



INFORMATION MANAGEMENT
PROCEDURE FOR THE
INTERNAL REPORTING SYSTEM

Document details

Document identification	Information Management Procedure for the Internal Reporting System
Geographical scope of application	Domestic and International
Rules replaced	None
Rules repealed	None
Person in charge of its surveillance	IRS Responsible
Proposing body or department	Legal Department and CSR Department
Approving body	Board of Directors
Date of Approval of the current version	31 May 2023
Applicability	13 June 2023
Available on	Intranet and IRS

Index

Document details	2
1. PURPOSE	4
2. SCOPE	4
2.1. Objective scope	4
2.2. Subjective scope	5
3. IRS RESPONSIBLE	5
4. REPORTING CHANNELS	6
4.1. Internal reporting channels	6
4.2. External reporting channels	7
5. INVESTIGATIONS	7
5.1. General issues	7
5.2. Receipt and acknowledgement of reports; admission/rejection of reports for processing	8
5.2.1. Receipt	8
5.2.2. Acknowledgement of receipt	8
5.2.3. Admission/rejection	8
5.3. Examination of the file	9
5.3.1. Appointment of the Investigating Officer	9
5.3.2. Investigation proceedings	11
5.3.2.1. Collecting and/or extracting information and documentation on any media	12
5.3.2.2. Interviews	13
5.3.3. Closing the Investigation	14
6. REGISTRY BOOK	15
7. AVAILABILITY OF INFORMATION	15
8. PROTECTION OF PERSONAL DATA	16
8.1. Data controller	16
8.2. Data protection obligations of the Body Responsible for the ISS	16
8.3. Limiting access to IRS personal data	17
9. REGULAR REPORTING FOR THE ORGANISATION	17
10. Annex	18

1. PURPOSE

The purpose of this procedure is to develop the general principles of the Internal Reporting System (the "**IRS**") set out in the "*Internal Whistleblower Defence and Infringement Reporting System Policy*" (the "**IRS Policy**") of the corporate group led by Gransolar (the "**Organisation**"), regulating the process of receiving information regarding any conduct that may involve a breach included in the objective scope of application set out below, as well as the conduct of any investigation that may result, in accordance with Spanish Act 2/2023 of 20 February on the protection of persons who report regulatory infringements and the fight against corruption (the "**Whistleblower Protection Act**").

2. SCOPE

2.1. Objective scope

This procedure applies to information received through the IRS channels concerning any potential infringement/non-compliance.

For the purposes of this procedure, the following are considered to be events of non-compliance:

- a. Any act or failure to act which may result in an infringement of European Union ("**EU**") law provided that they:
 1. Fall within the scope of the EU measures listed in the Annex to *Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law*, irrespective of how such acts or failures to act are classified by national law.
 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. Have an impact on the internal market, as referred to in Article 26(2) TFEU, including infringements of EU competition rules and regulations governing aid granted by States, as well as infringements relating to the internal market in relation to acts in breach of corporate tax rules or practices aimed at obtaining a tax advantage that would defeat the object or purpose of corporate tax law.
- b. Any act or failure to act that could constitute a criminal offence or a serious or very serious administrative infringement.

Likewise, for the purposes of this procedure, any conduct contrary to the Criminal Compliance Model (the "**CCM**") and the measures included therein, to the prevention protocols against harassment at work, sexual or gender-based harassment, sexual violence and LGTBI persons that the Organisation has in place, or otherwise contrary to any other measures implemented to prevent any illegal action or action against the principles and values defined by the Organisation, shall be considered an event of non-compliance.

The aforementioned breaches may also be reported when they are committed by third parties outside the Organisation, provided that such parties are involved in the exercise of corporate activities on behalf of the Organisation.

2.2. Subjective scope

A whistleblower shall be considered to be any natural person who files a report on possible breaches in an employment or professional context under the terms set out in Section 3 of the Whistleblower Protection Act.

For the purposes of this procedure, the following may be considered whistleblowers, namely: employees, shareholders and members, suppliers, contractors, subcontractors, customers, members of governing, management or supervisory bodies, including non-executives, volunteers, interns, trainees, job applicants and persons who have maintained an employment or corporate relationship with the Organisation, even if such relationship is terminated.

The informants detailed in the preceding paragraph, and those to whom they recipients of the Organisation's CCM have an obligation to report any conduct that may be contrary to the CCM and any measures therein.

The informants detailed in the preceding paragraph, and those to whom such consideration may be extended, shall have the obligation to report through the channels made available to them any unlawful conduct, contrary to national and international legislation, as well as any conduct contrary to the provisions of the Code of Conduct, policies and procedures and/or the Organisation's CCM, as well as the measures that form part of the latter.

3. IRS RESPONSIBLE

The Organisation's Managing Body has designated as the IRS Responsible a collegiate body composed by the person holding each of the following positions within the Organisation: the Quality Manager, the Chief Technical Officer and the Head of the CEO's office.

The list of current members of the IRS Responsible is set out in **Annex I**.

The IRS Responsible shall delegate to one of its members the authority to manage the IRS and to process investigation files.

The IRS Responsible shall notify to the Independent Whistleblower Protection Authority, both the list of the members of the IRS Responsible and to whom of its members the IRS Responsible delegates the authority to manage the IRS and to process investigation files, within 10 days as from the date of the corresponding designation.

The IRS Responsible shall duly assume the management of the information received through the IRS channel, ensuring due application of this procedure, including, where appropriate, the relation with the software and specialised technology providers for the provision of this type of communications.

Under the general principles set out in the IRS Policy, the IRS Responsible has the material and personal resources necessary for the due performance of its functions, which it carries out autonomously and independently from the remaining bodies within the Organisation. Its actions shall be governed by the general principles set out in such Policy.

The IRS Responsible will rely on the Corporate Social Responsibility Committee and the CSR department of the Organisation for the administration and management of the IRS, for statistical

and auditing purposes. The Corporate Social Responsibility Committee, and by extension the Organisation's CSR department, will not be able to access or view the data and information received through the IRS. The information that the Corporate Social Responsibility Committee will handle will be that necessary to determine the auditable traceability of the data.

4. REPORTING CHANNELS

4.1. Internal reporting channels

The Organisation shall keep permanently at the disposal of its directors, managers, employees, shareholders, suppliers, as well as other third parties related to the Organisation, the channel described below, as a suitable instrument for reporting or disclosing potential breaches that refer to or affect the scope of their professional activity, without prejudice to their rights to address their reports to the Independent Whistleblower Protection Authority or to any other competent authority or body.

The channel enabled through the Organisation's IRS for the reporting of information relating to potential non-compliance is the **Gransolar Whistleblowing Channel**.

Individuals may submit their reports on potential non-compliance through the aforementioned channel via the following link: <https://gransolar.integrityline.com/> for verbal and written communications.

Communication following the formulation of the complaint will be made through the "secure communication mailboxes" of the Gransolar Whistleblowing Channel, which in any case, may be anonymous.

The confidentiality of the report and the identity of the whistleblower and of any third party mentioned in such report shall be protected by:

- a. Technical measures: guaranteed by the relevant supplier -EQS Group- through its Integrity Line tool, designed in accordance with the specifications of the Whistleblower Protection Act.
- b. Organisational measures provided for in this procedure.

The identity of the whistleblower, if known, and of the third parties identified in the report, may only be disclosed to the judicial authorities, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation, following notice thereof to the whistleblower or the third party concerned, provided that the provision of such notice does not compromise any ongoing investigation or judicial proceedings.

Whistleblowers shall act in good faith. Reports shall be made in accordance with the criteria of truthfulness and proportionality and shall only refer to facts related to the Organisation. False or malicious reports or information may result in the application of the disciplinary regime in force in the Organisation, and may lead to the filing of the relevant legal action for any resulting damages.

Retaliation, including threats and attempts of retaliation against whistleblowers and related individuals, is expressly prohibited under the terms of the IRS Policy, and shall ensure that its professionals do not adopt, either directly or indirectly.

Where the information provided by whistleblowers relates to the breaches listed under 2.1. a) and b) of this procedure, the following support measures, if any, will be available to such whistleblowers from the Independent Whistleblower Protection Authority or other competent authority or body:

- Information and advice complete, independent and free of charge on the procedures and remedies available, on protection against reprisals and the rights of the relevant individual.
- Assistance by the competent authorities regarding any relevant authority involved in their protection against retaliation, including certification that they are eligible for protection under the Whistleblower Protection Act.
- Legal assistance in criminal proceedings and cross-border civil actions in accordance with EU law.
- Financial and psychological support, on an exceptional basis, if so decided by the Whistleblower Protection Authority, after assessing the circumstances arising from the submission of the communication.

4.2. External reporting channels

Without prejudice to the preferential nature of the internal channel described above, for the reporting of potential infringements, whistleblowers may also access the existing channels opened by the public authorities for these purposes (the "**external channels**"), either directly or following communication through the aforementioned internal channel.

The above shall not apply to reports of events of non-compliance consisting of any conduct contrary to the measures described in the Organisation's CCM.

5. INVESTIGATIONS

5.1. General issues

An Investigation compiles all actions carried out and measures taken to verify and clarify the facts described in the reports of which the IRS Responsible becomes aware.

The IRS Responsible will document the different phases of the investigation and shall ensure that all documentation generated during the processing on any type of support is kept properly secure. It shall also take all necessary measures to guarantee the confidentiality of the Investigation and comply with the regulations on the protection of personal data.

This is without prejudice to the custody tasks that may be entrusted to those teams or persons who may support the Investigating Officer in charge of the Investigation.

All notices to be sent to the whistleblower, as well as to the members of the Organisation and other third parties related to the Investigation, shall be sent from an e-mail address or, where appropriate, from a specific platform, that allows communications to be sent and received in a reserved and confidential manner, so that only the IRS Responsible or the Investigating Officer has access to such communications.

If the Organisation's protocols for the prevention of workplace, sexual or gender-based harassment, sexual violence and harassment and/or violence against LGBTI persons provide for specific investigation and/or inquiry procedures, those procedures shall be followed (instead of

those provided for in this Section 5), provided that the content of the report can be subsumed under the conduct governed by such procedures. In all matters not provided for in such procedures, this paragraph 5 shall subsidiarily apply.

5.2. Receipt and acknowledgement of reports; admission/rejection of reports for processing

5.2.1. Receipt

The IRS Responsible shall open an Investigation whenever it becomes aware of facts or circumstances that may constitute an event of non-compliance, either *ex officio* or as a result of any report or information received through the relevant channel or otherwise.

The most common ways of becoming aware of such facts or circumstances are as follows:

- Communications received through the specific channel set up for this purpose.
- Press releases.
- Court/prosecutor's office/police summons.
- Findings in the framework of an internal control procedure.

In the event that any member of the Organisation, other than the IRS Responsible, receives any communication or information regarding a potential event of non-compliance, he/she must immediately forward it to the IRS Responsible, while preserving at all times the confidential nature of the communication and, if applicable, the identity of the whistleblower.

The IRS Responsible shall inform about the above referral obligation and the consequences of non-compliance. Any failure to refer the relevant communication or information shall be a very serious infringement.

All information and communications brought to the attention of the IRS Responsible shall be assigned a registration number.

5.2.2. Acknowledgement of receipt

In the event that the Investigation is initiated upon receipt of a communication, the IRS Responsible shall, provided that the communication is not anonymous or the whistleblower has not waived the right to receive notifications, send the whistleblower an acknowledgement of receipt within **seven calendar days** of receipt of the communication, except if this could jeopardise the confidentiality of the communication.

5.2.3. Admission/rejection

Once the communication has been received and registered and the existence of a conflict of interest has been ruled out, the IRS Responsible must decide whether the report is admissible or should be rejected. To do so, it shall verify whether the information relates to facts potentially constituting an infringement as defined in this document.

If necessary to decide on the admissibility or inadmissibility of the information for

processing, the IRS Responsible may request additional information from the whistleblower on the facts which are the subject of the communication received, provided that the whistleblower is not anonymous or has not waived the right to receive communications.

In any event, the inadmissibility of a communication must be based on at least one of the following grounds:

- The facts reported are not credible.
- The facts alleged do not constitute an infringement within the meaning of this procedure.
- The communication is manifestly unsubstantiated or there are, in the opinion of the IRS Responsible, reasonable grounds to believe that the information contained in the communication was obtained through the commission of an offence.
- The communication does not contain significant new information on any infringement compared to a previous communication for which the relevant procedures have been completed, unless there are new factual or legal circumstances that justify a different follow-up.

The decision on the admissibility (or inadmissibility) of the report received shall be taken within **ten business days** from the date of its registration and shall be brought to the attention of the whistleblower within **five business days** of the adoption of the decision. If the report is not admitted for processing, then any reasons shall be communicated to the whistleblower (except where the whistleblower waive any right to receive notices).

If the facts on which the information is based are suspected of constituting a criminal offence, the Public Prosecutor's Office or the European Public Prosecutor's Office, as appropriate, shall be informed, based on the provisions in the Organisation's "*Special Protocol for internal investigations concerning legal entities*".

5.3. Examination of the file

Investigation shall start once the communication has been accepted for processing. This will include all measures aimed at verifying the accuracy of the facts that are the subject of the information.

The Investigation may not exceed **three months** from the receipt of the communication or information¹ except in cases of particular complexity that require an extension of such period, in which case it may be extended up to a maximum of **three additional months**.

All stages of the Investigation must be properly documented, under the direction and supervision of the IRS Responsible, in an appropriate and sufficient manner to ensure traceability and to enable the procedure to be validated before any third party.

5.3.1. Appointment of the Investigating Officer

The IRS Responsible shall designate the individual responsible for processing the Investigation and coordinating the investigative measures to be carried out (the "**Investigating Officer**"), who may be any of its members, a manager or employee of the Organisation or a professional external to the Organisation.

Likewise, the designated Investigating Officer may designate a collaborator member of the Organisation for the processing of the Investigation.

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

- If the communication or report concerns a member of the Board of Directors or the individual assuming the function of General Manager, a person external to the Organisation must be appointed as Investigating Officer.
- In the event that the communication or report affects any of the members of the IRS Responsible, the relevant individual may not participate in the Investigation, the remaining members of the IRS Responsible may appoint the relevant Investigating Officer.
- In the event that the individual reported is a member of the works council, a staff delegate or a delegate of a trade union section, the specific formalities applicable to this condition must be taken into account and the manager responsible for Human Resources at the Organisation must be informed.

In the event that an internal Investigating Officer, other than the IRS Responsible, is appointed, the IRS Responsible shall notify him/her of this appointment.

A service agreement shall be entered into whenever an external Investigating Officer is appointed, as well as a data processor agreement if required by personal data protection regulations.

The Investigating Officer shall guarantee confidentiality and impartiality in the performance of his or her duties, which may include, without limitation, the following:

- Gathering of background information and relationship to the Organisation of the individuals involved in the information received.
- Informing the persons potentially responsible for the facts that are the subject of the report or information received (the "**person concerned**") of the existence of the Investigation.
- Deciding on the investigative measures deemed necessary to clarify the facts, in accordance with a time-bound plan.
- Determine, if applicable, the functions or departments of the Organisation that should be involved in the Investigation.

¹ If no acknowledgement of receipt was sent to the whistleblower, the three month period shall run from the expiry of a seven calendar day term from the receipt of the information.

- Identifying individuals who can give an account of the facts and provide additional information.
- Identifying the need for documentation to be provided to third parties.
- Opening, if necessary, new lines of investigation in the light of the evidence obtained.
- Evaluate all relevant evidence obtained during the investigation.

The Investigating Officer may, in compliance with the rules on the protection of personal data, request the assistance of external consultants or staff from internal bodies or departments of the Organisation. In the latter case, any conflict of interest must be ruled out beforehand.

5.3.2. Investigation proceedings

During the course of the investigation, the Investigating Officer shall take all necessary measures to investigate and clarify the facts contained in the communication or report admitted for processing.

Respect for the presumption of innocence and the reputation of the person concerned, as well as the protection of his or her personal data, shall be guaranteed at all times. The Investigating Officer will notify the person concerned of the opening of the investigation and of the facts against them, as well as of their right to be heard at any time, at a time and in a manner deemed appropriate for the proper conduct of the investigation.

Where such information might encourage the person concerned to conceal, destroy or tamper with any evidence, the notice may be postponed until the time of his or her interview, and the reasons for such a decision shall be recorded in the investigation file. In no case shall the person concerned be informed of the identity of the whistleblower or be given access to the report.

If the presence of the person concerned in the Organisation during the investigation period is likely to jeopardise the success of the Investigation, he/she may, on the proposal of the Investigating Officer, be suspended (while retaining his/her remuneration) in order to ensure that the necessary investigative activities may proceed without interference. Such suspension shall be agreed for the time necessary to carry out the necessary investigative work, but shall in no case be extended beyond the duration of the Investigation.

If it is necessary for the success of the investigation, the Investigating Officer may request additional information from the whistleblower regarding the facts that are the subject of the communication sent, provided that the whistleblower has not waived the right to receive notices.

Similarly, if, as a result of the Investigation carried out, other facts are discovered which may constitute new infringements, the IRS Responsible, having been informed in advance by the Investigating Officer, will resolve on the opening of a new investigation or, if it is related to the matter already under investigation, on the extension of the current Investigation.

If, as a result of the investigative measures taken in the course of the Investigation, evidence of the possible existence of a criminal offence is found, the Public Prosecutor's

Office or the European Public Prosecutor's Office, as the case may be, shall be informed, in all cases in accordance with the provisions of the Organisation's "*Special Protocol for internal investigations concerning legal entities*".

5.3.2.1. Collecting and/or extracting information and documentation on any media

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

Where necessary, the Investigating Officer shall coordinate the access to and the collection of information (*e-discovery*) from equipment, devices and computer systems that may contain information relevant to the investigation, applying appropriate proportionality and security measures, such as the selection of key words that will allow such information to be extracted. Access to equipment, devices and IT systems shall be in accordance with the regulations applicable to the use of the Organisation's IT resources and in full compliance with personal data protection regulations.

The documentation and information collected shall become part of the Investigation and may be used to defend the interests and rights of the Organisation.

The Investigating Officer may rely on a forensic investigation team to carry out the technical work required, either internally or externally:

- Internal forensic team: the collaboration of internal professionals or departments with the technical capacity to collect and process the information and documentation necessary for the development of the Investigation shall be requested. The existence of a conflict of interest must be ruled out beforehand.
- External forensic team: an external company specialised in forensic work will be hired to collect and process the information and documentation necessary for the development of the Investigation.

In the event that the intervention of these forensic teams is necessary, they will carry out mainly the following tasks:

- *E-discovery*: consisting of the acquisition, processing and indexing of information stored in the equipment, devices and computer systems included in the Investigation perimeter.
- *Forensic accounting*: aimed at analysing economic-financial corporate documentation.
- *Corporate intelligence*: analysis of the corporate and asset structure and the personal, financial and asset links that may exist between the persons concerned.
- *Data tracking*: analysis of information flows to identify possible unlawful collection or use of information.

In carrying out these tasks, the forensic team will also be responsible for the

preservation of all documents and information, in whatever format, acquired and generated in the course of the Investigation. To this end, they shall establish the necessary technical safeguards to ensure confidentiality and chain of custody.

5.3.2.2. Interviews

In the course of the investigation, the Investigating Officer may conduct as many interviews as deemed necessary to verify and clarify the facts.

Interviews shall be announced in good time and shall be conducted by the Investigating Officer in the presence of at least one other person, always respecting the rights of the person interviewed to privacy, integrity, defence and the presumption of innocence:

- Person concerned: the interview will begin by informing the person concerned of his/her rights, in particular the right to be informed of the facts reported and to provide any documents or evidence that he/she considers relevant to his/her defence, which will be included in the investigation. The individual shall be informed of all matters relating to the processing of personal data in accordance with the provisions applicable to such purposes, unless this information is included in the specific privacy policy for the corresponding category of data subjects. He/she shall be invited to give his/her version of the facts and may refuse to answer all or any of the questions put to him/her or may answer only those questions which he/she deems appropriate.
- Individuals other than the person concerned: the interview will begin by informing the interviewee of the obligation to maintain the utmost confidentiality with regard to the Investigation in progress and his/her involvement. He/she will be informed of all matters relating to the processing of personal data, in compliance with the regulations applicable to these purposes, unless this information is included in the specific privacy policy for the corresponding category of data subjects. He/she will also be informed of his/her duty to collaborate in the progress of the Investigation by answering all questions loyally and truthfully, and by providing any data that may be required of him/her in the course of the Investigation.

Interviews will always be conducted with full respect for the rights of interviewees.

A written record of the interview will be made, which will include the content of the interview. The transcript shall be read to the interviewee so that he/she can agree with its content. If there are any discrepancies, these should be reviewed and, if necessary, the transcript should be amended or a note should be made of such discrepancies. The transcript should be signed by both the interviewer and the interviewee at the end of the interview. If the interviewee does not wish to sign, his/her refusal shall be noted.

In addition, if the interviewee so authorises, the interview may be recorded and included in the file in *lieu* of a written record. In this case, an equally effective alternative procedure shall be provided and a reference to the processing of image and/or voice data shall be included in the relevant data protection notice.

If the person concerned or one of the members of the Organisation duly summoned to appear as part of the Investigation does not acknowledge receipt of the notices

sent or otherwise fails to confirm his/her participation in the Investigation as requested, the Investigating Officer shall seek such confirmation by telephone or even by personal contact, always guaranteeing the confidentiality of the communication, and shall document the result of this approach.

If, following this communication, the person summoned fails to appear for the procedure for which he/she was summoned, the Investigation shall continue and the Investigating Officer shall report such failure to cooperate to the individual in charge of human resources of the Organisation for the purpose of taking the appropriate decision.

If third parties who do not have a contractual relationship with the Organisation fail to appear after the first written communication containing the information required by the data protection regulations, they shall be deemed to have refused to participate in the Investigation, and no further communication shall be sent.

5.3.3. Closing the Investigation

Upon completion of all investigative measures, the Investigating Officer shall issue a report containing at least the following information:

- Identification code assigned to the communication or information that gave rise to the Investigation.
- Chronological description of the main milestones in the processing of the Investigation.
- List of the investigative measures taken to verify the credibility of the facts that are the subject of the information, as well as the documentation provided.
- Assessment of the outcome of the investigative actions carried out and the conclusions reached.
- Proposed decision.
- Recommendations or proposals for improvement to be taken into account in the Organisation's CCM.

If the Investigating Officer is a person other than the IRS Responsible, the Investigating Officer shall submit the report together with the investigation files to the IRS Responsible, that shall adopt one of the following resolutions in light of the conclusions reached in the report:

- Favourable resolution: this will be adopted in cases where it is clear that no event of non-compliance has been found, which will determine the end of the investigation without the need to adopt any measure. The decision shall be notified to the person concerned.
- Unfavourable resolution: this will be adopted when it is determined that an infringement attributable to the person concerned has been established.

In this case, the appropriate measures shall be taken in accordance with the

applicable disciplinary rules and, in particular, the provisions of the collective agreement applicable to the relevant relationship and the Workers' Statute.

If the relationship of the person concerned with the Organisation does not allow for the application of labour regulations regarding disciplinary matters, the relevant legal or regulatory provisions shall apply.

In the case of non-compliance consisting of conduct contrary to the CCM and the measures forming part of the CCM, the specific sanction regime provided for in the CCM, where applicable, shall apply.

The IRS Responsible will communicate to the whistleblower the outcome of the Investigation, unless the whistleblower has waived receipt of communications or the confidentiality of the information received is compromised.

6. REGISTRY BOOK

The Gransolar Whistleblowing Channel (or, in case the Gransolar Whistleblowing Channel does not offer such functionality, the IRS Responsible) shall keep a register of the information and communications received and the Investigations to which they have given rise, while ensuring the confidentiality of this information.

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

- Date of receipt
- Registration number
- Internal investigation procedure: yes / no
- Closing date

The information contained in this register shall be kept in accordance with the provisions of the regulations on the protection of personal data. In particular, personal data included in this register, if any, may be kept only for the period necessary to establish compliance with Spanish Act 2/2023 and, in any case, may not be kept for more than ten years.

7. AVAILABILITY OF INFORMATION

The IRS Responsible shall ensure that the information necessary for whistleblowers to use of the communication channels described in this procedure is provided in a clear and easily accessible manner.

This information is available on the Organisation's corporate website at www.gransolar.com

8. PROTECTION OF PERSONAL DATA

The processing of personal data within the framework of the IRS shall be conducted in full compliance with the general principles and obligations established in all personal data protection regulations and in Spanish Act 2/2023.

8.1. Data controller

The person responsible for the processing of personal data collected and processed within the framework of the IRS is the Managing Body of Gransolar Holdings, S.L., which may comply with the obligations established in any applicable personal data protection regulations through the execution of agreements with third parties or, where mandatory, by establishing a system of joint control with the Organisation.

In any case, the IRS Responsible shall be in charge of ensuring compliance with the obligations set out in the data protection regulations.

8.2. Data protection obligations of the Body Responsible for the ISS

Among other obligations, the IRS Responsible will ensure that the following principles are followed:

- The principle of transparency, and the whistleblower, the data subject or any third party involved in the investigation must be provided with the necessary information regarding the protection of personal data. To this end, the data controller shall draw up the relevant information clause to be provided to the data subjects.

In particular, the whistleblower must be informed that his/her identity will in any case remain confidential and that it will not be disclosed to the person concerned or to any third party, with the exception of the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation, in accordance with the provisions of Spanish Act 2/2002.

- The principle of data minimisation, whereby no more data should be collected than is strictly necessary and essential for the correct operation of the IRS; if more data than is strictly necessary is collected by accident, it will be deleted as soon as possible.
- The principle of purpose limitation, whereby no personal data collected through the IRS must be processed for any purpose other than the management of communications and the conduct of the Investigation.
- The principle of limitation of the retention period, whereby personal data should only be processed for as long as necessary to decide whether to open an investigation into the facts reported by the whistleblower.
- In any case, personal data must be erased after three months have elapsed from the receipt of the communication without an investigation having been opened, unless the purpose of the retention is to leave evidence of the operation of the system.
- Communications that have not been acted upon can only be kept in anonymous form, and shall not be subject to any blocking obligation provided for under any applicable personal data protection regulations.

- The principle of accuracy, such that any personal data included in the information communicated that is not true must be deleted (unless the lack of truthfulness may constitute a criminal offence, in which case the information will be kept for the time necessary during the legal proceedings).
- The principle of integrity and confidentiality, guaranteeing the confidentiality of the whistleblower and third parties, as indicated in the procedure. Likewise, all technical and organisational security measures necessary to protect the information against unauthorised or unlawful processing and accidental loss, destruction or damage shall be implemented.

No additional personal data may be collected than those necessary and essential for the proper management of the process.

8.3. Limiting access to IRS personal data

Access to the personal data contained in the IRS shall only be granted to third party service providers who qualify as data processors and to the Data Protection responsible.

The following individuals may also access personal data held in the IRS:

- The Head of the Human Resources Department, who shall have access to personal data solely and exclusively where disciplinary measures may be taken against an employee.
- The Head of Legal Services, who shall have access to personal data solely and exclusively in the event of legal action being taken in relation to the facts described in the communication.

9. REGULAR REPORTING FOR THE ORGANISATION

The IRS Responsible will produce a specific annual report as part of annual ESG report as well as the Organisation's CCM annual plan, including information on communications received by the Organisation's IRS relating to any conduct contrary to the Code of Conduct, Corporate Policies or CCM and the measures forming part of them, with an indication of their current stage.

In the event of an unfavourable outcome of the Investigation, the report shall include (i) the specific nonconformities identified; (ii) the area(s) of activity affected by the nonconformities; and (iii) the corrective actions that, according to the criteria of the IRS Responsible, could be implemented as responsive measures in the process of updating and continuous improvement of the Code of Conduct, Corporate Policies and the CCM.

Annex I

Members of the IRS Responsible

- Quality Manager: Alexandr Sidorenko
- Chief Technical Officer: Ivan Arkipoff
- Head of the CEO's office: Rocío de Luis



Polígono Industrial Castilla
Vial 14, Parcelas 7 & 9
46380 Cheste, Valencia (Spain)
(+34) 960 918 522 | contact@pvhardware.es