Protocol on the Handling and Transmission of Inside Information

INDEX

INTRODUCTION

This Protocol on the Handling and Transmission of Inside Information (hereinafter the "**Protocol**") of PROMOTORA DE INFORMACIONES, S.A. ("**PRISA**" or the "**Company**") and its subsidiaries and investees to which apply the Internal Code of Conduct on Stock Exchange Matters of the PRISA GROUP (hereinafter the "**ICC**"), was approved, pursuant to a report from the Appointments, Remuneration and Governance Committee by the Company's Board of Directors at its meeting on 26 October 2021, implementing the ICC, especially Section 1 of Heading III, which includes amendments approved by the Board of Directors at its meeting on 31 October 2023.

This Protocol, which is based to a large extent on the "Guide for Action on the Transmission of Inside Information to Third Parties" published by the Spanish Securities Market Regulator (Comisión Nacional del Mercado de Valores, CNMV) of 9 March 2009, as well as on the Regulation 596/2014 of the European Parliament and of the Council, of 16 April, on market abuse, establishes in a question and answer format the PRISA GROUP's rules and procedures for personnel and third parties outside the PRISA GROUP, to safeguard the interests of investors and prevent and avoid market abuse.

The duty to be familiar with and adhere to this Protocol applies without prejudice to the duty of persons to which the ICC applies to be familiar with and adhere to the ICC.

This protocol must be interpreted in accordance with any legislation applicable to the PRISA GROUP and the regulations set forth in the Company's corporate documents, especially in fulfilment of the provisions on these matters laid down in the ICC. Any terms not expressly defined in the Protocol must have the same meaning as those defined in the ICC.

The Compliance Unit is responsible for clarifying any queries or doubts relating to the content, interpretation and application of this Protocol or compliance therewith.

INSIDE INFORMATION AND GENERAL CODE OF CONDUCT

1) What is Inside Information?

Inside Information shall mean any information of a precise nature that directly or indirectly refers to GRUPO PRISA or one or more Transferable Securities or Financial Instruments[1] issued by any GRUPO PRISA company or by issuers outside GRUPO PRISA, which has not been made public and that, if it were made public, would be likely to have a significant effect on the prices of such Transferable Securities or Financial Instruments or, if applicable, of related derivative financial instruments[2].

2) How may a person become privy to Inside Information?

A person may gain access to Inside Information for several reasons, including the following:

a) Because of his/her position in the PRISA GROUP;

b) Because of being involved in a project or transaction involving Inside Information; and

c) Due to a leak of Inside Information, i.e. when Inside Information is transferred by means other than those specified in the applicable rules.

3) What are the obligations of persons privy to Inside Information?

As a general rule, recipients of Inside Information at any point in time are bound by the following duties, irrespective of their position in or relationship with the PRISA GROUP or the reason for being privy to the Inside Information:

a) Duty to abstain; and

b) Duty to safeguard.

4) What is the duty to abstain?

Recipients of Inside Information who are aware or should have been aware that the Information is privileged must abstain from directly or indirectly performing any of the following actions on their own behalf or that of a third party:

---

[1] Transferable Securities or Financial Instruments shall mean:

1. Fixed or variable income securities issued by any GRUPO PRISA company that are traded on an official secondary market or other regulated markets, in multilateral trading facility or in other organised secondary markets.
2. Financial instruments and contracts of any kind that grant the holder the right to acquire the aforementioned securities, including those that are not traded in secondary markets.
3. Financial instruments and contracts, including those that are not traded in secondary markets, whose underlying basis is composed of securities or instruments issued by any GRUPO PRISA company.
4. Any securities or financial instruments issued by other companies or entities in relation to which Inside Information is held.

Securities include, for example, shares, bonds, debt and debentures of PRISA or PRISA GROUP companies traded in official or organised markets in Spain or abroad (the Stock Exchange (Bolsa de Valores), AIAF, etc.).

[2] For example, Inside Information would include information on the start of negotiations over a merger with another entity, a significant asset sell-off, or any other significant transaction or information, knowledge of which could benefit the person privy to it because it may be presumed that once published, said Information would affect the trading price of the Securities in the secondary market or organised trading facility (the Stock Exchange (Bolsa de Valores), AIAF, etc.) on which they are traded.

a) Preparing or carrying out any transaction on Transferable Securities or Financial Instruments[3] involving the instruments referred to in the Information.

It should be taken into account that the duty to abstain does not apply to the preparation and performance of transactions whose existence is in itself Inside Information, or to transactions carried out pursuant to an obligation, that is already due, to acquire or assign such Transferable Securities or Financial Instruments, if such obligation is envisaged in a contract concluded before the person with Inside Information received the Inside Information. Transactions carried out in accordance with the applicable law are also exempted.

b) disclosing such Inside Information to third parties unless this is necessary for the responsible pursuit of their job, profession, position or role, with the requirements provided for in the RIC.

In particular, this Information may be disclosed by means of a media absolutely guaranteeing the confidentiality of the information:

(i) In the context of the relevant decision-making process, to persons with a higher level of seniority, in such a way that it can be defined as a higher joint structure;

(ii) When the Information is disclosed to the Compliance Unit to enable it to carry out its functions in this field; and

(iii) When expressly approved by the Head of Area[4].

c) Recommending or inducing third parties to acquire or assign Transferable Securities or Financial Instruments, or modify an order relating to them, or to make someone else acquire, transfer or assign them, or cancel or modify an order relating thereto, all this based on Inside Information.

The subsequent disclosure of such recommendations or inducements shall also constitute an unlawful disclosure of Inside Information where the person disclosing the recommendation or inducement knows or should know that it was based on Inside Information. If the person is a legal person, this article shall also apply to those natural persons who are involved in the decision to acquire, transfer or assign, or cancel or modify an order relating to, Transferable Securities or Financial Instruments on behalf of the legal person concerned.

[3] That is, acquiring, transmitting or assigning, directly or indirectly, either on their own behalf or on that of a third party, the Transferable Securities or Financial Instruments or any other security, financial instrument or contract of any kind, whether or not it is traded on a secondary market, whose underlying assets are Transferable Securities or Financial Instruments to which the Inside Information relates. The use of this type of information cancelling or modifying an order relating to the Transferable Security or Financial Instrument to which the information relates shall also be considered Inside Information if the order was given before the interested party had knowledge of the Inside Information.

[4] The Head of Area is –as defined in the ICC– the person in charge of the corresponding unit or division performing the financial, legal or business transaction (under consideration or negotiation) in which Inside Information is received or generated.

The aforesaid restrictions and duties apply to PRISA GROUP personnel and their Related Parties[5], the latter being:

(i) a spouse, or a partner considered to be equivalent to a spouse in accordance with national law in force;

(ii) a dependent child, irrespective of whether or not they live with him;

(iii) a relative who has shared the same household for at least one year on the date of the transaction concerned;

(iv) a legal person, trust or partnership in which the persons covered by the ICC or the persons defined in the preceding paragraphs discharge a managerial responsibility or are in charge of its management; which is directly or indirectly controlled by such a person, which is set up for the benefit of such a person, or the economic interests of which are substantially equivalent to those of such a person; and

(v) any other individuals or entities that are given this status under the legal provisions in force at any given time.

5) What is the duty to safeguard?

Any person who possesses Inside Information has the obligation to safeguard the confidential nature of said Information and avoid disclosing it to other persons, without prejudice to their duty to report to and collaborate with the legal and administrative authorities, where applicable.

Pursuant to this, suitable measures must be adopted to prevent said Inside Information from being subject to abusive or unfair use.

The duty to keep Inside Information confidential will remain until this Information has been communicated to the CNMV or otherwise ceases to be considered confidential, as determined by the Compliance Unit.

6) What steps should be taken in the event that Inside Information is used abusively or unfairly?

Any person who has knowledge that Inside Information is being used in an abusive or unfair manner must immediately notify the Compliance Unit, irrespective of the fact that – depending on the nature of the Inside Information concerned – such an event can be reported via the Whistle-blowing Channel in place at PRISA as per its in-house procedure, bearing always in mind that Inside Information confidentiality shall be guaranteed.

RULES AND PROCEDURES FOR THE HANDLING AND TRANSMISSION OF INSIDE INFORMATION

[5] In short, "Related Persons" are "closely related" individuals: relatives (parents, offspring, siblings living under the same roof, spouses, etc.) as well as companies or enterprises over which the Affected Person has direct or indirect control or in which they hold a significant position.

7) Who decides that information is of a privileged nature?

The Head of Area of the unit or division where this information is generated/received in each instance is responsible for analysing the information to determine whether or not it is Inside Information.

8) What are the principal obligations of the Head of Area?

As soon as the Head of Area decides that the information is of a privileged nature, it must be handled and transmitted according to the provisions laid down in the ICC and this Protocol. In this regard, the Head of Area must:

a) Strictly restrict access to this Information to those persons who need to know about it.

In this regard, special care must be taken to ensure the Inside Information is not disclosed to the Treasury Share Officer[6] and any other individuals managing the treasury share portfolio.

b) Notify the Compliance Unit as soon as possible, by any means absolutely guaranteeing the confidentiality of the information, of projects where Inside Information will be received, generated or handled. Notifications to the Compliance Unit must also include the following details:

(i) the source and nature of the Information;

(ii) the identity of the persons who have had access to the Information

(iii) the date on which this Information became known;

(iv) the Negotiable Securities or Financial Instruments affected; and

(v) confirmation that appropriate measures have been put in place to safeguard the confidentiality of this Inside Information.

c) In any event, the Head of Area may consult the Compliance Unit if he/she is uncertain whether Inside Information is held.

9) What is the Insiders List?

The "Insiders List" is a register that must be created and maintained up-to-date by the Compliance Unit or, where applicable, the person to whom this duty is delegated, and in which the identity of all persons with access to Inside Information shall be included.

The Compliance Unit must ensure that the Insiders List remains confidential.

10) Who can be privy to Inside Information?

The Head of Area is the gatekeeper of Inside Information and is in charge of informing the Compliance Unit of any persons in or outside the PRISA GROUP who are notified of the existence of Inside Information and those who are granted access to this Information (hereinafter the "Insiders" or "Affected Persons").

The Compliance Unit will also establish and notify Insiders of the security measures needed to prohibit unauthorised parties from accessing Confidential Documents.

[6] The Treasury Share Officer is in charge of managing the PRISA GROUP's treasury share portfolio and assumes the functions conferred upon him/her in Heading V of the ICC.

The Compliance Unit will regularly review the Insiders List.

11) What steps must be taken when Inside Information has been accessed without following the established procedure?

Any individuals who possess or believe they possess Inside Information are obliged to inform the Compliance Unit of this circumstance as soon as possible, either directly or through the Head of Area for the purposes of including them in the Insiders List.

Without prejudice to the aforesaid, any Insiders who erroneously or for any other reason disclose or provide access to Inside Information to an unauthorised person are also required to inform the Compliance Unit of this situation through the channels described in the previous paragraph.

12) How can documents containing Inside Information be identified?

For the purpose of protecting the confidentiality of Inside Information, the Head of Area will assign each transaction where Inside Information is generated or received a codename. This codename will be used in all communiqués and documents associated with the transaction, protecting the identity of the parties involved and ensuring the characteristics thereof are not revealed.

All documents containing Inside Information (hereinafter "Confidential Documents") must be clearly marked with the word "CONFIDENTIAL" on the title page and on each of the pages therein, including the date of issue. Regarding computerized documents, a notice indicating that they are confidential must be shown prior to accessing those documents.

13) What are the rules of conduct or criteria to be followed when Inside Information is received?

Insiders must adhere to the following rules of conduct and criteria at all times and wherever they may be:

a) Do not discuss matters concerning Inside Information in conversations with any parties unauthorised to access this Information or in situations or circumstances (e.g. public places or areas in or outside PRISA GROUP offices) where conversations may be overheard by unauthorised parties.

b) Take the utmost care to avoid unauthorised parties seeing Confidential Documents (e.g. during business trips and in public places such as airports, on aircraft or trains, in taxis, etc., or in common areas in PRISA GROUP offices such as the cafeteria, toilets, etc.); and ensure they are not left behind, mislaid or stolen.

c) Keep Confidential Documents on their person at all times, ensuring they are not left in luggage being checked in, inside a vehicle (even if it is locked), or in a hotel room when not occupying it. If Confidential Documents must be left at a hotel, where possible, they should be kept in a safe.

d) Insiders must not use shared local or external network resources to temporarily or permanently store Confidential Documents, unless it can be guaranteed that only these individuals can access the Information contained therein.

e) Confidential Documents in electronic format must be encrypted and the password thereto only known by Insiders. In this regard, a document will be considered as encrypted if the device or location where it is stored is encrypted.

f) Insiders must also take the upmost care while working on Confidential Documents to avoid unauthorised parties from seeing them; and not use any computers, even remotely, that are not adequately protected.

g) Local not networked printers must be used to print Confidential Documents. If local printers are not available, print jobs sent to networked printers must be password protected and copies of the documents must be collected as soon as they are printed out. In any event, the printers must be located in areas with restricted access.

h) When an Insider leaves his/her desk, Confidential Documents must be safeguarded.

i) As far as possible, Insiders must work on Confidential Documents in areas with restricted access and must keep them in locked filing cabinets, the keys or combination numbers of which are only available to these individuals.

14) When must Confidential Documents be destroyed?

Insiders privy to Inside Information must destroy any Confidential Document (both final versions and drafts, copies, extracts and other working documents) related therewith when it is no longer needed, except when it must be kept for legal or business reasons.

15) Who can destroy Confidential Documents?

Only Affected Persons can destroy Confidential Documents. These individuals cannot delegate responsibility for destroying Confidential Documents to anyone not authorised to access them.

Should External Advisors be involved in the destruction of such documentation, the associated service contracts must include clauses that ensure the confidentiality of any Inside Information which the External Advisors have had access to during the destruction thereof. The aforesaid External Advisors may also be required to present certification or another equivalent document confirming that the Confidential Documents have been destroyed.

16) What precautions must be taken when destroying Confidential Documents?

The following rules must be adhered to in addition to any specific rules that may be established by the Head of Area:

a) Confidential Documents and any copies and/or drafts thereof must be destroyed in such a way as to guarantee they are eliminated.

b) When the Compliance Unit or Head of Area determines that it is appropriate and feasible, Confidential Documents in electronic format may be destroyed using a tool that deletes the files in such a way as to render them irrecoverable.

c) When PRISA GROUP computers (on which Inside Information is stored or has been stored) are withdrawn or disposed of, or the hard disk or other data

storage device replaced, said equipment must be destroyed in such a way that the information stored on them cannot be recovered.

17) How can Inside Information be disseminated and/or transmitted?

Express prior approval of the Head of Area is required before Inside Information can be disseminated or transmitted, and in a way that guarantees as far as possible, the most appropriate means are used to ensure the Confidential Documents are received directly by the recipient.

18) What rules or criteria must be adopted when disseminating and/or transmitting Inside Information?

Without prejudice to the additional measures that may be put in place by the Compliance Unit, the Head of Area will determine the criteria for copying, distributing and transmitting Inside Information, allowing this information to be traced. The Head of Area will inform the Affected Persons involved in the transaction in question of these criteria.

The following criteria apply in addition to the rules imposed by the Head of Area on disseminating and/or transmitting Inside Information:

a) With regard to copies of Confidential Documents:

(i) Copies for Affected Persons can only be prepared subject to the Head of Area's express prior authorisation.

(ii) Only Insiders can make copies of Confidential Documents.

(iii) The recipients of copies must be informed that further copies cannot be made.

(iv) The same rules for safeguarding and controlling original Confidential Documents apply for copies thereof.

b) Means of transmitting Inside Information:

(i) Precautions will be taken when discussing Inside Information by telephone. Efforts will be made to avoid using fax machines or electronic means for transmitting Inside Information.

(ii) Where it is unavoidable, recipients must be notified before Inside Information is sent by fax to ensure they collect the document as it prints out.

(iii) If Information is disseminated by electronic means, it must be ensured that these devices can only be accessed by the recipient.

c) Preferably, hard copies of Confidential Documents must be transferred in person. If this is not possible:

(i) It will be transmitted in a sealed envelope addressed to the recipient Affected Person and with the word "CONFIDENTIAL" clearly shown on the outside.

(ii) The envelope must be a single use security envelope enabling any unauthorised opening to be detected.

(iii) An email must also be sent to the recipient informing them that the Information is being sent, without indicating the nature thereof. The recipient will be required to send a reply confirming receipt of this email.

19) How must Inside Information be sent outside the Company?

Confidential Documents can only be sent outside the Company by authorised personnel, implementing the security measures needed to ensure they are sent securely.

Confidential Documents must be sent outside the Company by courier and confirmation of delivery obtained. In any event, such dispatches must be logged in a ledger showing documents received and sent.

During delivery, Confidential Documents must be stored at locations that meet the access control and storage requirements specified above. The Company must be notified immediately if deliveries are lost or stolen.

20) What are the criteria for transmitting Inside Information to External Advisors?

Further to the rules and criteria defined in the previous headings, Inside Information will only be transmitted to External Advisors when the Head of Area determines that it is necessary. The following rules particularly apply in such circumstances:

a) The Compliance Unit must be informed that the External Advisors are privy to the Inside Information.

b) The Inside Information will be transmitted to the External Advisors as late as possible depending on the transaction in question.

c) External Advisors will be included in the Insiders Ledger.

d) In the event an External Advisor is not already professionally bound by a confidentiality obligation, prior to any Inside Information being transmitted to that External Advisor they must sign a confidentiality agreement indicating the confidential nature of the information to which they will be privy, their inclusion in the Insiders Ledger, and their duty to comply with and to ensure that their staff comply with prevailing legislation, and the provisions of the ICC and this Protocol regarding the handling and transmission of Inside Information.

e) External Advisors must be requested to keep their own ledgers of individuals who have access to the Inside Information, stating the reason for and date on which each person became privy to or accessed this Inside Information, and specifying the type of information concerned.

21) What criteria apply to communications with analysts or the media about transactions which contain Inside Information?

Transactions, events or projects, which still remain confidential, shall not be communicated to analysts or media. If any doubts arose in this respect, the Compliance Unit or, if applicable, the Chairman of the Board, the Secretary of the Board or any of the officers responsible for liaising with the National Securities Market Regulator (CNMV) shall be previously consulted.