INTERNAL REPORTING SYSTEM COMMUNICATIONS MANAGEMENT PROCEDURE

Onyx CenterSource

2023

CONTENTS

1. INTRODUCTION

Following approval of Act 2/2023, of 20 February 2023, governing the protection of persons reporting regulatory breaches and the fight against corruption (hereinafter, "Act 2/2023"), the legislation transposing into Spanish law Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, the purpose of which is to strengthen the culture of reporting as a means of preventing and detecting threats to the public interest, there is now an obligation on the part of certain natural or legal persons to have in place an internal reporting system (hereinafter, the "Internal Reporting System").

Pursuant the above, the Onyx Group, comprising Pegasus Business Intelligence, LP, Onyx CenterSource Spain, S.A. ("Onyx Spain"), Onyx CenterSource AS ("Onyx AS") and Onyx CenterSource Limited ("Onyx UK") (hereinafter, "Onyx Group"), in order to undertake its professional activities in accordance with the legal regulations in force, hereby implements the necessary measures to put in place an internal reporting system in accordance with the provisions of Act 2/2023.

2. PURPOSE

The purpose of implementing the Internal Reporting System is to:

a) Adapt the existing system to channel communications with regard to illegal or irregular practices that have been or could be committed within the context of the Onyx Group.

b) Protect individuals who detect serious or very serious criminal or administrative violations of European Union Law from reprisals within an occupational or professional context and report them by means of the mechanisms established therein.

c) Provide the Onyx Group with a measure of control over its own activity.

d) Detect in advance and identify activities which could provide a context for the perpetration of those violations that the organisation aims to avoid.

e) Enable the imposition of penalties against the perpetrators of the conduct reported, in those cases where this would be appropriate.

f) Allow the Onyx Group to inform the authorities of violations detected via the Internal Reporting Channel.

g) Contribute to the continuous improvement of internal reporting processes for

the management and control of activity carried out in the organisation.

h) Strengthen the Onyx Group's culture of information, the organisation's structural integrity, and promote a culture of information and communication as a mechanism to detect and prevent threats to the public interest. .

3. SCOPE OF APPLICATION

The procedure for the administration of communications within the Internal Reporting System (hereinafter, the "Procedure") applies to all companies of the Onyx Group. The governing body of Onyx Spain, as the entity directly subject to Act 2/2023, shall reach the relevant decisions in order to incorporate the provisions of this Procedure, by adapting the governance framework in accordance with the principle of proportionality, in line with the particularities of its structure of governing bodies, committees and departments, while aligning their operational principles, methodologies and processes with the terms of this document.

The Internal Reporting System may be used by the following persons belonging or related to the Onyx Group:

- Employees.
- Independent contractors.
- Shareholders and directors.
- Executive personnel.
- Any person working for or under the supervision and management of contractors, subcontractors and suppliers.
- Whistleblowers communicating or publicly disclosing information as to violations learned of within the context of an occupational or statutory relationship which has already ended.
- Volunteers.
- Interns.
- Workers on training schemes, whether or not they receive remuneration, and those whose occupational relationship has not yet begun, in those cases where information as to the Violations was obtained during the process of selection or pre-contractual negotiation.

Each of them shall hereinafter be referred to as a "Whistleblower", and collectively as the "Whistleblowers".

Whistleblowers may issue communications as to the conduct indicated below (hereinafter, "Violation" or "Violations"):

1. Any of the actions or omissions that could constitute violations of European Union Law wherever they would:

   1.º Fall within the scope of application of European Union acts listed in the annex to EU Directive 2019/1937 of the European Parliament and Council Assembly of October 23, 2019, concerning the protection of individuals who report breaches of European Union law, irrespective of the classification given to them under domestic legal systems;

   2.º Affect the financial interests of the European Union as defined in Article 325 of the Treaty on the Functioning of the EU, (herein referred to as the "TFEU"); or

   3.º Affect the internal market, as defined in Article 26, paragraph 2 of the TFEU, including breaches of European Union rules on competition and state aid, as well as violations related to the internal market concerning acts that contravene corporate tax regulations or involve practices aiming to gain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

2. Actions or omissions which could constitute a criminal offence or serious or very serious administrative infringement.

Under no circumstances may the Internal Reporting Channel be used to report:

- Routine occupational problems (e.g., in connection with days of holiday, salary, performance reviews, etc.); this type of matter must be addressed with the departmental manager of the person affected, or where applicable, with the Human Resources Department.

- Information related to claims involving private disputes or that solely pertain to the whistleblower and the individuals referred to in the report.

- False, distorted, or implausible information, or any that was unlawfully obtained.

- Information that is already entirely available to the public or that which constitutes mere rumors.

- Information referring to actions or omissions not covered within the “scope of application”.

Such actions shall be excluded from protection against reprisals.

4. POLICY ON INTERNAL REPORTING SYSTEM AND WHISTLEBLOWER PROTECTION

This policy is based on the following pillars:

a) It allows Whistleblowers to report any information as to those Violations set out in the above subsection.

b) It is designed, established and managed in a secure manner, thereby ensuring the confidentiality of the identity of the Whistleblower and of any third party mentioned in the communication, and any actions which may take place in the handling and administration thereof, in addition to data protection, preventing access by unauthorised personnel.

c) It allows the presentation of written or verbal communications, or both.

d) It allows the presentation of anonymous communications.

e) It incorporates any different internal reporting channels that have been or may be established within the organisation.

f) It ensures that the communications presented are processed effectively within the Onyx Group, the aim being that the Organisation itself should be the first to learn of any possible irregularity.

g) A System Manager has been put in place.

h) Provision is made in order appropriately to inform members of the Organisation of the existence and principles of the Internal Reporting System, the guarantees established for the protection and defence of Whistleblowers, and the communication channels established for this purpose.

i) It has a procedure in place for the management of the reports received.

j) It establishes guarantees to protect Whistleblowers within the context of the Organisation itself.

Likewise, any natural person may use the external reporting channel of the Independent Whistleblower Protection Authority (AAI) governed by Act 2/2023, or of any corresponding regional authorities or bodies that may likewise have established a general reporting channel, or any other national or European public body that has a specific channel to report the perpetration of Violations.

5. SYSTEM MANAGER

The Internal Reporting System Manager is designated by the Governing Body of Onyx Spain, and only this Body shall have the authority to decide on their removal or termination. Both the appointment and termination of the System Manager must be communicated to the A.A.I., or where applicable, to the relevant authorities or bodies of the autonomous communities within their respective jurisdictions, within ten business days. In the event of termination, the justifications for such action must be specified.

He/she will undertake his/her functions independently and autonomously with regard to other bodies of the Onyx Group, will not receive instructions of any kind in the pursuit thereof, and will have access to all human and material resources needed in order to fulfil them. He/she will likewise have the professionalism, knowledge and experience required in order properly to perform the assigned function.

The functions and responsibilities of the Internal Reporting System Manager are in general as follows:

- Participate in the implementation of the IRS and in the generation of the relevant documentation.

- Ensure the application of appropriate procedures and controls, and oversee fulfilment of the IRS, and in particular of this document.

- Handle the processing of information received through the Internal Reporting System.

- Organise and administer appropriate training for those Whistleblowers belonging to the Organisation with regard to the IRS and be available for them to raise any questions and queries they may see fit. Such Whistleblowers will thus be informed of the existing possibilities to submit communications on the terms established herein.

- Wherever possible, inform the Organisation as to significant legal changes connected with the IRS.

- Directly or through the corresponding outsourcing process, administer any communications received via the Internal Reporting Channel, or any other mechanism established for this purpose.

- Safeguard the documentation comprising the IRS.

- Safeguard the record book of communications received and any resulting internal investigations.

- In any event, the Internal Reporting System Manager will process the information and documentation obtained in absolute confidence and may not use it for any purpose other than that determined by his/her responsibilities and functions.

6. INTERNAL REPORTING CHANNEL

A completely confidential Internal Reporting Channel is set up, available to all Whistleblowers.

In order properly to administer the communications received, they must contain the necessary data to allow an analysis of the events communicated, and must:

- Contain an explanation of the events.

- Identify the person(s) involved in the behaviour communicated, or with knowledge thereof.

- Indicate the moment when the event occurred or was occurring.

- If deemed necessary, provide documents, files or other information seen as relevant for the appraisal and resolution of the communication.

- Provide a means of contact to request any further information, except in the case of anonymous communications.

- The greater the information provided about the specific situation, the greater the operational capacity to handle the communication.

The following means are provided to enable the presentation of information with regard to the violations set out in the previous subsections:

- Presentation of communication via the communications inbox set up on the Company website. In this case, the System Manager will send a receipt of acknowledgement to the Whistleblower within a maximum period of 7 calendar days of receiving the information, unless doing so may jeopardize the confidentiality of the report.

- Presentation of the communication to the Internal Reporting System Manager in person, by means of an appointment to be arranged within a maximum period of 7 calendar days of the corresponding request by the Whistleblower. During this meeting, a receipt of acknowledgement of the information provided to the System Manager will be handed to the Whistleblower.

Verbal communications will be documented in any of the following forms, with the prior consent of the Whistleblower:

- by means of a telephone call, using a secure, lasting and accessible format, or

- through a complete and precise transcription of the conversation conducted by the personnel responsible for dealing with the matter. The Whistleblower will be given the opportunity to sign in confirmation, rectification and acceptance of the aforementioned transcription.

Any of the preceding mechanisms ensures lasting storage of the information conveyed.

Communication may be conducted with the identification details of the Whistleblower, or anonymously.

- **Communication with identification of the Whistleblower:**
  If the Whistleblower decides to send the communication with contact details, the Investigating Committee may contact him/her for further information, if necessary. When the communication is sent, the Whistleblower may indicate a postal address, email address or secure location to receive notifications.

- **Anonymous communication:**
  If the Whistleblower decides to send the communication anonymously, he/she must retain the codes generated by the application enabled for this purpose. In such cases, these codes are the only way of tracking the communication and checking whether the Investigating Committee requires additional information.

It is important to emphasise that any additional information that might be required by the Investigating Committee is necessary in order properly to administer the communication and

prevent the case from being shelved because of a lack of information.

The Internal Reporting Channel is a two-way process with regard to individuals. In other words, workers can report other workers, their line managers, executives and members of the governing body; and line managers, members of the governing body and executives may report other workers and their managerial peers.

The Internal Reporting System incorporates the different internal reporting channels already established at the Organisation, or any that might be established in the future. As a consequence of the above, communications regarding the material context of the Internal Reporting System as provided in the internal protocols already implemented may be sent via the means provided for within the Reporting Channel established in this subsection.

Whistleblowers may likewise use the external reporting channel of the Independent Whistleblower Protection Authority (AAI) governed by Act 2/2023, or of any corresponding regional authorities or bodies that may likewise have established a general reporting channel, or any other national or European public body that has a specific channel to report the perpetration of Violations.

7. OPERATIONAL PROTOCOL IN RESPONSE TO A REPORT

7.1 Persons responsible for the investigation (Investigating Committee)

The System Manager will be responsible for handling communications and will, where applicable, take on the role of the Investigating Committee for the communication. He/she may likewise appoint other individuals belonging to the Organisation to join the Committee, for organisational reasons.

Depending on the circumstances, complexity and/or nature of the communication, the Investigating Committee may comprise one or several members. In the latter case, one of them will serve as case investigator, receiving support from the other members of the Committee.

The case investigator, who will act by delegation and with the authority of the Investigating Committee, if this is not a single-person body, will have the role of gathering all necessary information about the case for proper investigation, which must be undertaken with the utmost speed, confidentiality, secrecy and participation of all those involved.

Members of the Investigating Committee who have any kind of conflict of interest, incompatibility or any other cause affecting their impartiality (family or personal relationship, clear enmity, direct or indirect interest, etc.), shall be removed from the Committee.

In any event, the members of the Investigating Committee must sign a non-disclosure agreement when they are appointed.

7.2 Phases of the investigation

The procedure will be undertaken within a maximum of 3 months of receipt of the communication, except in cases of particular complexity requiring an extended period, in which case the term may be extended by a maximum of a further three months.

Communications may be rejected from processing for reasons including the following:

- If the events recounted lack all credibility.

- If the events recounted do not constitute a Violation of European Union law or a serious or very serious criminal or administrative offense.

- If the communication clearly lacks any basis, or in the judgment of the Investigating Committee, there is reasonable evidence that the information was obtained by committing an offence. In this last case, aside from rejecting the communication, the Investigating Committee may suggest that the Governing Body inform the State Prosecution Service of any acts that they believe could constitute an offence.

- If the communication does not contain new and significant information about Violations in comparison with a prior communication concerning which the corresponding procedures have been concluded, unless new factual or legal circumstances arise that would justify a different continuation of the case.

If the communication is not admitted for processing, the Investigating Committee will issue a brief Conclusions Report, explaining the rejection of the communication, of which the Whistleblower will be informed. The communication will be archived in the register book of communications, irrespective of any actions that the Whistleblower may take in other spheres.

Once the investigation is concluded:

a) If the conclusion ultimately reached is that the events do not constitute a Violation of European Union law or a serious or very serious criminal or administrative offense, a Conclusion Report will be drawn up indicating this circumstance. Immediately thereafter, the communication will be archived in the communications register book.

b) If the events could constitute Violations, a Conclusions Report will be drawn up, in which the Investigating Committee may include any measures that it suggests the Organisation should adopt, both in connection with the events that have already occurred, and to prevent any future repeat. If this is approved, the matter will be

monitored until the outcome is validated and the case closed. Immediately thereafter, the communication will be archived in the communications register book.

Additionally, the information will be immediately forwarded to the Public Prosecution Office when the report may constitute a criminal offense. In cases where the report may impact the financial interests of the European Union, the information will be sent to the European Prosecutor's Office.

8. RIGHTS OF THE PERSON AFFECTED

Those persons referred to in the events recounted in the communication must be granted particular protection, to address the risk that although the information may apparently seem plausible, it may have been manipulated, be false, or be derived from legally unacceptable motives. Such individuals maintain all their rights of legal protection, defence, dignity, access to the case record, confidentiality, identity protection, and the presumption of innocence.

The right of the person concerned to be informed of the actions or omissions attributed to them, and to be heard at any time, is guaranteed. They will furthermore be informed of their right to submit written allegations and the processing of their personal data. Nonetheless, this information may be provided at the hearing if it is felt that prior presentation could facilitate the concealment, destruction or alteration of the evidence. Under no circumstances will the identity of the Whistleblower be disclosed to the affected parties, nor will they be given access to the communication.

Notwithstanding the right to submit written arguments, the investigation will, wherever possible, include an interview with the person affected, at which they will, with absolute respect for the presumption of innocence, be invited to set out their version of the events and to provide any evidence they may deem appropriate and relevant.

In order to guarantee the right of defence of the person affected, they will have access to the case file, without disclosing information that could identify the Whistleblower, and have the right to be heard at any time, being advised of the possibility of attending with a lawyer.

9. RECORD OF REPORTS

The Onyx Group has a record book of reports received and the resulting internal investigations, ensuring in all cases the requirements of confidentiality set forth in Act 2/2023, of 20 February 2023, governing the protection of persons reporting regulatory violations, and the fight against corruption.

This record will not be public, the contents of the aforementioned record being accessible in whole or in part only at the reasoned request of a competent court authority, by means of a ruling issued within the context of court proceedings, and under the protection of the court.

Personal data regarding the reports received and internal investigations will be stored only for the necessary and proportionate period in accordance with the terms set forth in this document. Under no circumstances may data be stored for more than 10 years.

10. MEASURES TO PROTECT THE WHISTLEBLOWER AND PROHIBIT RETALIATION

10.1 Protective measures

Those communicating or disclosing Violations will be entitled to protection as long as the following circumstances apply:

a) They have reasonable grounds to believe that the report submitted is accurate, at the time when it was communicated or disclosed, even if they do not provide conclusive evidence, and that the report falls within the objective scope of application of this document.

b) The communication or disclosure was made in accordance with the requirements set forth in the Act 2/2023.

An explicit exclusion from protection applies to those communicating or disclosing:

- Information contained in communications that have been rejected under the terms of this document.
- Information connected with claims concerning interpersonal disputes or those affecting solely the Whistleblower and the persons to whom the communication or disclosure refers.
- Information that is already fully available to the public, or would constitute mere rumour.
- Information referring to actions or omissions not covered by the objective scope of application.

Those communicating or publicly disclosing information anonymously as to actions or omissions covered by the objective scope of application, but who are subsequently identified, will be entitled to the protection set out in the document, if they fulfil the conditions established therein.

10.2 Prohibition of retaliation

The Onyx Group explicitly prohibits any acts that would constitute retaliation, including threats and attempts at retaliation against those submitting a communication in accordance with the terms of this document.

Any conduct that could be categorised as retaliation and that is taken within two years of the completion of the investigations will be declared null and void.

Retaliation should be understood as any actions or omissions that are unlawful, or that directly or indirectly entail unfavourable treatment placing the victims thereof at a particular disadvantage compared with another in an occupational or professional context, simply because of their status as Whistleblowers or because of the disclosure they made public.

For the purposes provided in this document, retaliation is understood to include, but not be limited to acts involving:

a) Suspension of employment contract, dismissal or termination of the occupational or statutory relationship, including non-renewal or early termination of a temporary employment contract once the trial period has ended, or premature termination or cancellation of goods or service contracts, imposition of any disciplinary measure, demotion or refusal of promotion and any other substantial modification of working conditions, or failure to convert a temporary employment contract into a permanent contract, if the worker had legitimate expectations that they would be offered a permanent post; unless these measures are conducted within the regular application of managerial authority protected by employment law or the legislation governing the corresponding public employee statute, as a result of proven circumstances, acts or violations unconnected with the communication submitted.

b) Harmful acts, including those involving reputation, economic loss, coercion, intimidation, harassment or ostracism.

c) Negative appraisal or references with regard to occupational or professional performance.

d) Inclusion on blacklists or distribution of information within a particular sectoral scope, that would hamper or prevent access to employment or works or service contracts.

e) Denial or cancellation of leave or leave of absence.

f) Denial of training.

g) Discrimination or unfavourable or unfair treatment.

11. DISSEMINATION, PUBLICITY AND VALIDITY OF THE INTERNAL REPORTING SYSTEM

In order properly to fulfil the provisions of the legislation in force, and for the proper implementation of the Internal Reporting System, effective provision is made to inform Whistleblowers of the existence and principles of the Internal Reporting System, the guarantees established for the protection and defence of Whistleblowers, and the communication channels enabled for this purpose.

Whistleblowers may in any event consult any query concerning the IRS with the System Manager, who will be available to them at all times.

All matters or issues not explicitly covered by this document will be subject to the provisions of Act 2/2023, of 20 February 2023, governing the protection of those reporting regulatory breaches, and the fight against corruption.