CENTRAL BANK OF THE RUSSIAN FEDERATION

No. 23-MR dated 14 September 2018

RECOMMENDED PRACTICE FOR THE DEVELOPMENT AND APPROVAL OF THE ORDER OF ACCESS TO INSIDER INFORMATION AND THE RULES FOR PROTECTING ITS CONFIDENTIALITY

ConsultantPlus: note.
Cl. 2 of Article 4 of Federal Law No. 224-FZ dated 27.07.2010 became null and void from 01.05.2019 in connection with enactment of Federal Law No. 310-FZ dated 03.08.2018.

This Recommended practice is developed in accordance with clause 11 of part 1 of Article 14 of Federal Law N 224-FZ dated July 27, 2010 "On counteracting the unlawful use of insider information and market manipulation and on amendments to certain legislative acts of the Russian Federation" (hereinafter - the Federal Law) in order to provide methodological assistance to legal entities referred to in clauses 1 - 8, 11 and 12 of Article 4 of the Federal Law (hereinafter referred to jointly as entities), in the development and approval by them the access to insider information and rules for the protection of its confidentiality, in compliance with clause 1 of Article 11 of the Federal law.

Chapter 1. General Provisions

1.1. It is recommended that the entities shall provide for the following provisions within the procedures developed and approved by them for access to insider information and the rules for protecting its confidentiality:

1.1.1. The principles of organizing processes to ensure access to insider information, its safety and protection, including the following principles:

the principle of following ethical standards (if any);

the principle of continuity and effectiveness of the process of protecting and preserving insider information;

the principle of preventing a conflict of interest in the circulation of insider information;

the principle of conformity of measures to ensure the protection and safety of insider information, including the prevention, detection and suppression of its misuse, the nature and scope of the entity’s activities.

1.1.2. The list of measures to ensure access, protection and safety of insider information, the adoption of which is recommended in accordance with Chapter 2 of this Recommended practice.

1.1.3. The procedure and terms for taking measures to prevent the unlawful use of insider information in the presence of information received from internal and external sources, including information about signs of unfair behavior of employees, as well as members of the entity’s management bodies.

1.1.4. The list of measures to ensure the prevention of illegal disclosure and (or) use of insider information by employees of the entity and (or) other persons who became aware of insider information, including by chance, in their own interests or in the interests of third parties, as well as the consequences resulting from illegal disclosure and (or) use of insider information.

1.1.5. The procedure for informing employees of the entity and its management bodies about requirements for compliance with the Federal Law and regulatory acts adopted in accordance with it.

1.1.6. The procedure for familiarizing employees of the entity and its management bodies with the current versions of the entity's internal documents developed in accordance with part 1 of article 3, part 1 of article 9, article 11 and parts 1 to 3 of article 12 of the Federal Law.

1.1.7. Ways to confirm the fact that employees who have access to insider information, as well as the persons set forth in subclause 1.1.16 of this clause, are familiar with the current list of insider information, the procedure for access to insider information, the rules for protecting its confidentiality, the requirements of the Federal Law and adopted in accordance with regulations on the consequences of the unlawful use of insider information, as well as the procedure for storing documents confirming such familiarization.

1.1.8. The procedure and frequency of training employees, including the persons referred to in subclauses 1.1.15 - 1.1.17 of this clause, as well as in clause 2.2.14 of of this Recommended practice, in order to increase their awareness of the rules for handling insider information and understanding the consequences as a result of their violation.

1.1.9. The rights and obligations of persons responsible for ensuring access, protection and safety of insider information, including an official (employees of a structural unit), whose duties include monitoring compliance with the requirements of the Federal Law and regulations adopted in accordance with it (hereinafter - the Responsible Official).

1.1.10. Rights and obligations of the entity's management bodies approving internal documents developed by entities in accordance with part 1 of article 3, clause 1 of part 1 of article 9, article 11 and parts 1 to 3 of article 12 of the Federal Law in order to protect and preserve insider information and implement measures to prevention, detection and suppression of its unlawful use.

1.1.11. The procedure for the formation and functioning of working (project) groups created for the operational solution of the entity's tasks requiring insider information processing, which, by the organization's decision, may include, in addition to the entity's employees, who have access to insider information for the performance of their duties, the employees of structural divisions whose official duties do not include obtaining insider information (hereinafter referred to as working (project) groups), as well as the procedure for provision of the working (project) groups with insider information.

1.1.12. The procedure for notifying persons included in the list of insiders of their inclusion in the list of insiders in accordance with clause 2 of Part 1 of Article 9 of the Federal Law before transferring insider information to them.

1.1.13. The procedure for maintaining the following lists:

the list of issuers in respect of which the insider information was received by the entity and transactions with respect to financial instruments of which are possible for the entity, as well as financial instruments with respect to which the insider information was received by the entity and transactions with which are possible for the entity (hereinafter - the observation list);

the list of issuers in respect of which the insider information was received by the entity and transactions with respect to financial instruments of which are prohibited for the entity, as well as financial instruments with respect to which the insider information was received by the entity and transactions with which are prohibited for the entity (hereinafter - the stop-list);

1.1.14. The procedure for familiarization with and access of the entity's employees to the information contained in the stop-list and observation list, and the rules for storing information contained in the stop-list and observation list.

1.1.15. Rights and obligations in the field of ensuring access, protection and safety of insider information of employees of a structural unit units) of an entity whose official duties, by virtue of agreements concluded with the entity's clients, are related to receiving insider information from entity's clients, including rights and obligations in the field of ensuring access, protection and safety of insider information of persons engaging the clients and persons evaluating engaged clients in accordance with requirements of the Russian Federation laws and (or) internal documents of the entity.

1.1.16. Rights and obligations in the field of ensuring access, protection and safety of insider information of employees of an entity's structural unit of an entity whose official duties include performing transactions for the benefits of the entity, including rights and obligations in the field of ensuring access, protection and safety of insider information of persons making decisions on performing transactions for the benefits of the entity, and persons conducting a preliminary assessment of the terms and conditions of transactions concluded by the entity, including their compliance with requirements of the Russian Federation laws (if such an assessment is carried out).

1.1.17. Rights and obligations in the field of ensuring access, protection and safety of insider information of employees of the entity's structural unit who provide analytical materials to the persons set forth in subclause 1.1.16 of this clause, and (or) public information to participants of the financial market, which is used in transactions with financial instruments, foreign currency and (or) goods.

1.1.18. The list of measures ensuring the exclusion of unauthorized access to the premises of the structural units set forth in subclause 1.1.15 of this clause, and to the workplaces of employees of such structural units.

1.1.19. Prohibition for employees of the structural units set forth in subclauses 1.1.16 - 1.1.17 of this clause to access insider information received from the entity's clients.

1.1.20. Restriction on the use by employees of the structural units set forth in subclause 1.1.16 of this clause of personal communications, personal computers and personal machine-readable media (flash drives, external hard drives and other devices) while carrying out their duties.

1.1.21. Restriction on the transfer of identification and authentication tools by the entity's employees having access to insider information when they used them when operating with insider information, to third parties.

1.1.22. The list of persons to whom the entity provides access to insider information, the procedure for transmitting insider information to these persons, including with the consent (without the consent of the Responsible Official), containing a request form for providing insider information, requirements for the content of the request, including justification for the need to obtain insider information, the terms of consideration of the request, the grounds for refusing to provide consent to the transfer of insider information, the consequences of violating the procedure for using and storing insider information.

1.1.23. The procedure for maintaining and storing the insider information transfer log, including an indication of the recording the date and time of insider information transfer, information about the persons transferring and receiving insider information, the nature of the insider information being transferred and the method of its transfer, the provision of consent to transfer insider information by the Responsible Official or other authorized person.

Chapter 2. Separate measures to ensure access to insider information, its protection and safety

2.1. Entities are encouraged to include in the procedure for access to insider information developed and approved by them and the rules for protecting its confidentiality, the measures provided for in clause 2.2 of this Recommended practice.

2.2. Entities are encouraged to take separate measures to ensure access to insider information, its protection and safety:

2.2.1. Ensuring the prevention of the implementation of functions by the structural units set forth in subclauses 1.1.15 - 1.1.16 of clause 1.1 of this Recommended practice that are not within the competence of such structural units.

2.2.2. The arrangements for workplaces for structural units' employees having access to insider information of the entity, as well as for the employees of structural units set forth in subclause 1.1.15 of clause 1.1 of this Recommended practice, in rooms separated from each other, as well as from rooms where workplaces of employees of other structural units of the entity are located.

If it is impossible to split workplaces, the entities are encouraged to develop other affordable and reasonable measures aimed at protecting and preserving insider information.

2.2.3 Ensuring the location of computer monitors for the employees who have access to insider information of the entity, as well as for the employees of structural units set forth in subclause 1.1.15 of clause 1.1 of this Recommended practice, eliminating the risks of other persons familiarizing themselves with insider information, including if the entity does not provide securing computers directly to a specific employee.

2.2.4. Differentiation of access rights to the databases of employees entering insider information into the databases and employees performing subsequent processing of insider information.

2.2.5. Ensuring the exclusion of unauthorized access to workplaces, computers, machine-readable media of the entity's employees having access to insider information of the entity, as well as employees of structural units of the entity set forth in subclause 1.1.15 of clause 1.1 of this Recommended practice, by employees of other structural divisions, including by the officials referred to in the third paragraph of clause 2.2.12 of this Recommended practice, by means of identification and authentication of the access subjects and objects, including the assignment of of unique access token (identifier) for the access subjects and objects.

2.2.6. Providing control over the transfer of tools of identification and authentication of the entity's employees having access to insider information of the entity, employees of (structural unit) structural units of the entity set forth in subclause 1.1.15 of clause 1.1 of this Recommended practice, as well as the Responsible Official, to other persons.

The entities are encouraged to be guided by Chapter 7 of the national standard of the Russian Federation GOST R 57580.1-2017 "Security of financial (banking) operations, while ensuring access to insider information. Protection of information of financial entities. The basic structure of organizational and technical measures "in part of process 1 "Ensuring the protection of information during access control".

2.2.7. The installation of copying machines, printers, and similar devices used by employees of the entity having access to insider information of the entity, as well as employees of the structural units set forth in subclause 1.1.15 of clause 1.1 of this Recommended practice, in places not accessible to other persons.

2.2.8. Ensuring compliance with restrictions on the use of personal communications, computers, machine-readable media by employees of the structural units set forth in subclause 1.1.16 of clause 1.1 of this Recommended practice while carrying out their duties.

2.2.9. Negotiations, including negotiations with the entity's clients, in separate premises (negotiation rooms), ensuring the exclusion of the possibility of unlawful dissemination of information about the fact and content of these negotiations, in the event of a risk of misuse of insider information.

2.2.10. Storage of documents containing information constituting insider information in places to which access is limited (for documents in hard copy, machine-readable media, it is recommended to provide lockable places (safes, cabinets, rooms, etc.).

2.2.11. Ensuring the exclusion of a conflict of interest and obtaining the consent of the Responsible Official or other authorized person obtained in the manner and within the terms stipulated by the procedure for access to insider information and the rules for protecting its confidentiality, when transferring (if necessary) insider information of the entity's clients to structural units performing operations in the entity's own interests, as well as to decision-makers on such transactions, and to persons conducting a preliminary assessment of the conditions of transactions, concluded by the entity, including their compliance with the Russian laws (when such an assessment is carried out).

2.2.12. Ensuring the possibility of transferring insider information without the consent of the Responsible Official or other authorized person in the following cases:

when transferring insider information within working (project) groups;

when transferring insider information to officials determined by the entity;

when transferring insider information received by the working (project) group to persons whose official duties do not include obtaining insider information, as well as when transferring insider information to the working (project) group, it is recommended to be guided by clause 2.2.11 of this Recommended practice.

2.2.13. Notification of information on the establishment of a working (project) group, including the subject and period of activity, its composition, to the Responsible Official or other authorized person.

2.2.14. Definition of officials to whom insider information is transferred without the consent of the Responsible Official or other authorized person from among the employees performing the following functions:

administrative and regulatory functions;

functions of internal control over the entity's operations;

entity's risk management functions;

entity's internal audit functions;

entity's legal support functions;

entity's functions of ensuring information and economic security.

2.2.15. Ensuring compliance with the ban on transactions by the entity for its own benefits with financial instruments included in (whose issuers are included in) the stop-list.

2.2.16. Ensuring timely familiarization of the entity's employees and its management bodies with the procedure for access to insider information and the rules for protecting its confidentiality.

2.2.17. Regular training of persons set forth in this Recommended practice in order to increase their level of knowledge in the field of access, protection and safety of insider information.

Chapter 3. Final Provisions

This Recommended practice is subject to publication in the Bulletin of the Bank of Russia.

First Deputy
Chairman of the Bank of Russia.
S.A. SHVETSOV