GUIDE FOR ACTION ON THE TRANSMISSION OF INSIDE INFORMATION TO THIRD PARTIES

SECONDARY MARKETS DIRECTORATE

9 MARCH 2009

I INTRODUCTION 3

II SCOPE OF THE GUIDE 4

1. OBJECTS TO WHICH THIS GUIDE APPLIES 4

2. PARTIES TO WHICH THIS GUIDE APPLIES 4

III MEASURES 5

1. ORGANISATIONAL 5

2. EMPLOYEE TRAINING AND INFORMATION 6

3. SAFEGUARDING AND CONTROLLING INFORMATION 7

4. COMMITMENTS AND CONTACT WITH THIRD PARTIES 9

5. TRADING WITH FINANCIAL INSTRUMENTS 10

6. LIST OF INSIDERS AT RECIPIENTS OF INSIDE INFORMATION 10

I. INTRODUCTION

Article 82 of Spain's Securities Market Act (hereinafter, the SMA) obliges issuers to disclose any significant information simultaneously to both the market and the CNMV, in order to grant all investors simultaneous access to the same information potentially affecting their investment decisions. Disclosure by any other means that does not conform to the regulations, or the leaking of significant information, undermines investor confidence in the integrity and efficiency of the securities markets, since a small number of people may benefit from such information.

Based on this idea, article 81.4 of the SMA establishes that all people and institutions acting in securities markets or performing activities linked thereto, and generally any person holding inside information is obliged to safeguard it and to implement adequate measures to prevent the information from being abused or misused.

Furthermore, in accordance with article 83 of the SMA, companies or groups of companies that provide investment services, operate in the securities markets or provide investment advisory services are obliged to establish the necessary measures to prevent inside information from flowing between their different areas of activity, so as to guarantee that each area makes its decisions independently and thereby avoid conflicts of interest.

Moreover, article 83 bis.1 of the SMA obliges issuers, while studying or negotiating legal or financial transactions, to protect the confidentiality of information concerning those transactions that might significantly impact the price of their securities or the financial instruments in question.

However, in practice, there are situations in which it is necessary or advisable to provide inside information to certain authorities or professionals not linked to the issuer generating it, and this disclosure must also be considered legitimate, but it is also subject to the duty of confidentiality as provided by article 7.2 of Royal Decree 1333/2005, dated 11 November. As part of the Initiative Against Market Abuse (ICAM) launched in 2007, the CNMV set as a priority objective that those legitimately handling inside information should take the utmost precautions to prevent its improper use. Apart from a penalty for the non-compliant party, failure to comply with the regulations regarding the custody and safekeeping of inside information has very negative consequences for the integrity of the market as a whole. Accordingly, it is necessary to adequately plan and implement a series of measures that have proved to be successful and effective, both domestically and worldwide.

In the CNMV's experience, measures to safeguard inside information could be improved by securities issuers and professionals and third parties who have legitimate access to this information for professional reasons.

This Guide contains a series of non-binding measures and recommendations to help ensure the confidentiality of inside information held by issuers and disclosed to third parties in accordance with the SMA. These measures and recommendations are addressed to both the sources and recipients of this information.

II. SCOPE OF THE GUIDE

1. OBJECTS TO WHICH THIS GUIDE APPLIES

The measures and recommendations contained in this Guide are the criteria to be followed in the disclosure of information under the provisions of articles 81.2 b) and 83 bis 1 of the SMA in respect of any inside information as defined in article 81.1 of the SMA.

The CNMV is particularly interested in entities applying these measures, with the flexibility required by each institution, to the transmission of inside information to third parties in the context of analysing and negotiating corporate or financial transactions. However, the references in this Guide to ""transactions" should be interpreted in the broadest sense and, therefore, includes any event or circumstance that constitutes inside information.

The purpose of the measures and recommendations contained in this Guide is to safeguard the confidentiality of inside information and prevent leaks and the ensuing risk of improper use of the information.

2. PARTIES TO WHICH THIS GUIDE APPLIES

2.1. Sources of information

The issuer of securities and other companies in its group (hereinafter, the issuer) that disclose inside information, via members of their board of directors, senior management, employees (under labour or mercantile contracts) and representatives, to any of the persons or entities listed in the following section is considered to be a source of inside information.

Furthermore, any person or entity operating in the securities markets or performing activities related thereto and, in general, anyone possessing inside information who legitimately discloses the information to the persons or entities listed in the following section is considered to be a source of inside information.

2.2. Recipients of information

Recipients of information include, on the one hand, any persons or entities external to the issuer and its group that need to know the information in order to provide professional services (e.g. to provide advice or analyse a corporate or financial transaction) and, on the other hand, the administrative authorities which require the information in order to perform their duties.

Direct recipients of information will, in turn, be considered to be sources of inside information when they disclose the information to third parties provided they deem this to be strictly necessary in order to perform their duties.

For the purposes of this Guide, there follows an non-exhaustive list of possible recipients of inside information:

- Administrative authorities
- Auditors
- Appraisers and valuers
- Rating agencies
- Financial institutions

- Consultants
- Attorneys
- Notaries and registrars
- Potential counterparties, for the purposes of studying specific transactions requiring the analysis of inside information
- Advertising agencies, communication agencies and printers, in the final phase of communicating and documenting a project or transaction
- Translators.

The CNMV considers it advisable for administrative authorities, which are legally bound to uphold secrecy, to consider (to the appropriate extent) the application of the main principles of this Guide (and some of the measures that may be applicable) to help safeguard the confidentiality of inside information.

In view of the varied nature of the possible recipients (from financial institutions to printers), application of the measures contained in this Guide require an adequate evaluation of the kind of professional or institution in question, the frequency with which they provide services, the degree of specialisation and their knowledge of securities market legislation, the applicable laws or regulations and the kind of information being handled.

III. MEASURES

The measures set forth below are intended as guidelines to both providers and recipients of inside information, inasmuch as their application may help to better manage and control the transmission of such information. For this purpose, each entity, whether a source or recipient, should consider the feasibility, effectiveness and advisability of implementing these measures, and may opt not to implement any of them that it does not consider appropriate or, indeed, to apply measures other than the ones mentioned here.

1. ORGANISATIONAL

Organisational systems must be aligned so as to achieve the utmost degree of compliance with the rules on preserving inside information. The procedures, organisational structure and communication methods must emphasise the responsibility of holding inside information and the need to prevent its improper use. Some good practices in this connection are as follows:

1.1. Internal Codes of Conduct (and equivalent standards in the case of non-issuers) of both sources and recipients should include the general principles of their policies on handling inside information.

1.2. These policies and internal procedures should be drafted, implemented and applied in a way that is commensurate with the size and nature of their business; they should be duly documented; they should be approved and reviewed periodically (for example, by the Audit and Control Committee, Board of Directors or another competent body); and they should be distributed internally to all employees to whom they might apply. Furthermore, it would be useful for a body, either internal or external, other than the body that established the procedures to assess their efficacy on a regular basis.

1.3. The issuer's internal procedures should specify the persons (executives, CEO, etc.) or bodies with the power to activate the mechanisms for classifying a corporate or financial transaction ("Transaction") as inside information.

1.4. The issuer should designate an executive or permanent body (e.g. the Compliance Unit) with the responsibility for applying and supervising general compliance with the control measures established for these situations of selective disclosure of inside information (hereinafter, the issuer's Head of Compliance[1]).

1.5. An executive should be placed in charge of each Transaction, tasked with managing the inside information, determining which information should be disclosed and to whom, and immediately notifying the Head of Compliance about all persons, inside and outside the organization, to whom the existence of the inside information has been notified and who have been afforded total or partial access to this information, so that the Head of Compliance can promptly set up the documentary record referred to in article 8 of Royal Decree 1333/2005 (list of insiders) and keep the persons referred to in measure 1.3 up to date on a permanent basis.

1.6. Recipients of inside information should designate an executive or permanent body (e.g. the Compliance Unit) with the responsibility for providing advice and enforcing compliance with the pertinent procedures and measures in order to uphold the confidentiality of the information (hereinafter, the recipient's Head of Compliance). Recipients of inside information must immediately notify its existence to their Head of Compliance.

1.7. Where appropriate, information barriers should be established between the various departments of an institution and even within the same department, and the form of communication between them should be set out in the internal procedure mentioned in measure 1.2.

1.8. Before disclosing any inside information to a potential recipient, confirmation should be obtained from the latter that it has established the measures required to safeguard the confidentiality of the information it will receive.

1.9. Clear and specific measures should be established concerning communications with the media in respect of transactions that are still in a confidential phase, including submitting external communications regarding the project, event or transaction for the approval of the Head of Compliance.

2. EMPLOYEE TRAINING AND INFORMATION

The purpose of these measures is to create a culture of compliance within the organisation, including the ancillary personnel who provide support to persons directly or indirectly related to the inside information, with the standards and procedures needed to preserve the inside information and increase awareness within the organisation in respect of these matters. The following good practices are notable:

2.1. Remind members of the internal group who will work with the inside information, as often and in the manner that each institution sees fit, of the regulations applicable to them and the general principles governing the institution's actions and the internal procedures for safeguarding inside information. The Head of Compliance will be responsible for applying both this measure and the next one.

[1] References to the Head of Compliance in the measures proposed in sections 1.5, 1.9 and 2.1 should also be understood to apply to persons who have been specifically assigned these duties, even where there is no specific position.

2.2. Implement an employee training and information plan regarding the obligation to safeguard inside information and to report leaks and improper use of inside information when detected, based on the protocol set out in measure 3.3.7. Such information measures can include periodic internal bulletins, internal memos and reminders, on-line courses or seminars to detail the internal regulations and procedures for handling inside information, etc.

2.3. Notify employees, executives and directors of the measures concerning the prohibition and restriction of transactions with financial instruments, also applicable to employees' relatives and related parties.

2.4. Both in writing and verbally, inform employees possessing inside information who abandon the organisation of their duty to continue to comply with the legal obligation to safeguard confidentiality.

3. SAFEGUARDING AND CONTROLLING INFORMATION

Both sources and recipients of inside information should establish internal measures to safeguard this information and control the traceability, access and delivery of documents containing inside information.

3.1. Implement measures to identify communications and their content, the project, the Transaction and the inside information as a whole. Examples of such measures are:

3.1.1. Assign a code name to the Transaction to which the inside information refers. Use the code name in all communications so that neither the parties involved nor the characteristics of the Transaction may be identified.

3.1.2. Visibly and clearly label all material media (documents, texts, reports, software, files, etc.) containing inside information with the word CONFIDENTIAL or a similar term.

3.1.3. Mark all e-mails, envelopes and faxes as CONFIDENTIAL.

3.2. Implement measures to limit access solely to previously-authorised persons. Examples of this kind of measure are:

3.2.1. Encrypt computer documents using a password known only to members of the team that will work with the information.

3.2.2. Establish restricted access areas in the computer network to prevent unauthorised access to confidential documents.

3.2.3. Never share the passwords of the team members' computers.

3.2.4. Never use any computer, even when working remotely from outside the office, that does not have an adequate security system installed.

3.2.5. Periodically verify and optimise the robustness of the IT security measures and adapt them to new information or identity theft techniques and methods.

3.2.6. When appropriate, a closed room should be available as a work space. All team members should ensure that all documents relating to the work are kept locked in the room or in a locked filing cabinet when not in use, as well as ensuring that they do not leave any notes on whiteboards or other similar material. When no such room is available, material media containing inside information should be kept in a specific location with protective measures.

3.2.7. Avoid leaving in sight of unauthorised persons any material being worked on (computer screens, papers on desks) which could reveal information regarding the existence or content of the Transaction.

3.3. Establish measures to ensure the proper delivery solely to insiders. Examples of such measures are:

3.3.1. Label written documents with a reference number, bar code or specific mark for each recipient of inside information.

3.3.2. Require prior authorisation for any copy of confidential documents.

3.3.3. Refrain from making second copies of confidential documents received.

3.3.4. Refrain from talking about inside information, even using code names with other insiders, and from handling material containing inside information (presentations or documents on paper or on a computer) in public places where it might be heard or seen by third parties. In particular, avoid holding conversations, both in person and by telephone, in areas where there is a risk of being overheard by persons who should not be party to the information, such as elevators, taxis, restaurants, aircraft, trains, buses, etc.

3.3.5. Implement strict security measures when using communications that may be insecure, such as mobile telephones, fax or e-mail. Set mobile devices (laptops, PDAs, mobile phones equipped with e-mail) to lock when idle.

3.3.6. Use the most suitable measures to ensure direct receipt of confidential documents by the correct addressee. For example, avoid sending information to devices that are unattended at the time or to which persons other than insiders may have access.

3.3.7. Establish, in the internal procedure mentioned in measure 1.2, a protocol for action in the event of detecting a leak or improper use of inside information, including the following points:

- Immediate notification, via secure channels, to the persons designated under the internal procedure, of any leak of inside information detected by an employee.
- Maximum protection of the identity of the person reporting the leak, including the absolute guarantee of anonymity, if necessary.
- As soon as possible, the recipient's Head of Compliance should notify the issuer's Head of Compliance that the leak has taken place so that, among other things, the latter can decide whether article 83 bis 1.f of the SMA is applicable and whether illegal conduct has taken place and should be reported to the authorities.

3.3.8. Establish mechanisms, when proportionate and feasible, to permit the detection of leaks or unauthorised deliveries of inside information. These mechanisms will also be designed to facilitate a subsequent audit of the procedures to trace the source of leaks.

3.3.9. Develop a specific procedure for destroying confidential documentation relating to the Transaction so as to ensure that no unauthorised persons have access to it (e.g. using a specialised company or through personal participation by a member of the team, creating a list of all destroyed documents, etc.).

3.3.10. File documents, copies or any other texts that refer to inside information in a location to which unauthorised persons do not have access, once the Transaction has been completed, suspended or cancelled or the professional services engaged by the source of the information have concluded.

4. COMMITMENTS AND CONTACT WITH THIRD PARTIES

These measures are aimed at explaining and recapping the implications of being party to inside information, and at urging extreme caution in the handling of such information vis-à-vis third parties, based on the following proposed best practices.

4.1. Inform third parties of the Transaction or include them in it as late as possible.

4.2. With external recipients (except those subject to laws or regulations that include the duty of confidentiality) enter into a non-disclosure agreement or commitment (which could be based on a pre-existing framework agreement) in which the recipient acknowledges to the source of the information that it is aware of the confidential nature of the information being provided and setting forth the specific conditions in which the recipient must maintain confidentiality and those in which it may transmit the information to other external persons. Where the recipient transmits the inside information to third parties, it must also remind them that the information is confidential.

4.3. Verbally explain the content and implications of the non-disclosure agreement, particularly when the third parties in question may not be familiar with the applicable legislation.

4.4. Maintain the confidentiality obligation until such time as determined by the Heads of Compliance or persons indicated in measure 1.3 or until all the essential elements of the inside information become publicly available; in other words, until it has been released as a Regulatory Disclosure (" Hecho Relevante") and the necessary time has elapsed, in accordance with the internal policies of each entity in this connection, for the market to know the details of the Transaction.

4.5. Require, furthermore, that the following persons and entities uphold the duty of confidentiality:

- Those persons external to the information source with whom the latter contacts during a preliminary phase and who are given a general overview of the Transaction in order to request financing or advisory services, but who do not ultimately participate in the Transaction. In these cases, it is considered good practice to expressly reiterate the warnings regarding the restricted nature of the Transaction at the time of notifying the entity that it has not been chosen to provide finance or advisory services.
- External recipients of inside information who cease to provide services to the information source before the Transaction is completed, suspended or cancelled.

5. TRADING WITH FINANCIAL INSTRUMENTS

These measures are aimed at preventing the abuse or misuse of inside information through breach of the prohibitions against trading, disclosing or recommending trades based on the information.

5.1. Notify in writing to the employees, executives and directors who are party to the content or existence of inside information of the financial instruments (including derivatives) which they are not allowed to trade or recommend to third parties for trading (banned securities) and any others in respect of which it is necessary to request authorisation (restricted securities), in accordance with the provisions of the internal regulations. This measure applies to both the source and the recipient of inside information.

5.2. Maintain restrictions with regard to trading in those financial instruments during a prudent period after the Transaction has concluded or been announced to the market. This period may be established beforehand either broadly or for specific transactions and must be notified in advance to employees.

5.3. The issuer (except where permitted under applicable regulations) and recipients of inside information should comply with the ban and restriction referred to in measure 5.1 in respect of trades they perform as legal entities, unless they already have effective measures in place in order to prevent the transmission of inside information (such as information barriers between departments).

5.4. Establish mechanisms to prevent the use of inside information in the internal policy on personal trading in financial instruments by employees, executives and directors. These include the following, for example:

- The Head of Compliance should periodically issue reminders of the need to observe the regulations established in internal policy.
- Establish the mechanisms for reporting and regularly updating personal trades.
- Exempt from compliance with the obligation and restriction referred to in measure 5.1 those trades performed on behalf of employees, executives and directors who have entrusted an institution with the discretionary and individualised management of investment portfolios, when there is no prior communication between the manager and the person on whose behalf the trade is performed, and personal trades in shares or units of UCITS, as provided by article 35.3 of Royal Decree 217/2008.

6. LIST OF INSIDERS AT RECIPIENTS OF INSIDE INFORMATION

Since recipients of inside information sometimes also become sources thereof, this measure is aimed at ensuring that external recipients also maintain control of the information.

6.1. The Head of Compliance at the recipient should also have his own "list of insiders". This list should include all the internal and external persons who are made aware of the information and should indicate whether they have full or partial access to it. This record should state the reason and date on which each person became aware of, or had access to, the information.