Guideline Concerning Protection of Personal Information

(Purpose)

Article 1.

1. The purpose of this Guideline (hereinafter referred to as "Guideline") is to prescribe—by taking into consideration, among others, the Act on the Protection of Personal Information (hereinafter referred to as "Protection Act"), the Order for Enforcement of the Act on the Protection of Personal Information (hereinafter referred to as "Enforcement Order"), the Enforcement Rules for the Act on the Protection of Personal Information (hereinafter referred to as "Enforcement Rules"), the Basic Policy on the Protection of Personal Information (cabinet decision), the Guideline for the Act on the Protection of Personal Information (General Rules (Public Notice of the Personal Information Protection Commission No. 6 of 2016), Provision to Third Party in Foreign Country (Public Notice of the Personal Information Protection Commission No. 7 of 2016), Obligation to Confirm/Record When Effecting Third Party Provision (Public Notice of the Personal Information Protection Commission No. 8 of 2016), and Anonymously Processed Information (Public Notice of the Personal Information Protection Commission No. 9 of 2016); hereinafter collectively referred to as "Personal Information Protection Commission Guideline"), and the Guidelines for Protection of Personal Information in the Finance Sector (Public Notice of Financial Services Agency No. 1 of 2017; hereinafter referred to as "Guidelines in Finance Sector")—concrete measures, etc. that should be taken by Regular Members and Electronic Public Offering Members for the purpose of ensuring proper handling of Personal Information in Self-Offering and Other Transactions, etc. (referring to the Self-Offering and Other Transactions, etc. provided for in Item (9) of Article 3 of the Articles of Incorporation) conducted by Regular Members and Electronic Public Offering Members.
2. Each Regular Member and Electronic Public Offering Member needs to establish a proper system to manage Personal Information according to Protection Act, Enforcement Order, Personal Information Protection Commission Guideline, Guidelines in Finance Sector, and other related laws and regulations, etc. in order to achieve such objectives as prevention of leakage or illegal distribution, etc. of Personal Information.

(Definitions)

Article 2.

In this Guideline, the terms set forth in each of the following Items shall have the definition ascribed to it in the relevant Item.

(1) Personal Information

This refers to the information regarding a living individual (not limited to the information such as individual name, address, gender, date of birth and facial image which identifies the individual, but includes all information that indicates facts, judgments or assessments on personal attributes such as physical features, assets, occupational category or title, including assessment information, information which has been made public by publications, etc. and information in the form of image or sound, regardless of whether it is being secured through encryption, etc.) which falls under any one of the following:

(a) Information containing individual name, date of birth, or other descriptions, etc. (referring to any and all matters (excluding Individual Identification Code) stated or recorded in document, drawing or electromagnetic record, or indicated by sound, motion or any other means) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby can identify a specific individual); or

(b) Information containing Individual Identification Code.

In the case where any information about a deceased individual at the same time constitutes information about a living individual such as a surviving family member, such information constitutes information about the living individual. Furthermore, although information about juridical person or any other group, such as a name of corporation, does not constitute "Personal Information" in principle, if a part of such information contains information about an individual such as a name of its officer, that part constitutes "Personal Information."

Moreover, the term "individual" includes foreign national as a matter of course.

(2) Individual Identification Code

This refers to any character, letter, number, symbol or any other code prescribed in Article 1 of Enforcement Order which can, by itself alone, identify a specific individual.

(3) Personal Information Database, etc.

This refers to a set of information which contains Personal Information and is set forth below; provided, however, that the information which is prescribed in Article

3, Paragraph 1 of Enforcement Order as having little possibility of harming individual's rights and interests in the light of the method of its use is excluded.

(a) A set of information which is systematically structured to enable search for particular Personal Information by using computer; or

(b) Other than what is described in (a), a set of information which is systematically structured by arranging Personal Information in accordance with certain rules to enable search for particular Personal Information easily, and kept under such a condition so that one can easily perform search by using a list of contents, indexes, symbols, etc.

(4) Personal Data

This refers to Personal Information comprising Personal Information Database, etc.

(5) Retained Personal Data

This refers to the Personal Data over which the relevant Regular Member or Electronic Public Offering Member has the entire authority to make its disclosure, to make correction or addition to or removal of its contents, to suspend its use, to make its deletion, or to suspend its provision to a third party, in response to a request made by Individual Concerned or his/her agent, except for the Personal Data set forth below and the Personal Data that is to be deleted within a 6-month period (other than such Personal Data that is to be renewed):

(a) Personal Data which, once its existence or nonexistence becomes known, is likely to result in giving rise to a threat to the life, body, or property of Individual Concerned or a third party;

(b) Personal Data which, once its existence or nonexistence becomes known, is likely to result in promoting or inducing unlawful or unjust act;

(c) Personal Data which, once its existence or nonexistence becomes known, is likely to result in endangering national security, damaging the relationship of trust with other nation or international organization, or causing disadvantage in negotiation with other nation or international organization; and

(d) Personal Data which, once its existence or nonexistence becomes known, is likely to result in hindering prevention, suppression or investigation of crime, or hindering maintenance of public safety and order in other forms.

(6) Individual Concerned

This refers to a specific individual who can be identified by Personal Information.

(7) Special-Care-Required Personal Information

This refers to the Personal Information which contains the race, belief, social status, medical history, criminal record or fact of having been victimized of a crime, in respect of Individual Concerned, or other descriptions, etc. prescribed in Article 2 of Enforcement Order as descriptions, etc. requiring special care in handling so as not to give rise to unjust discrimination, prejudice or other disadvantages against Individual Concerned.

(Specifying Purpose of Use)
Article 3.

1. When handling Personal Information, each Regular Member and Electronic Public Offering Member must specify as much as possible the business and the purpose for which the Personal Information would be provided or used so that Individual Concerned can form reasonable expectation thereof.
2. In specifying the purpose of use pursuant to the preceding Paragraph, because such an abstract purpose of use as "will be used for the purposes necessary for our company" does not meet the requirement of "specify as much as possible," each Regular Member and Electronic Public Offering Member must strive to specify the purpose of use by indicating the financial instruments and services to be offered.
3. If the purpose of use is to be changed, the relevant Regular Member or Electronic Public Offering Member must limit the scope of change so that the purpose of use subsequent to such change can be reasonably recognized as being related to the purpose of use before such change.
4. In the case where the purpose of use of any specific Personal Information is restricted by laws and regulations, etc., the relevant Regular Member or Electronic Public Offering Member must clearly indicate such fact.

(Form of "Consent")
Article 4.

When procuring the consent of Individual Concerned prescribed in the following Article and Article 13, each Regular Member and Electronic Public Offering Member must procure it in writing (which includes the form of electromagnetic record; the same shall apply hereinafter) as a general rule. In such cases as that Individual Concerned does not possess the ability to make judgment regarding the consequences which could arise from giving consent to the handling of Personal Information because the Individual Concerned is a minor, adult ward, person under curatorship or under assistance, it becomes necessary

to procure consent of a person who has parental authority, is a statutory agent or has authority equivalent thereto in respect of such Individual Concerned.

(Restriction Based on Purpose of Use)
Article 5.

1. Regular Member and Electronic Public Offering Member must not handle Personal Information beyond the scope necessary for achieving the purpose of use which was specified pursuant to Article 3 without procuring prior consent of Individual Concerned; provided, however, that use of Personal Information to procure prior consent of Individual Concerned (e.g., transmitting e-mail or making telephone call) does not constitute unintended use even if such use is not described in the initially specified purpose of use.
2. In the event any Regular Member or Electronic Public Offering Member acquired Personal Information as a result of succeeding to a business of other "personal information handling business operator" because of a merger or any other reason, the relevant Regular Member or Electronic Public Offering Member must not, without procuring prior consent of Individual Concerned, handle such Personal Information beyond the scope necessary for achieving the purpose of use held by such other "personal information handling business operator" prior to the relevant succession; provided, however, that use of Personal Information to procure prior consent of Individual Concerned does not constitute unintended use even if such use is not described in the purpose of use existed prior to the relevant succession.
3. The provisions of the preceding two Paragraphs shall not apply to the following cases:
   (1) In the case it is based on any law or regulation;
   (2) In the case it is necessary for protecting person's life, body or property (including juridical person's property), and it is difficult to procure the consent of Individual Concerned;
   (3) In the case it is particularly necessary for improving public health or promoting sound growth of children, and it is difficult to procure the consent of Individual Concerned; and
   (4) In the case it is necessary to cooperate in the execution of work, which is prescribed by any law or regulation, by any national government organ, local government or person entrusted by any of the foregoing, and procuring the consent of Individual Concerned is likely to hinder the execution of such work.

(Sensitive Information)

Article 6.

1. Regular Member and Electronic Public Offering Member must not acquire, use or provide to a third party Special-Care-Required Personal Information, or information (excluding the information falling under Special-Care-Required Personal Information) regarding membership in labor union, family origin, registered domicile, health care or sex life (excluding the information which has been published by Individual Concerned, national government organ, local government, or any person stipulated in any Item of Paragraph 1 of Article 76 of Protection Act or in any Item of Article 6 of Enforcement Rules, and the information which is obvious in appearance and acquired by looking at or taking picture of Individual Concerned; hereinafter referred to as "Sensitive Information") except in the cases provided below:
   (1) In the case it is based on any law or regulation;
   (2) In the case it is necessary for protecting person's life, body or property;
   (3) In the case it is particularly necessary for improving public health or promoting sound growth of children;
   (4) In the case it is necessary to cooperate in the execution of work, which is prescribed by any law or regulation, by any national government organ, local government or person entrusted by any of the foregoing;
   (5) In the case Sensitive Information regarding employee, etc. such as affiliation with or membership in political or religious organization or labor union is to be acquired, used or provided to a third party to the extent necessary for executing the work of collecting withholding tax or the like;
   (6) In the case Sensitive Information is to be acquired, used or provided to a third party to the extent necessary for the execution of transfer, etc. of rights and obligations under an inheritance procedure;
   (7) In the case Sensitive Information is to be acquired, used or provided to a third party—on the ground of the necessity for securing appropriate business operation of Self-Offering and Other Transactions, etc. conducted by the relevant Regular Member or Electronic Public Offering Member—based on the consent of Individual Concerned, to the extent necessary for the execution of the business; and
   (8) In the case biometric authentication information, which falls under Sensitive Information, is to be used for identity verification based on the consent of Individual Concerned.

2. When acquiring, using, or providing to a third party Sensitive Information under any of the cases set forth in the preceding Paragraph, the relevant Regular Member or Electronic Public Offering Member must handle it especially carefully so as not to make such acquisition, use or provision to a third party in deviation from the conditions set forth in the preceding Paragraph.
3. When acquiring, using, or providing to a third party Sensitive Information under any of the cases set forth in Paragraph 1, the relevant Regular Member or Electronic Public Offering Member must act appropriately in accordance with the laws and regulations, etc. related to protection of Personal Information.
4. When providing Sensitive Information to a third party, the relevant Regular Member or Electronic Public Offering Member must not apply the provision of Article 23, Paragraph 2 (opt out) of Protection Act.

(Appropriate Acquisition of Personal Information)
Article 7.

1. Regular Member and Electronic Public Offering Member must not acquire Personal Information by a fraudulent or any other dishonest means. When acquiring Personal Information from a third party, the relevant Regular Member or Electronic Public Offering Member must not unjustly infringe upon the interest of Individual Concerned.
2. When acquiring any Personal Information provided by a third party, the relevant Regular Member or Electronic Public Offering Member must check the status of compliance with laws and regulations by the information provider and confirm that the relevant Personal Information has been lawfully acquired.

(Notification, Publication, Indication, etc. of Purpose of Use Upon Acquisition of Personal Information)
Article 8.

1. When having acquired Personal Information, the relevant Regular Member or Electronic Public Offering Member must promptly notify the purpose of its use to Individual Concerned or publish it, unless such purpose of use has already been published. In such case, the relevant "notice" must be made in writing as a general rule, and the relevant "publication" must be made in an appropriate manner—such as publishing it on the Internet website, etc., or displaying or making available document

at a counter, etc. of its business office—in accordance with its mode of business such as its method of selling financial instruments.

2. Notwithstanding the provision of the preceding Paragraph, when Personal Information described in a written agreement or other document is to be acquired as a result of concluding agreement with Individual Concerned, the relevant Regular Member or Electronic Public Offering Member must expressly indicate the purpose of its use to the Individual Concerned in advance; provided, however, that the foregoing does not apply to the case where the Personal Information is needed urgently in order to protect the life, body or property of a person.
3. When any Regular Member or Electronic Public Offering Member has changed the purpose of use, it must notify to Individual Concerned, or publish, the changed purpose of use.
4. The provisions of the preceding three Paragraphs shall not apply to the following cases:
   (1) In the case notifying to Individual Concerned, or publishing, the purpose of use is likely to result in harming the life, body, property or any other right or interest of the Individual Concerned or a third party;
   (2) In the case notifying to Individual Concerned, or publishing, the purpose of use is likely to result in harming the right, or just and proper interest, of the relevant Regular Member or Electronic Public Offering Member;
   (3) In the case it is necessary to cooperate in the execution of work, which is prescribed by any law or regulation, by any national government organ or local government, and notifying to Individual Concerned, or publishing, the purpose of use is likely to result in hindering the execution of such work; and
   (4) In the case the purpose of use is deemed to be clear in the light of the circumstances of the acquisition.

(Securing Accuracy of Data)

Article 9.

Each Regular Member and Electronic Public Offering Member must strive to maintain Personal Data accurate and up-to-date to the extent necessary for achieving the purpose of use, through such means as developing the procedure to collate and verify Personal Data at the time of inputting it in Personal Information Database, etc., developing the procedure for making correction, etc. upon finding error, etc., updating recorded matters and establishing the retention period. It is not necessary to make the retained Personal Data to

be updated uniformly or constantly, and it shall be sufficient if its accuracy and recency is secured in accordance with the corresponding purpose of use and to the extent necessary for such purpose.
Furthermore, each Regular Member and Electronic Public Offering Member must prescribe retention period for retained Personal Data in accordance with the purpose of use by, for example, setting the retention period for Personal Data regarding customers, etc. to be of such length so that it expires within a certain period of time after the termination of the relevant agreement, and must delete the retained Personal Data after the lapse of the relevant period.
However, the foregoing shall not apply to the case where the retention period is prescribed under any law, regulation, etc.

(Security Control Measures)
Article 10.

1. Each Regular Member and Electronic Public Offering Member must take necessary and appropriate measures—such as developing fundamental policy/handling rules, etc. on security control, and developing a system for implementing security control measures—for the purpose of preventing leakage or loss of or damage to Personal Data it handles and other security control for Personal Data. The necessary and appropriate measures must include "Systematic Security Control Measures," "Human Security Control Measures," and "Technological Security Control Measures" for each stage of acquisition, use, retention, etc. of Personal Data.
   The measures must be prepared in consideration of the extent of infringement of rights and interests that will be suffered by Individual Concerned if Personal Data is leaked, lost, damaged, etc., and must be corresponding to the risks attributable to such factors as the scale and nature of the business, the condition of handling Personal Data (including the nature and volume of Personal Data being handled), and the nature of the medium which records Personal Data. The definitions of the terms used in this Article are as set forth below:
   (1) Systematic Security Control Measures
   This refers to the development of systems and implementation of measures by each Regular Member and Electronic Public Offering Member, which consist of the following acts among others: defining the responsibilities and authorities of officers and employees (referring to those who are within the organization of the relevant Regular Member or Electronic Public Offering Member, directly or indirectly

subject to the instructions and supervision of the relevant Regular Member or Electronic Public Offering Member and engaged in the business conducted by the relevant Regular Member or Electronic Public Offering Member, and they are not limited to the employees (full-time employees, contract employees, part-time employees, part-timers, nonregular workers, etc.) having employment relationship with the relevant Regular Member or Electronic Public Offering Members, but also include those who do not have employment relationship with the relevant Regular Member or Electronic Public Offering Member (including the directors, accounting advisors (in the case where the accounting advisor is a corporation, its employees who perform such duties), company auditors, executive officers, temporary workers sent from temp agencies, etc.); the same shall apply hereinafter) concerning security control measures for Personal Data; preparing and operating rules, etc. on security control; and checking and inspecting their implementation status.

(2) Human Security Control Measures

This refers to the supervision over the officers and employees to ensure execution of security control for Personal Data through, among others, conclusion of agreement with the officers and employees regarding nondisclosure of Personal Data and provision of education and training for the officers and employees.

(3) Technological Security Control Measures

This refers to the technological measures concerning security control for Personal Data, such as controlling access to Personal Data and to the information system handling Personal Data, and monitoring the information system.

2. For the development of the fundamental policy/handling rules, etc. on security control for Personal Data, each Regular Member and Electronic Public Offering Member must implement the following "Systematic Security Control Measures."

(1) Development of rules, etc.

(a) Development of fundamental policy on security control for Personal Data;

(b) Development of handling rules on security control for Personal Data;

(c) Development of rules on checking and inspecting the condition of handling Personal Data; and

(d) Development of rules on outsourcing.

(2) Handling rules on security control at each control stage

(a) Handling rules for the acquisition and input stage;

(b) Handling rules for the use and processing stage;

(c) Handling rules for the safekeeping and retention stage;

(d) Handling rules for the transfer/transmission stage;
(e) Handling rules for the deletion/disposition stage; and
(f) Handling rules for the stage of dealing with leakage incident, etc.

3. Each Regular Member and Electronic Public Offering Member must implement the following "Systematic Security Control Measures," "Human Security Control Measures" and "Technological Security Control Measures" for the development of systems of implementing security control for Personal Data.

(1) Systematic Security Control Measures
(a) Appointing a person who is responsible for managing Personal Data;
(b) Enhancing the work rules, etc. with security control measures;
(c) Operating in accordance with the handling rules on security control for Personal Data;
(d) Developing the method to check the condition of handling Personal Data;
(e) Developing and implementing systems to check and inspect the condition of handling Personal Data; and
(f) Developing system to deal with leakage incident, etc.

(2) Human Security Control Measures
(a) Concluding agreement regarding nondisclosure of Personal Data, etc. with the officers and employees;
(b) Clarifying the roles, responsibilities, etc. of the officers and employees;
(c) Making security control measures thoroughly known to the officers and employees, and providing education and training for the officers and employees on such measures;
(d) Checking the status of compliance with Personal Data control procedures by the officers and employees.

(3) Technological Security Control Measures
(a) Identifying and authenticating users of Personal Data;
(b) Establishing demarcations of Personal Data for control, and controlling access to Personal Data;
(c) Managing the authority to access Personal Data;
(d) Personal Data leakage, damage, etc. preventive measures;
(e) Recording and analyzing access to Personal Data;
(f) Recording and analyzing the condition of operation of the information system handling Personal Data; and
(g) Monitoring and inspecting the information system handling Personal Data.

(Supervision Over Officers and Employees)

Article 11.

1. Each Regular Member and Electronic Public Offering Member must, in making its officers and employees handle Personal Data, establish appropriate internal control system and exercise necessary and appropriate supervision over such officers and employees so that security control will be exerted for the relevant Personal Data. Such supervision must be exercised by taking into consideration the extent of infringement of rights and interests which will be suffered by Individual Concerned if the Personal Data is leaked, lost, damaged, etc., and must be corresponding to the risks attributable to such factors as the nature of business and the condition of handling Personal Data.
2. Each Regular Member and Electronic Public Offering Member must exercise the "necessary and appropriate supervision" over its officers and employees provided for in the preceding Paragraph by developing the following systems, etc.:
   (1) Concluding with officers and employees at the time of hiring, etc. an agreement, etc. prohibiting the relevant officer or employee, while he/she is with the relevant Regular Member or Electronic Public Offering Member and after he/she left such Member, from allowing a third party to know and from using for any purpose other than the intended purpose of use, Personal Data which he/she has come to know in relation to the Self-Offering and Other Transactions, etc. conducted by such Member;
   (2) Clearly defining the roles and responsibilities of officers and employees through establishing handling rules for appropriate handling of Personal Data, making security control obligation thoroughly known to officers and employees, and providing education and training for officers and employees regarding such obligation; and
   (3) Developing system to check, among others, the status of compliance with the matters prescribed under internal security control measures, and system to check and inspect the protection of Personal Data by officers and employees, for the purpose of preventing officers and employees from taking out Personal Data.

(Supervision Over Entrusted Party)

Article 12.

1. When entrusting handling of Personal Data in whole or in part (which includes all agreements, regardless of their forms or types, under which the relevant Regular

Member or Electronic Public Offering Member causes other person to handle the whole or part of Personal Data), the relevant Regular Member or Electronic Public Offering Member must exercise necessary and appropriate supervision over the entrusted party in order to ensure that security control for the Personal Data the handling of which was entrusted is exerted. The supervision must be exercised by taking into consideration the extent of infringement of rights and interests which will be suffered by Individual Concerned if the Personal Data is leaked, lost, damaged, etc., and must be corresponding to the risks attributable to such factors as the scale and nature of the entrusted operation and the condition of handling Personal Data.

2. Each Regular Member and Electronic Public Offering Member must, when it is to entrust operation to other party, select a party which can be recognized as handling Personal Data properly, and, in order to ensure that security control measures will be exerted for the Personal Data entrusted, must secure measures of security control for Personal Data also at the party which is to be entrusted with operation (in the case where operation is to be entrusted through two or more steps, supervision must be exercised also to check whether the business operator, which is the party entrusted with the operation initially, is exercising sufficient supervision over the business operators to which the operation was re-entrusted, etc.). To be more specific, for example, the following measures, among others, must be taken.
   (1) In order to secure security control for Personal Data, prescribe in the criteria for selecting the party to be entrusted with operation details of such matters as the development of organizational system and the formulation of fundamental policy/handling rules on security control at the party to be entrusted with operation, and review such criteria on a regular basis. In selecting the party to be entrusted with operation, it is desirable to have such persons as those who are responsible for managing Personal Data make assessments appropriately after checking by visiting, if necessary, the site where Personal Data will be handled, or by other reasonable alternative method.
   (2) Include in the relevant entrustment agreement the security control measures which consist of the following: entrusting party's authorities regarding supervision, inspection and collection of reports; prohibition of leakage, unauthorized use, alteration and use for any purpose other than the intended purpose of use, of the Personal Data at the party entrusted with operation; the terms and conditions for re-entrustment; and the responsibility of the party entrusted with operation in the event of occurrence of leakage, etc. And by such means as regularly performing

inspection, check the status of compliance with the security control measures prescribed in the relevant entrustment agreement on a regular basis or at any time and review the security control measures.

With regard to the status of compliance with the security control measures, etc. prescribed in the relevant entrustment agreement, it is desirable that such persons as those who are responsible for managing Personal Data make appropriate assessments including examining need to make any revision to the relevant security control measures, etc.

If the party entrusted with operation intends to re-entrust the operation to other party, it is desirable that the relevant Regular Member or Electronic Public Offering Member sufficiently checks—by such means as requiring the party entrusted with operation to present report or complete approval procedure in advance, or regularly performing inspection, directly or through the party entrusted with operation, on such matters as the party to be re-entrusted with operation, details of the operation to be re-entrusted, and the method of handling Personal Data by the party to be re-entrusted with operation—to make sure, just like when making the initial entrustment, that the party entrusted with the operation appropriately exercises the supervision, which is referred to in this Article, over the party re-entrusted with the operation and that the party re-entrusted with the operation implements the security control measures pursuant to Article 20 of Protection Act. The foregoing matters concerning re-entrustment shall also apply to any further re-entrustment made by the party re-entrusted with operation and by any subsequent party.

(Restriction of Provision to a Third Party)

Article 13.

1. Regular Member and Electronic Public Offering Member must not provide Personal Data to a third party (referring to any person, regardless of whether it is a natural person, juridical person or any other organization, other than the relevant Regular Member or Electronic Public Offering Member intending to provide the Personal Data, and the Individual Concerned who is the subject of the relevant Personal Data; the same shall apply hereinafter except for the following Article through Article 16) without procuring the consent of Individual Concerned in advance, except in the cases set forth below. In procuring such consent, the relevant Regular Member or Electronic Public Offering Member must clearly indicate to reasonable and appropriate extent the

details that are deemed necessary, in the light of such factors as the scale and nature of the business and the condition of handling Personal Data (including the nature and volume of the Personal Data handled), for Individual Concerned to make decision regarding the consent.

(1) In the case it is based on any law or regulation;

(2) In the case it is necessary for protecting person's life, body or property (including juridical person's property), and it is difficult to procure the consent of Individual Concerned;

(3) In the case it is particularly necessary for improving public health or promoting sound growth of children, and it is difficult to procure the consent of Individual Concerned; and

(4) In the case it is necessary to cooperate in the execution of work, which is prescribed by any law or regulation, by any national government organ, local government or person entrusted by any of the foregoing, and procuring the consent of Individual Concerned is likely to hinder the execution of such work.

2. With regard to Personal Data (excluding Sensitive Information; the same shall apply hereafter in this Paragraph) that is to be provided to a third party, in the case where provision to a third party of Personal Data which can identify Individual Concerned has been suspended in accordance with the request of the Individual Concerned, if the relevant Regular Member or Electronic Public Offering Member has in advance notified the Individual Concerned of the matters set forth below or placed these matters under such condition so that the Individual Concerned can easily know them, and also notified these matters to Personal Information Protection Commission, it may provide the relevant Personal Data to a third party notwithstanding the provision of the preceding Paragraph. The relevant Regular Member or Electronic Public Offering Member must also publish the contents of such notification to Personal Information Protection Commission through use of the Internet or any other appropriate method.

(1) Provision to a third party shall be made a purpose of use;

(2) Items of Personal Data to be provided to a third party;

(3) Method of provision to a third party;

(4) Provision to a third party of Personal Data which can identify Individual Concerned will be suspended in accordance with a request of Individual Concerned; and

(5) Method of receiving the request of Individual Concerned.

3. When any of the matters set forth in Item (2), (3) or (5) of the preceding Paragraph is to be changed, the relevant Regular Member or Electronic Public Offering Member

must, in advance, notify Individual Concerned of the details of change or place those details under such condition so that Individual Concerned can easily know them, and also notify those details to Personal Information Protection Commission.

If the relevant Regular Member or Electronic Public Offering Member made notification of the required matters to Personal Information Protection Commission pursuant to this Paragraph, it must also publish the contents of such notification.

4. The person who receives provision of the relevant Personal Data in the cases set forth below does not fall under a third party:
   (1) In the case Personal Data is provided as a result of entrustment by the relevant Regular Member or Electronic Public Offering Member of the entire or a part of handling of Personal Data within the extent necessary for achieving the purpose of use;
   (2) In the case Personal Data is provided as a result of succession of a business because of a merger or any other reason (limited to the case where the Personal Data continues to be used, even after the succession of the business, within the scope of the purpose of use which existed prior to its provision resulting from the relevant succession of the business); and
   (3) In the case Personal Data, which is to be used jointly with other specific persons, is provided to such specific persons, and such fact, the items of Personal Data to be used jointly, the scope of such joint users, the users' purpose of use, and the individual name or name of the person responsible for the management of the relevant Personal Data (referring to the person who is primarily responsible for receiving and processing complaint, for making disclosure, correction, etc., for making decisions on such matters as suspension of use, and for security control, at such joint users; such person being referred to as "Control Manager" in Paragraph 6) have already been notified to Individual Concerned or placed under such condition so that Individual Concerned can easily know them.
5. The notification to be made by the relevant Regular Member or Electronic Public Offering Member pursuant to the provision of Item (3) of the preceding Paragraph shall be in writing as a general rule. With regard to the notification, etc. concerning "the scope of such joint users," the relevant Regular Member or Electronic Public Offering Member must strive to individually list each of such joint users.
6. When the users' purpose of use or the individual name or name of Control Manager provided for in Item (3) of Paragraph 4 is to be changed, the relevant Regular Member or Electronic Public Offering Member must, in advance, notify Individual Concerned

of the details of change or place those details under such condition so that Individual Concerned can easily know them.

(Restriction of Provision to a Third Party in Foreign Country)
Article 14.

If Regular Member or Electronic Public Offering Member is to provide Personal Data to a third party (excluding those which have developed a system conforming to the standards prescribed in Enforcement Order that are considered to be necessary for continuously implementing the measures equivalent to the measures which "personal information handling business operator" is required to implement for handling of Personal Data; the same shall apply hereafter in this Article) in a foreign country (referring to any nation or region outside the territory of Japan; the same shall apply hereinafter), it must procure the consent of Individual Concerned to the provision to a third party in a foreign country in advance, except in the cases set forth in each Item of Paragraph 1 of the preceding Article. In such case, the provisions of the said Article shall not apply.

(Preparation, etc. of Record of Provision to a Third Party)
Article 15.

1. The relevant Regular Member or Electronic Public Offering Member must, when it provided Personal Data to a third party (excluding those set forth in each Item of Paragraph 5, Article 2 of Protection Act; the same shall apply in this Article and the following Article), prepare record of the date on which the relevant Personal Data was provided, the individual name or name of the relevant third party, and all other matters prescribed in Enforcement Rules; provided, however, that the foregoing shall not apply if the relevant provision of Personal Data falls under any Item of Paragraph 1 or any Item of Paragraph 4 of Article 13 (or, in the case of provision of Personal Data under the provision of the preceding Article, any Item of Paragraph 1 of Article 13).
2. The relevant Regular Member or Electronic Public Offering Member must retain the record stipulated in the preceding Paragraph during the period prescribed in Enforcement Rules from the date of the preparation of such record.

(Confirmation, etc. When Receiving Provision from a Third Party)
Article 16.

1. The relevant Regular Member or Electronic Public Offering Member must confirm the matters set forth below when it receives provision of Personal Data from a third party;

provided, however, that the foregoing shall not apply if the relevant provision of Personal Data falls under any Item of Paragraph 1 or any Item of Paragraph 4 of Article 13.

(1) The relevant third party's individual name, name, address, and if it is a juridical person, the individual name of its representative (if it is an organization without legal personality but has its designated representative or manager, such representative or manager); and

(2) The circumstances leading to the acquisition of such Personal Data by the relevant third party.

2. The relevant Regular Member or Electronic Public Offering Member must, when it made the confirmation pursuant to the provision of the preceding Paragraph, prepare record of the date on which it received provision of the relevant Personal Data, the matters pertaining to the relevant confirmation, and all other matters prescribed in Enforcement Rules, and retain such record during the period prescribed in Enforcement Rules from the date of the preparation of such record.

(Publication, etc. of Matters pertaining to Retained Personal Data)
Article 17.

1. With regard to Retained Personal Data, each Regular Member and Electronic Public Offering Member must place the matters set forth below under such condition so that Individual Concerned can know them (which includes making reply without delay in response to a request made by Individual Concerned). If the purpose of use includes provision to a third party, the relevant Regular Member or Electronic Public Offering Member must describe such fact as a matter set forth in Item (2).

(1) Name of the Regular Member or Electronic Public Offering Member;

(2) Purpose of use of all Retained Personal Data (except for the cases which fall under any of Items (1) through (3) of Paragraph 4 of Article 8);

(3) Procedures to respond to the request referred to in the following Paragraph or to the demand referred to in Paragraph 1 of the following Article, Paragraph 1 of Article 19, or Paragraph 1 or 2 of Article 20 (if the amount of handling fee has been prescribed pursuant to the provision of Article 23, including the amount of handling fee);

(4) The section of the relevant Regular Member or Electronic Public Offering Member which has been designated to receive complaint regarding handling of Retained Personal Data; and

(5) Name of Accredited Personal Information Protection Organization and its section to file a request for resolving complaint.

2. Each Regular Member and Electronic Public Offering Member must, when it was requested by Individual Concerned to notify the purpose of use of Retained Personal Data which can identify the Individual Concerned, notify the Individual Concerned of it without delay; provided, however, that the foregoing shall not apply if the situation falls under either of the Items set forth below:
   (1) If the purpose of use of Retained Personal Data which can identify the Individual Concerned is clear as a result of the provision of the preceding Paragraph; or
   (2) If the situation falls under any of Items (1) through (3) of Paragraph 4 of Article 8.
3. If the relevant Regular Member or Electronic Public Offering Member has decided not to notify the purpose of use of Retained Personal Data requested as referred to in the preceding Paragraph, it must notify the Individual Concerned to such effect without delay.

(Disclosure)

Article 18.

1. Each Regular Member and Electronic Public Offering Member must, when it received from Individual Concerned a demand to disclose Retained Personal Data which can identify the Individual Concerned (including a demand to notify non-existence of such data if such data does not exist), disclose to the Individual Concerned the relevant Retained Personal Data without delay by means of delivering document (or if there is a method to which the person who made the demand for disclosure has agreed, by such method); provided, however, that if disclosure would result in a situation which falls under any of the Items set forth below, the relevant Regular Member or Electronic Public Offering Member may decide not to disclose all or a part of such data.
   (1) It is likely to result in harming the life, body, property or any other right or interest of the Individual Concerned or a third party;
   (2) It is likely to cause serious hindrance to appropriate execution of the business of the relevant Regular Member or Electronic Public Offering Member; or
   (3) It will result in a violation of other law or regulation.
2. If the relevant Regular Member or Electronic Public Offering Member has decided not to disclose all or a part of Retained Personal Data pertaining to the demand referred to in the provision of the preceding Paragraph, or if no such Retained Personal Data exists, it must notify the Individual Concerned to such effect without delay.

(Correction, etc.)

Article 19.

1. When any Regular Member or Electronic Public Offering Member received a demand from Individual Concerned to correct, add or delete (hereinafter referred to as "Correction, etc.") contents of Retained Personal Data which can identify the Individual Concerned, on the ground that the contents of the relevant Retained Personal Data is not reflecting facts, it must perform necessary investigation such as verifying facts, etc. without delay to the extent necessary to achieve the purpose of use, and make Correction, etc. of the contents of the relevant Retained Personal Data based on the result of such investigation.
2. When the relevant Regular Member or Electronic Public Offering Member made Correction, etc. of all or a part of the contents of Retained Personal Data pertaining to the demand referred to in the provision of the preceding Paragraph, or made decision not to make Correction, etc., it must notify the Individual Concerned to such effect (including the details of Correction, etc. if Correction, etc. was made) without delay.

(Suspension of Use, etc.)

Article 20.

1. When any Regular Member or Electronic Public Offering Member received a demand from Individual Concerned to suspend use of or delete (hereinafter referred to as "Suspension of Use, etc.") Retained Personal Data which can identify the Individual Concerned, on the ground that the relevant Retained Personal Data was handled in violation of the provisions of Article 5 or that such data was obtained in violation of the provisions of Article 7, if such demand is found to have a valid ground, it must effect Suspension of Use, etc. of the relevant Retained Personal Data without delay to the extent necessary to cure the violation; provided, however, that the foregoing shall not apply to the case where it would require a large amount of expense to effect Suspension of Use, etc. of the relevant Retained Personal Data, nor to the case where it would be otherwise difficult to effect the Suspension of Use, etc., if an alternative measure necessary to protect the rights and interests of the Individual Concerned is implemented.
2. When any Regular Member or Electronic Public Offering Member received a demand from Individual Concerned to suspend provision to a third party of Retained Personal Data which can identify the Individual Concerned on the ground that the relevant

Retained Personal Data is being provided to a third party in violation of the provisions of Paragraph 1 of Article 13 or Article 14, if such demand is found to have a valid ground, it must suspend provision to a third party of the relevant Retained Personal Data without delay; provided, however, that the foregoing shall not apply to the case where it would require a large amount of expense to suspend provision of the relevant Retained Personal Data to a third party, nor to the case where it would be otherwise difficult to suspend the provision to a third party, if an alternative measure necessary to protect the rights and interests of the Individual Concerned is implemented.

3. When the relevant Regular Member or Electronic Public Offering Member effected Suspension of Use, etc. of Retained Personal Data pertaining to the demand referred to in the provision of Paragraph 1, or made decision not to effect such Suspension of Use, etc., or when it suspended provision to a third party of all or a part of Retained Personal Data pertaining to the demand referred to in the provision of the preceding Paragraph, or made decision not to suspend such provision to a third party, it must notify the Individual Concerned to such effect (including details of the measures if measures different from those requested by the Individual Concerned are to be implemented) without delay.

(Explanation of Reason)
Article 21.

When the relevant Regular Member or Electronic Public Offering Member notifies Individual Concerned—pursuant to the provisions of Paragraph 3 of Article 17, Paragraph 2 of Article 18, Paragraph 2 of Article 19, or Paragraph 3 of the preceding Article—of its decision not to implement all or a part of the measures, or decision to implement measures entirely or partially different from the measures requested or demanded by the Individual Concerned, and explains the reasons therefor to the Individual Concerned, it must indicate the grounds for the decision not to implement the measures or for the decision to implement different measures, as well as the facts constituting such grounds.

(Procedures for Accommodating Demand, etc. for Disclosure, etc.)
Article 22.

1. With regard to the request referred to in the provision of Paragraph 2 of Article 17, or the demand referred to in the provision of Paragraph 1 of Article 18, Paragraph 1 of Article 19, or Paragraph 1 or Paragraph 2 of Article 20 (hereinafter referred to as "Demand, etc. for Disclosure, etc."), each Regular Member and Electronic Public

Offering Member may prescribe the procedures to receive such request or demand as set forth below. In such case, the relevant Regular Member or Electronic Public Offering Member must keep posting on its Internet website, or must post or make available at a counter of its business office, etc., such procedures together with Declaration of Protection of Personal Information prescribed in Article 26.

(1) Its section to which Demand, etc. for Disclosure, etc. should be made;
(2) Forms of documents to be submitted when making Demand, etc. for Disclosure, etc., and any other formalities of Demand, etc. for Disclosure, etc.;
(3) Method of identity-verification of the person making Demand, etc. for Disclosure, etc.;
(4) The amount of and the method of collecting the handling fee provided for in Article 33, Paragraph 1 of Protection Act (which includes the case where no fee is charged);
(5) Matters that are necessary for identifying the Retained Personal Data which is the subject of Demand, etc. for Disclosure, etc.; and
(6) Method of making reply to Demand, etc. for Disclosure, etc.

2. As a procedure for the case in which an agent (referring to the agent prescribed in Article 11 of Enforcement Order; the same shall apply in this Paragraph) makes Demand, etc. for Disclosure, etc., each Regular Member and Electronic Public Offering Member must prescribe the following matters in addition to each Item of the preceding Paragraph. Making disclosure, etc. directly to the Individual Concerned only is not prevented when responding to Demand, etc. for Disclosure, etc. made by the agent prescribed in Article 11, Item 2 of Enforcement Order.
   (1) Method of identity-verification of the agent; and
   (2) Method of confirming the agent's authority to represent.
3. In prescribing the procedures for Demand, etc. for Disclosure, etc. pursuant to the provisions of the preceding two Paragraphs, each Regular Member and Electronic Public Offering Member must be considerate so that they will not become excessively burdensome to Individual Concerned.

(Handling Fee)
Article 23.

1. Each Regular Member and Electronic Public Offering Member may, when it received a demand for notification of the purpose of use referred to in Paragraph 2 of Article 17

or for disclosure referred to in Paragraph 1 of Article 18, charge handling fee for the execution of the relevant measures.

2. When the relevant Regular Member or Electronic Public Offering Member is to charge handling fee pursuant to the provision of the preceding Paragraph, it must determine the amount of handling fee within the range which can be recognized as reasonable in the light of the actual cost.

(Complaint Processing by Regular Member and Electronic Public Offering Member)
Article 24.

1. Each Regular Member and Electronic Public Offering Member must strive to process complaint regarding handling of Personal Information appropriately and promptly.
2. By developing complaint processing procedure, creating a section to receive complaints, and providing sufficient education and training for the officers and employees who engage in complaint processing, for example, each Regular Member and Electronic Public Offering Member must strive to establish systems that are necessary for properly and promptly executing complaint processing.

(Dealing with Personal Information, etc. Leakage Incident, etc.)
Article 25.

1. Upon occurrence of an accident of either Personal Information leakage incident, etc. or information leakage incident concerning the description, etc. or Individual Identification Code which have been deleted from the Personal Information used for preparing “Anonymously Processed Information” (referring to the information defined in Article 2, Paragraph 9 of Protection Act) or concerning the processing method adopted pursuant to the provision of Article 36, Paragraph 1 of Protection Act (hereinafter referred to as “Personal Information, etc. Leakage Incident, etc.”), the relevant Regular Member or Electronic Public Offering Member must immediately report it to the Financial Services Agency and the Association.
2. When an accident of Personal Information, etc. Leakage Incident, etc. has occurred, the relevant Regular Member or Electronic Public Offering Member must promptly publish, among others, the facts of the relevant Incident, etc. and recurrence prevention measures, from the perspective of preventing the secondary damage, avoiding occurrence of a similar incident, and the like.
3. When an accident of Personal Information, etc. Leakage Incident, etc. has occurred, the relevant Regular Member or Electronic Public Offering Member must, among

others, promptly notify the facts, etc. of the relevant Incident, etc. to the Individual Concerned who is the subject of the relevant Incident, etc. (Dealing with Leakage Incident, etc.)

(Preparation of Declaration of Protection of Personal Information)
Article 26.

1. Each Regular Member and Electronic Public Offering Member must, in consideration of the importance of providing in advance explanation on its policy of dealing with Personal Information in an easily understandable manner, prepare and publish a declaration regarding the business operator's approach and policy on protection of Personal Information (so-called "privacy policy," "privacy statement," etc.; hereinafter referred to as "Declaration of Protection of Personal Information").
2. Declaration of Protection of Personal Information shall include, for example, the matters set forth below:
   (1) Declaration of the policy of dealing with protection of Personal Information, such as to comply with applicable laws and regulations, not to use Personal Information for anything other than the intended purpose of use, and to appropriately engage in complaint processing;
   (2) Easily understandable explanation on the procedures of notification, publication, etc. of the purpose of use provided for in Article 18 of Protection Act;
   (3) Easily understandable explanation on various procedures regarding handling of protection of Personal Information, such as the procedures for disclosure, etc. provided for in Article 27 of Protection Act; and
   (4) Section to contact for inquiries and complaint processing regarding handling of Personal Information.
3. Each Regular Member and Electronic Public Offering Member must strive to include as much as possible in Declaration of Protection of Personal Information statements which take into account the following points from the perspective of protection of rights and interests of Individual Concerned such as consumers in the light of the characteristics, scale and actual condition of the business activities:
   (1) If Individual Concerned him/herself makes a request regarding Retained Personal Data, the relevant Regular Member or Electronic Public Offering Member is to voluntarily accommodate request for suspension of use, etc., such as suspension of sending direct mail;

(2) The relevant Regular Member or Electronic Public Offering Member is to improve transparency of entrustment process by, for example, clarifying existence or nonexistence of entrustment and details of the operation to be entrusted;
(3) The relevant Regular Member or Electronic Public Offering Member is to make the purpose of use clearer for Individual Concerned by, for example, indicating the purpose of use by limiting it according to each different type of customers based upon reflection on details of its business, or voluntarily engaging in limiting the purpose of use based on elections made by Individual Concerned; and
(4) The relevant Regular Member or Electronic Public Offering Member is to expressly state the source of Personal Information or the method of its procurement (type of the source of information, etc.) as concretely as possible.

(Report to the Association)
Article 27.

1. The Association may request, at its discretion, any Regular Member or Electronic Public Offering Member to provide report so that the Association can check the relevant Member's compliance with this Guideline.
2. The Association shall give guidance or admonition to, or take any other measures against, any Regular Member or Electronic Public Offering Member, that are necessary to make the relevant Member comply with this Guideline.

Supplementary Provisions (May 20, 2011)

This Guideline shall become effective from the date on which the Association is certified by the Prime Minister as Financial Instruments Firms Association provided for in Article 78, Paragraph 1 of the Financial Instruments and Exchange Act (June 30, 2011).

Supplementary Provisions (May 26, 2015)

This amendment shall become effective from the date (May 29, 2015) provided for in the main text of Article 1 of the Supplementary Provisions of the Act for Amendment of the Financial Instruments and Exchange Act (2014, Act No. 44).

(Note) Amended provisions are as follows:

Amended Paragraphs 1 and 2 of Article 1; Item (4) of Article 2; Paragraphs 1 through 4 of Article 3; Article 4; Paragraphs 1 and 2 of Article 5; Paragraph 1, Item (7) of the said Paragraph, and Paragraph 2 of Article 6; Article 7; Paragraphs 1 through 3, and Item (2) of Paragraph 4 of Article 8; Article 9; Paragraph 1, Item (1) of the said Paragraph, Paragraphs 2 and 3 of Article 10; Paragraphs 1 and 2, and Item (1) of Paragraph 2 of Article 11; Paragraphs 1 and 2 of Article 12; Paragraphs 1, 2, 3, 4, 5 and 6 of Article 13; Paragraph 1, Item (1) of said Paragraph, and Paragraphs 2 and 3 of Article 14; Paragraph 1, Item (2) of said Paragraph, and Paragraph 2 of Article 15; Paragraphs 1 and 2 of Article 16; Paragraphs 1 through 3 of Article 17; Article 18; Paragraphs 1, 2 and 3 of Article 19; Paragraphs 1 and 2 of Article 20; Paragraphs 1 and 2 of Article 21; Paragraphs 1 through 3 of Article 22; Paragraph 1 and Item (3) of Paragraph 3 of Article 23; and Paragraphs 1 and 2 of Article 24.

Supplementary Provisions (August 26, 2015)

This amendment shall become effective from August 26, 2015.

(Note) Amended provisions are as follows:

(1) Amended Paragraph 1 of Article 1; the main text of Paragraph 1 of Article 10 and Item (3) of Paragraph 3 of the said Article; Paragraph 1 of Article 11; Paragraph 1 of Article 12; and the main text and Items (1) and (2) of Paragraph 2 of the said Article; and

(2) Newly added Paragraph 2 of Article 7.

Supplementary Provisions (April 28, 2017)

This amendment shall become effective from May 30, 2017.

(Note) Amended provisions are as follows:

(1) Amended Paragraphs 1 and 2 of Article 1;

(2) Amended Item (1) of Paragraph 1 of Article 2; newly added Item (2) of the said Paragraph, and moved down former Item (2) of the said Paragraph by one item so that it has become Item (3), and amended the said Item; moved

down former Items (3) through (5) by one item each; and newly added Item (7) of the said Paragraph;

(3) Amended Paragraphs 3 and 4 of Article 3; Article 4; Paragraphs 1 and 2 of Article 5; the main text of Paragraph 1, and Paragraphs 2 through 4 of Article 6; Paragraphs 1 and 2 of Article 8; Article 9; and the main text of Paragraph 1 of Article 10;

(4) Amended the main text of Paragraph 1, and the main text and Item (3) of Paragraph 2 of Article 13, and newly added Item (5) of the said Paragraph; and amended Paragraph 3, Items (1) through (3) of Paragraph 4, and Paragraph 5 of the said Article;

(5) Newly added Articles 14 through 16;

(6) Moved down former Article 14 to become Article 17; and amended Items (2) and (3) of Paragraph 1, and the main text of Paragraph 2 of the said Article;

(7) Moved down former Article 15 to become Article 18; and amended the main text of Paragraph 1, and Paragraph 2 of the said Article;

(8) Moved down former Article 16 to become Article 19; and amended Paragraphs 1 and 2 of the said Article;

(9) Moved down former Article 17 to become Article 20; and amended Paragraphs 1 through 3 of the said Article;

(10) Moved down former Article 18 to become Article 21 and amended the said Article;

(11) Moved down former Article 19 to become Article 22; and amended the headword, the main text and Items (1) through (6) of Paragraph 1, the main text of Paragraph 2, and Paragraph 3 of the said Article;

(12) Moved down former Article 20 to become Article 23; and amended Paragraphs 1 and 2 of the said Article;

(13) Moved down former Article 21 to become Article 24; and amended Paragraph 1 of the said Article;

(14) Moved down former Article 22 to become Article 25; and amended the headword and Paragraphs 1 through 3 of the said Article;

(15) Moved down former Article 23 to become Article 26; and amended Paragraph 1, and Items (2) and (3) of Paragraph 2 of the said Article; and

(16) Moved down former Article 24 to become Article 27.