INTERNAL INFORMATION SYSTEM POLICY

1. INTRODUCTION

Law 2/2023, dated 20 February, regulates the protection of individuals who report on regulatory offences and cases of corruption. This law, which transposes Directive (EU) 2019/1937 of the European Parliament and Council, dated 23 October 2019, on the protection of persons who report breaches of European Union law, recognizes the importance of the collaboration of citizens for legal efficacy.

Law 2/2023 applies to both the public and private spheres and is fundamentally intended to protect persons who report on the actions or omissions listed in its Article 2 from potential reprisals. The law states two kinds of information systems that citizens can use to report in confidential and anonymous conditions:

A) An internal system: this is the preferred channel to report the actions or omissions set forth in the law, provided that the breach can be dealt with effectively by internal methods. It is preferable for the organization to be aware of irregular conduct so it can correct or reduce potential harm as quickly as possible.

b) An external system: this provides citizens with a channel of communication through a specialised public service such as the Independent Whistleblower Protection Authority (IWPA) or similar regional agencies. This may generate greater confidence in whistleblowers, given that it dissipates the fear of reprisals from their immediate environment.

Nonetheless, the choice of system will depend on the whistleblower, their circumstances and the risk of potential reprisals.

The policy presented in this document meets the provisions of Article 5.2 h) of Law 2/2023, which require the implementation of a strategy or policy that sets forth the general principles.

The regulations defined in this document describe the rules and principles that govern the Orbinox Group Whistleblower Channel. These regulations will be valid for all reports made by persons associated with the Group, as well as for claims or queries sent by third parties through the form provided by the company for that purpose.

2. PURPOSE

The Internal Information System implemented by the Orbinox Group has two purposes:

a) To protect persons who notice and report regulatory offences and corruption (whistleblowers) within their work or professional environment, as well as the persons involved in the events that are reported.

b) To encourage a corporate environment where information and communication in the organization serve as a means to detect and prevent threats to the public interest.

3. PRINCIPLES

To guarantee system efficiency, the Orbinox Group will ensure that it complies with all the requirements set forth in Law 2/2023, dated 20 February, which regulates the protection of persons who report on

regulatory offences and corruption. This includes the following:

3.1. Accessibility

The Internal Information System must allow all the individuals within its sphere of application to report on regulatory offences and corruption.

3.2. Independence

The company's Internal Information System must be independent and clearly differentiated from other Orbinox Group reporting systems, as well as other associated agencies and bodies. Moreover, the system manager must be fully independent and free of interference from other Orbinox Group bodies.

3.3. Independence of the System Manager

The Orbinox Group shall guarantee full independence of the System Manager and therefore ensure the following:

- Objectivity and impartiality: the reports will be examined objectively and without bias, ensuring that the evidence is taken into account fairly.
- Prevention of conflicts of interest: situations where conflicts of interest may arise and therefore compromise the impartial nature of the report examination process shall be avoided.
- Presumption of innocence: the principle that states that a person must be considered innocent until found guilty shall be adhered to and none of the individuals mentioned in the report shall be judged in advance.
- Right to defence: all parties involved shall be guaranteed the opportunity to defend themselves and present their version of the events in the report examination process.
- Thoroughness: the system shall ensure that all information that is meaningful is collected and examined.
- Integrity: the integrity of the information collected shall be preserved.
- Confidentiality: the information shall be kept secret and the identity of the whistleblower shall be protected.
- Prohibition of unauthorised access: unauthorised persons shall not be granted access to the information.
- Long-standing storage of the information: preservation of the information over time shall be ensured.
- Full protection of the whistleblower: the whistleblower shall be guaranteed protection from reprisals or harm.
- Good faith: all interactions associated with the report or report processing shall be fair and ethical.

3.4. Confidentiality

The company guarantees the confidentiality of the whistleblower's identity and of any other person mentioned in the report, as well as the measures taken during handling and processing of the report. The internal information channel will also allow the submission and processing of anonymous reports.

3.5. Personal data protection

The Orbinox Group Information System shall be characterised by its strict standards of personal data protection, in compliance with current regulations. This involves the following features:

- Confidentiality: all the information and personal data provided through the whistleblower channel shall be considered confidential and will only be known by authorised personnel who must manage and find a solution for the situation reported.
- Consent: the personal data shall only be collected and processed with the explicit consent of the whistleblower, except where the law allows other processing based on another legitimate cause.
- Security: appropriate and secure technical and organizational measures shall be taken to protect the personal data from unauthorised access, disclosure, modification or destruction.
- Rights of the interested parties: the rights of the interested parties over their personal data shall be enforced and exercised in accordance with applicable data protection regulations.

3.6. Ensuring report secrecy

The Information System shall ensure the secrecy of the reports and that all interactions through the system are secure and private. This includes:

- Reporting security: all reports made through the channel shall be encrypted and protected against interception or unauthorised access.
- Restricted access: only duly qualified authorised personnel shall have access to the reports and their associated information, which they shall maintain in utmost secrecy.
- Secure storage: records of the reports shall be stored securely and only for the time required to manage and find a solution for the report, in accordance with Orbinox Group data safekeeping policies.

3.7. Adhering to the presumption of innocence and honour of the persons involved

The Orbinox Group commits to enforcing the presumption of innocence and honour of all the individuals mentioned in the reports to ensure fair and equal treatment. This involves the following features:

- Presumption of innocence: all the persons affected by a report shall be considered innocent until they are proven guilty by a fair and objective investigation.
- Impartial treatment; the reports shall be investigated from a viewpoint that is impartial and free of prejudice, thereby ensuring that all the parties involved have the opportunity to submit their version of the events.
- Protection of honour: measures shall be taken to protect the reputation and honour of the affected individuals, including prevention of unnecessary disclosure of information and restricting knowledge of the report and its details to those persons who are strictly necessary to reach a solution.
- Transparency and communication: communication with the parties involved shall be transparent and they will be informed about the status and result of the investigation while ensuring that the process remains confidential and sound.

4. INTERNAL INFORMATION SYSTEM MANAGER

As set forth in Article 5.1 of Law 2/2023, dated 20 February, the Orbinox Group management body is in charge of implementing the Internal Information System and processing personal data. It also has the authority to name, dismiss or fire the System Manager.

The Internal Information System Manager must be a collective body or an individual, as stated in Article 8 of Law 2/2023. The body assigned as the System Manager by the management body is the Persons Committee.

The System Manager is in charge of meticulous management of the Internal Information System and dealing appropriately with the corresponding reports.

As stated in Article 8.4 of Law 2/2023, dated 20 February, the System Manager "shall perform its functions independently and free from interference from the rest of the bodies belonging to the organization or company; it cannot receive instructions of any kind when exercising its duties and must have all the personal and material means at its disposal to perform the latter".

As stated in Article 8.3 of Law 2/2023, the Orbinox Group management body shall inform the Independent Whistleblower Protection Authority of the appointment of the Orbinox Group Internal Information System Manager within ten days after the appointment. The Manager's dismissal or resignation and the underlying reasons thereof shall also be notified within the same period.

5. CREATION OF THE INTERNAL INFORMATION SYSTEM

The Orbinox Group has created an internal information system to receive information about actions or omissions that may be serious or very serious criminal or administrative offences or other transgressions set forth in Article 2 of Law 2/2023.

The channel is managed by the Internal Information System Manager.

The internal information channel must have the technical capacity to safeguard the confidential nature of the whistleblower's identity or ensure their anonymity, with the aim of protecting the whistleblower from leaks and potential subsequent reprisals.

6. SUBJECTIVE SCOPE

The purpose of the Orbinox Group Internal Information System is to receive and process information that refers to actions or omissions set forth in Article 2 of Law 2/2023, dated 20 February, which regulates the protection of persons who report breaches of regulations and cases of corruption.

As set forth in Article 3 of Law 2/2023, dated 20 February, this includes the following categories of individuals:

a) All Orbinox Group employees

b) Self-employed professionals, suppliers, contractors, subcontractors and other third parties that have or have had a business or professional relationship with the Orbinox Group, which also includes individuals who work for them or are under their supervision or management.

c) People with a working or statutory relationship with the Orbinox Group that has ended, volunteers, interns, apprentices and persons in training programs, regardless of whether they receive payment or not. This also applies to persons who participate in personnel screening processes, provided the information about the offence has been obtained during the screening process or negotiation prior to hiring.

The protection measures set forth in Heading VII of the Law shall also apply specifically to the legal representatives of workers while performing their whistleblower counselling and assistance duties.

7. MATERIAL SCOPE

As regards the purpose of the information, Law 27/2023 indicates that the internal information channel can be used to report serious improper conduct or alleged corruption; it follows that these may constitute serious or very serious criminal or administrative offences associated with Orbinox Group activities that the whistleblower has witnessed or that they have received information about while working for the Orbinox Group or during their professional relationship with any Orbinox Group company.

Law 2/2023 and Directive (EU) 2019/1937 list the following examples of this kind of information:

1. Offences included in the scope of application listed by the European Union in the annex of the aforementioned Directive, associated with the following:

- Public contracts
- Financial services, products and markets, prevention of money-laundering and financing of terrorism
- Product safety and conformity
- Transport safety
- Environmental protection
- Protection against radiation and nuclear safety
- Food and feed safety, animal health and well-being
- Public health
- Consumer protection
- Privacy and personal data protection and computer network and information systems security

2. Actions or omissions that may be offences against European Union law, provided they affect the financial interests of the European Union as set forth in Article 325 of the Treaty on the Functioning of the European Union (TFEU)

3. Offences that affect the internal market, as stated in Article 26, Section 2 of the TFEU, including breaches of European Union regulations concerning competition and aid granted by States, as well as breaches of the internal market concerning corporate tax legislation or steps taken to obtain tax benefits contrary to the purpose of applicable corporate tax laws.

4. Actions or omissions that may be serious or very serious criminal or administrative offences. This shall include all serious or very serious criminal or administrative offences that involve subversion of the National Treasury or Social Security.

5. Labour law offences against occupational health and safety reported by workers regardless of the specific regulations that correspond

8. PERSONAL DATA PROTECTION

Processing of personal data derived from the application of Law 2/2023 will be subject to the provisions set forth in the General Data Protection Regulation (RGPD) and Organic Law 3/2018, dated 5 December, on Personal Data Protection and guarantee of digital rights (LOPDPGDD).

The Internal Information System must guarantee protection against unauthorised access. It must also preserve the identity and confidentiality of the data of the persons involved, as well as those of any third party mentioned in the report, especially the identity of the whistleblower, if it is known. The identity of the whistleblower may only be revealed to a judicial authority, the Public Prosecutor or competent administrative authority within the context of a criminal, disciplinary or punitive proceeding and shall be

provided with the safeguards set forth in applicable regulations.

If the information that is received includes categories of personal data that are subject to special protection, these shall be eliminated immediately, unless processing is necessary for reasons of public interest, as defined in Article 9.2.g) of the RGPD and Article 30.5 of Law 2/2023.

Personal data that have not been clearly proven to be significant for processing specific information shall not be collected; however, if they are collected by mistake, they shall be eliminated at once.

Reports that have not been considered for examination shall only appear as anonymous and are not subject to the restriction set forth in Article 32 of the LOPDPGDD.

9. PROTECTION MEASURES

Prohibition of reprisals

Acts of reprisal are explicitly forbidden; this includes threats of reprisals and any attempt at reprisal against the persons that submit a report as set forth by legislation.

“Reprisal” is defined as any action or omission forbidden by law or that directly or indirectly results in harmful treatment that places the affected persons at a particular disadvantage in their work or professional surroundings simply because they are whistleblowers or have participated in public disclosure.

As regards Law 2/2023, the following actions are considered reprisals, although this list is not comprehensive:

a) Suspension of the employment contract or dismissal or termination of the work or statutory relationship. This includes non-renewal or early termination of a temporary employment contract after having passed the trial period, as well as the early termination or cancellation of goods and services contracts. It also includes taking disciplinary measures, delaying or refusing to promote workers and making any other significant changes to their working conditions and not converting a temporary employment contract into a full-time contract when the conditions and expectations for such are legitimate. All of the above can only take place if the following conditions are met:

- The measures are applied according to labour legislation and correspond to the normal exercise of managerial authority.

- The measures are the result of circumstances, events or offences that have been proven and are outside the scope of the submitted report.

b) Harm, including harm to a reputation, financial losses, constraint, intimidation, harassment or ostracism.

c) Negative assessments or references concerning occupational or professional performance.

d) Blacklisting or disclosure of information in a specific sectoral setting that hinders or impedes access to employment or contracting of goods and services.

e) Refusal or cancellation of a license or permit.

f) Refusal to provide training.

g) Discrimination or unfavourable or unfair treatment.

If anyone's rights are affected by their report or its disclosure after two years have passed, they may request protection from the competent authority. Said authority may prolong the period of protection in exceptional cases and if properly justified, after having interviewed the affected parties or bodies.

Protection measures versus reprisals

Individuals who provide information about the actions or omissions mentioned above, or who engage in public disclosure as stated in Law 2/2023, shall not be considered responsible for breaching restrictions on information disclosure and shall not incur in any liability as regards said information or public disclosure. This shall hold true provided there are reasons to believe that the report or public disclosure of that information was needed to reveal an act or omission as defined by said law, notwithstanding the provisions in the specific regulations for the protection of the work environment. It should be noted that this provision does not affect criminal liability.

The provisions stated in the previous paragraph also apply to reports submitted by worker representatives, even if they are legally responsible for not disclosing confidential information, notwithstanding the specific regulations for the protection of the work environment.

Whistleblowers shall not be held liable for acquiring or accessing the information they report or disclose publicly, unless said acquisition or access constitutes a crime.

Any other potential responsibility derived from acts or omissions that are not related to the report or public disclosure, or that are not necessary to reveal an offence as contemplated in Law 2/2023, shall be enforceable according to applicable regulations.

As regards legal proceedings or proceeding carried out by other public authorities related to harm undergone by whistleblowers, once the whistleblower has reasonably demonstrated that they have made a report or public disclosure in accordance with Law 2/2023 and undergone harm, it will be assumed that said harm is a reprisal for having made the report or public disclosure. In these cases, the person who has caused the harm must prove that the measure taken was duly motivated and not associated with the report or public disclosure.

In legal proceedings, including those concerning libel, infringement of copyright, violation of secrets, infringement of data protection regulations, disclosure of business secrets or requests for compensation based on labour or statutory law, whistleblowers shall not be held liable for reports or public disclosures protected by Law 2/2023. In their defence and within the framework of the corresponding legal proceedings, these individuals shall have the right to allege that the report or public disclosure was needed to expose an offence as stated in Law 2/2023, provided they had reasonable cause to believe so.

Measures for the protection of the persons involved

During case proceedings, the persons affected by the report shall have the right of presumption of innocence, the right to be defended and the right to access the case records as set forth in Law 2/2023. They shall also enjoy the same protection provided for whistleblowers, including the protection of their identity and the guarantee that the events and information related to the proceedings shall remain confidential.

Conditions for exemption and reduction of penalties

If the person who has committed the administrative offence reveals the facts by submitting information

before having been notified that investigation or disciplinary proceedings have begun, the body responsible for reaching a solution may exempt them from satisfying the administrative penalty by proposing a substantiated decision, provided the following events can be proven:

a) That the offence was no longer being committed when the report or disclosure was submitted and that they have identified the other persons who participated in or facilitated the offence.

b) That they have collaborated fully, continuously and thoroughly throughout the investigation.

c) That they have provided true and meaningful information, means of proof or important data that contribute to certify the events under investigation, without destroying or hiding them, or directly or indirectly revealing their contents to third parties.

d) That reparation for the harm caused has been made by those responsible.

If all these requirements are not met, including partial reparation of the harm caused, the competent authority shall evaluate to what degree they contribute to resolving the case and decide whether to reduce the corresponding penalty. This will only apply if the whistleblower or author of the disclosure has not been previously penalised for events similar to those that gave rise to the proceedings.

Reduction of the penalty may also be extended to other participants in the offence, depending on the degree of their active collaboration in clarifying the events, the identification of other participants and reparation or reduction of the harm caused, as decided by the body in charge of reaching a solution.

It is important to note that Law 2/2023 excludes from these provisions the offences stated in Law 15/2007, dated 3 July, on Defence of the Competition.

10. MANAGEMENT OF INFORMATION RECEIVED

The information can be submitted to the Orbinox Group anonymously. If this is not the case, the whistleblower's identity will be kept confidential and known only by Orbinox Group Internal Information System Management (IISM).

The information must be reported through the internal information channel by using the electronic application specifically designed for this purpose; this application can be found and accessed from the Orbinox Group's website. The application shall allow reports to be submitted in writing. Any information related to Law 2/2023 and received by other means in the Orbinox Group shall be forwarded to the internal information channel under the supervision of the Orbinox Group Internal Information System Manager. If requested by the whistleblower, a face-to-face meeting may be arranged, to take place within a maximum of seven business days.

If necessary, the whistleblower will be informed that the report will be recorded and given information about their data processing as stated in the General Data Protection Regulation (RGPD) and Organic Law 3/2018 on Personal Data Protection and guarantee of digital rights (LOPDPGDD).

When submitting the report, the whistleblower must provide an address, e-mail address or secure location to receive notifications, unless they explicitly refuse to receive any communication related to the actions performed by the IISM resulting from the information provided.

The Internal Information System Manager (IISM) must document oral reports, even those that take place in face-to-face meetings, in one of the following ways:

a) By recording the conversation in a secure, long-lasting and accessible format.

b) By means of a complete and accurate transcription of the conversation by the personnel in charge of the same.

Notwithstanding their rights as stated in personal data protection regulations, the whistleblower will be offered the chance to verify and correct the transcription of the message and accept it by providing their signature.

Once the report is submitted, it will be filed in the information management system and assigned an identification code. This record will be contained in a secure and restricted database, exclusively for use by authorised Orbinox Group IISM personnel. This record will include all the details of the reports received, which will contain:

a) Date of reception

b) Identification code

c) Actions performed

d) Measures taken

e) Date closed

Once the information is received, the whistleblower will be issued a receipt in no more than 7 calendar days, unless they explicitly refuse to receive communications related to the investigation or the Orbinox Group IISM considers that the confirmation of receipt may compromise protection of the whistleblower's identity.

After filing the information, the IISM will study whether it is admissible in accordance with the material and personal factors stated in Articles 2 and 3 of Law 2/2023. This admission process and subsequent actions will be performed according to the information management procedure established in the Orbinox Group.

11. POLICY REVIEW

The Orbinox Group will review the policy that sets forth the general principles of the Internal Information System and whistleblower protection, as well as its information management procedure, at least every three years, Changes will be made to the policy if necessary. These reviews will take into consideration the experience acquired during its application and the experience of other competent bodies.