKEN.

All the information generated by the communications will be kept in the systems and with the security measures established within the framework of its data protection management system, for the retention periods that may be determined internally in application of the

applicable principles on personal data protection or during the periods from which, by law, responsibilities could arise as a result of the actions investigated.

Next, the retention periods are established according to the classification of the communications received, including the need to keep them in anonymised form in the systems once the processing of the personal data that may include such communications is no longer relevant.

Furthermore, in the event that the information has to be kept for a long period of time, the possibility of keeping the information blocked and only accessible to the Internal System Manager and the Regulatory Compliance Unit may be examined.

Classification		**Retention period**	**Anonymisation of personal data**	**Need for Blocking**
Consultations		Indefinite, as a knowledge repository	YES (sender ID is not considered relevant)	N/A
Non-admission		3 months (unless the purpose of the storage is to provide evidence of the operation of the system)	YES (communications that have not been processed may only be recorded in anonymised form)	N/A
Referral to other Channels		3 months		
Investigation Cases	Investigation shelved with no consequences	3 months once the case is closed	Not applicable (identification of the data subjects is relevant and indispensable)	YES
	Investigation with identification of a possible breach or unlawful act	As long as personal or company responsibilities may arise. In no case may the data ever be retained for a period longer than ten years.	Not applicable (identification of the data subjects is relevant and indispensable)	YES

XVIII. PROTECTION OF PERSONAL DATA.

A. Legal regime for the processing of personal data and lawfulness of the processing.

The processing of personal data arising from the management of these communications will be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), Spanish Organic Law 3/2018 of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), in 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 the enforcement of criminal sentences and in Law 2/2023.

The legitimate basis for the processing of personal data in this context will be governed by the following provisions:

- ✓ It is permissible to create and maintain an information system through which the Organisation can be informed, even anonymously, of the commission within it or in the actions of third parties contracting with it, of acts or conduct that may be contrary to the general or sectoral regulations that apply to it.
- ✓ The processing of data necessary to ensure the protection of persons who report regulatory breaches is lawful. Data may be processed for the purposes of prevention, detection, investigation and prosecution of criminal offences and the enforcement of criminal sentences.
- ✓ The processing of data in internal channels will be carried out on the basis of the legal obligation of article 6.1.c of the GDPR when the organisation is obliged by Law 2/2023 to set up an internal channel.
- ✓ If it is not mandatory, it is presumed to be protected by the legitimate interest of Article 6.1.e of the GDPR. The processing of special categories of personal data for reasons of an essential public interest may be carried out in accordance with the provisions of Article 9.2.g) of the GDPR.

B. Duty to provide information and exercise of rights.

- ✓ Employees and third parties must be informed about the existence of these information systems.
- ✓ The person to whom the facts relate shall under no circumstances be informed of the informant's identity.
- ✓ Data subjects may exercise the rights referred to in Articles 15 to 22 of the GDPR, through the Organisation's data protection channel.
- ✓ In the event that the person to whom the facts related in the communication relate exercises the right to object, it will be presumed that, in the absence of proof to the contrary, there are compelling legitimate grounds that legitimise the processing of their personal data.

C. Access to data.

Access to the data contained in these systems will be limited exclusively to:

- ✓ The Internal System Manager and whoever manages it directly.
- ✓ The human resources officer or the duly designated competent body, only when disciplinary measures could be taken against an employee. In the case of public employees, the competent body for processing the case.
- ✓ The person in charge of the legal services of the entity or body, if it is appropriate to take legal action in relation to the facts reported in the communication.
- ✓ The data processors that may be appointed.
- ✓ The Data Protection Officer.

However, it will be lawful for other persons to access the data, or even to disclose them to third parties, when it is necessary for taking disciplinary measures or for the processing of the legal proceedings that may be appropriate.

Without prejudice to the reporting to the relevant authority of facts constituting a criminal or administrative offence, only when disciplinary measures could be taken against a worker, such access shall be allowed to personnel with human resources management and control functions.

The necessary measures must be taken to preserve the identity and ensure the confidentiality of the data in respect of the persons affected by the information provided, in particular that of the person who brought the facts to the attention of the entity, if he or she identified him/herself.

Personal data that is not manifestly relevant for the processing of specific information will not be collected or, if collected by accident, will be deleted without undue delay.

All data that may have been reported and that refer to conduct that is not included in Law 2/2023 shall be deleted.

The data of the person making the communication and of the employees and third parties must be kept in the complaints system only for the time necessary to decide on the appropriateness of initiating an investigation into the facts reported.

Once the existence of untruthful information has been proven, it will be immediately deleted, unless such veracity may entail a criminal offence, in which case it may be kept while the legal proceeding is in progress.

If the information received contains personal data included in the special data categories, it will be immediately deleted, without being recorded and processed, unless such information is an essential part of the reason for the complaint.

In any case, if three months have elapsed since the communication was received and no investigation proceedings have been initiated, it must be deleted, unless the purpose of the retention is to provide evidence of the operation of the Internal Information System.

Complaints that have not been dealt with may only be recorded anonymously; the blocking obligation provided for in article 32 of the LOPDGDD shall not apply.

After the expiry of the period mentioned in the previous paragraph, the data may continue to be processed by the body responsible for the investigation of the reported facts, and may not be kept in the internal complaints information system itself.

Employees and third parties must be informed about the processing of personal data within the framework of the Internal Information System.

D. Protection of the informant's identity.

The following must be taken into account:

- ✓ Anyone who submits a communication or makes a public disclosure has the right not to have his or her identity disclosed to third parties.
- ✓ No data will be obtained that would allow the identification of the informant. The System, and in particular the reporting channel, shall have appropriate technical and organisational

security measures in place to preserve the identity and guarantee the confidentiality of the data relating to the persons concerned and to any third party mentioned in the information provided, especially the identity of the informant if he/she has been identified.

- ✓ The identity of the informant may only be communicated to the judicial authority, the Public Prosecutor's Office or the relevant administrative authority in the context of a criminal, disciplinary or punitive investigation.

The Internal System Manager shall ensure that these requirements are met.

XIX. APPROVAL AND ENTRY INTO FORCE.

This procedure is approved by the Board of Directors of VALORIZA SERVICIOS MEDIOAMBIENTALES, S.A. on 20 March 2024, this being its first version to take effect.

The procedure is effective upon its approval and is suitably disseminated through the VALORIZA Group's usual communication channels and is regularly updated in accordance with regulatory changes or structural changes of the Group or the introduction of improvements arising from the reviews of the Corporate Governance System or the Compliance Model. The latest version of it can be found at www.valorizasm.com

In the event of any discrepancy between the translation of this Code into other languages and its original Spanish version, the latter shall prevail.

Versions record:

DATE	EDITION	REVISION	RESPONSIBLE PARTY	CHANGES DESCRIPTION
29 November 2023	V1	Changes.	Regulatory Compliance Unit	Initial draft.
06 February 2024	V2	Changes.	Regulatory Compliance Unit	Draft V2.
06 March 2024	V3	Board Approval.	Regulatory Compliance Unit	Board Approval version.
20 March 2024	V4	Board Approval.	Board	Board Approval.