GUIDELINE FOR PROTECTION OF PERSONAL INFORMATION

(February 9, 2005)

(Purpose)

Article 1 The purpose of the Guideline for Protection of Personal Information (hereinafter referred to as "Guideline") is to prescribe concrete measures etc. that should be taken by an Association Member for the purpose of ensuring proper handling of personal information in the course of business related to the Sale and Purchase or Other Transactions of Securities, etc. and other incidental business thereof by a Regular Member as set forth in the provision of Article 3, Item 8 of the Articles of Association; the business set forth in the provision of Article 5, Item 2(a) or (b) of the Articles of Association conducted by a Specified Business Member; and the Registered Financial Institution Business by a Special Member as set forth in the provision of Article 5, Item 3 of the Articles of Association (hereinafter referred to as "Securities Business, etc. by an Association Member"), based on the Act on the Protection of Personal Information (hereinafter referred to as "Protection Act"), the Enforcement Order for the Act on Protection of Personal Information (hereinafter referred to as "Enforcement Order"), the Basic Policy on the Protection of Personal Information (cabinet decision), the Guideline for Personal Information Protection in the Financial Business (Notice No.63 of Financial Services Agency in 2009; hereinafter referred to as "Guideline in the Financial Business"), and others.

2. An Association Member needs to establish a proper system to manage the Personal Information pursuant to the Protection Act, Enforcement Order, the Basic Policy on the Protection of Personal Information, the Guideline for Personal Information Protection in the Financial Business, and other relevant laws and regulations in order to prevent leakage or illegal distribution, etc. of Personal Information.

(Definitions)

Article 2 In the Guideline, the definition of the terms set forth in each of the following Items shall be as prescribed therein:

(1) Personal Information

Information about a living individual which can identify the specific individual from the descriptions such as name, date of birth and so on (including such information as will allow easy reference to other information and will thereby enable to identify the specific individual). If "information about a dead person" also constitutes the information living person such as bereaved family, etc., such information can also be considered Personal Information about such living person.

"Information about an Individual" shall mean not only factual information such as name, gender, date of birth, address, age, occupation, and family relationship but also all information that indicates judgment and evaluation on personal attributes such as physical features, property, job type, and title, and shall include information that is publicly available by publications, video and voice. If such "Information about an Individual" is combined with a name and/or any other descriptions, by which "a specific individual can be identified", such "Information about an Individual" shall become the "Personal Information."

If Information about an Individual who does not live any more also constitutes information about living individual such as members of the bereaved family, etc., such information can also be considered Personal Information about such living individual.

Although information about juridical person, or other entity such as name of company is not Personal Information in principle, if part of the information includes the Information about an Individual such as the names of officers, such part can also be considered Personal Information.

"Individual" shall naturally include foreigner.

(2) Personal Information Database, etc.
A set of information including the Personal Information set forth below:

(i) Systematically Aggregated information arranged to be able to search the specific Personal Information using a computer;

(ii) In addition to the information set forth in the provision of (i), the systematically aggregated information that is arranged according to a certain set of rules to enable to readily search specific Personal Information, and is in a state wherein Personal Information can be readily search by reference to list of contents, indexes, symbols, etc.

(3) Personal Data
Personal Information constituting a Personal Information Database, etc;

(4) Retained Personal Data
The Personal Data for which an Association Member has the authority to disclose, correct, add, or delete the content, to suspend its use, to erase, and to suspend its provision to a third party, all of which are requested by the person him/herself or its agent, and excluding the following data:

(i) Personal Data that are likely to pose a threat to the life, body, or property of the Person or a third party if presence of the data is known;

(ii) Personal Data that are likely to aid or trigger illegal or unjust acts if presence of the data is known;

(iii) Personal Data that are likely to endanger national security, damage mutually trustful relationships with other countries or international organizations, or cause disadvantage in the course of negotiation with other countries or international organizations if presence of the data is known;

(iv) Personal Data that is likely to impede the maintenance of public safety and order such as prevention, suppression, or investigation of crime if presence of the data is known.; and

(v) Personal Data that are to be deleted within six months.

(5) Person
A specific Individual who can be identified by reference to the Personal Information.

(Specification of Purpose of Use)

Article 3 When handling Personal Information, an Association Member must specify, to the extent possible, for what business and for what purpose the Personal Information is used that enables the Person to reasonably assume such business and purpose.

2. When specifying the purpose of use in the preceding Paragraph, as an abstract description such as "using the Personal Information for our company's purpose" shall not be considered sufficient in terms of "specify to the extent possible," an Association Member must endeavor to specify the purpose by presenting the financial instruments and services it intends to provide.

3. When an Association Member changes the purpose of use, the purpose of use after the change must not be wider range than is commonly assumed by the Person based on the purpose of use before the change. If an Association Member changes the purpose of use beyond the common assumption by the Person, the Association Member must obtain consent of the Person.

4. When the purpose of use of specific Personal Information is limited by laws and regulations, etc., an

Association Member must endeavor to clearly indicate so.

(Purpose of Use for Granting the Credit Line)

Article 4 In case an Association Member acquires Personal Information at the time of a margin transaction, a when-issued transaction, or making a loan based on securities under custody as collateral (limited to lending based on securities under custody as collateral by a Regular Member; the same shall apply to the next Paragraph), the Association Member must endeavor to obtain the consent of the Person by setting a confirmation column in a document, etc. that clearly indicates the purpose of use. In such case, the purpose of use under an agreement, etc. shall be clearly described separately from other provisions in the agreement, etc.

2. An Association Member must not exploit its advantageous position in the transaction as a condition of allowing a customer to make a margin transaction or when-issued transaction or to receive a loan based on securities under custody as collateral and must not force him/her to agree to use the Personal Information for sending direct mail marketing for financial instruments that is not related to those business.

(Format of "Consent")

Article 5 When obtaining the consent of the Person as prescribed in the provision of the next Article and Article 14, an Association Member shall, in principle, obtain it in writing (including a record made by an electronic means, magnetic means, or any other means that cannot be recognized by human senses; the same shall apply hereinafter).

If the Person is a minor, subject to the adult guardianship system, assistantship system, or supporter-ship system, and has no ability to understand the consequence of the consent to the handling of Personal Information, it is necessary to obtain consent of a person with parental authority or a legal representative, etc.

(Restriction by the Purpose of Use)

Article 6 An Association Member must not handle the Personal Information beyond the scope necessary for achieving the purpose of use specified under Article 3 without obtaining prior consent of the Person.

Provided, however, that the Personal Information is used to obtain consent of the Person in advance, this does not constitute a use out of the purpose of use even if such purpose is not listed on the initial purpose of use.

2. When having acquired the Personal Information as a result of a taking over the business of another Personal Information Handling Entity in the course of a merger or other reasons, an Association Member must not handle such Personal Information beyond the scope necessary for the achieving the purpose of use of the Personal Information concerned before the take-over.

Provided, however, that such situation as the Personal Information being used to obtain consent of the Person in advance does not fall under a use out of the purpose of use even if such purpose is not listed on the purpose of use before the takeover.

3. The provisions of the preceding two Paragraphs shall not apply to the following cases:

(1) In case it is required by laws and regulations;

(2) In case it is necessary for protecting the lives, bodies, or property of persons (including property of a juridical person) and it is difficult to obtain consent of the Person;

(3) In case it is specifically necessary for improving the public health or promoting sound growth of children, and it is difficult to obtain consent of the Person; and

(4) In case it is necessary for cooperating with a state organ, a local government, or a person or entity

entrusted by either of such bodies in executing the operations prescribed in laws and regulations, and obtaining consent of the Person may impede the execution of such operations.

(Sensitive Information)

Article 7 An Association Member shall not acquire, use, or provide to a third party information on a person's political views, creed (i.e. religious belief, thought and belief), participation in a labor union, race, ethnic group, family origin, domicile of origin, health condition and sexual life, and information on criminal history (hereinafter referred to as "Sensitive Information") except for the cases set forth below:

(1) In case it is required by laws and regulations;

(2) In case it is necessary for protecting the life, body, or property of a person;

(3) In case it is specifically necessary for improving the public health or promoting sound growth of children;

(4) In case it is necessary for cooperating with a state organ, a local government, or a person or entity entrusted by either of such bodies in executing the operations prescribed laws and regulations;

(5) In case the Sensitive Information of an employee is acquired, used, or provided to a third party, such as information regarding the person's belonging to or participation in a group of politics, religion, etc., or labor union, within a scope that is necessary to execute the operations related to the collection of withholding tax, etc.;

(6) In case the Sensitive Information is acquired, used, or provided to a third party within a scope that is necessary to transfer rights and obligations, etc. in an accession procedure;

(7) In case an Association Member acquires, uses, or provides to a third party the Sensitive Information based on the consent of the Person to ensure the proper operation of its business such as the securities business, etc. within a scope that is necessary to implement its business task; and

(8) In case the biometrical authentication information that falls under the Sensitive Information is used to confirm the identification of the Person based on the consent of the Person.

2. When acquiring, using, or providing to a third party the Sensitive Information due to the reasons prescribed in the preceding Paragraph, an Association Member shall handle it carefully so as not to acquire, use, or provide to a third party to an extent that deviates from the reasons set forth in the preceding Paragraph.

(Proper Acquisition of Personal Information)

Article 8 An Association Member must not acquire the Personal Information by a fraudulent or other dishonest means. When acquiring the Personal Information from a third party, an Association Member must not unreasonably infringe the interest of the Person.

2. When acquiring any Personal Information provided by a third party, an Association Member must check the status of compliance by the information provider and confirm that such Personal Information has been lawfully obtained.

(Notification, Publication and Indication, Etc. of the Purpose of Use upon Acquisition of the Personal Information)

Article 9 When having acquired the Personal Information, an Association Member must immediately notify the purpose of use to the Person, or publicize it unless the Association Member publicizes the purpose of use in advance. In such case, the "Notice" shall be made in writing in principle, and the "Publication" shall be made in a proper way; *e.g.*, by displaying or placing a document at a counter of its sales office, or

listing it on its web page on the Internet, etc., depending on the nature of business, such as a marketing method.

2. Notwithstanding the provision of the preceding Paragraph, when acquiring the Personal Information that is described in an agreement or other documents at the time of executing the agreement with the Person, an Association Member must expressly indicate the purpose of use to the Person in advance. Provided however that, this provision shall not apply to the case where the acquiring of the Personal Information is necessary to protect the life, body, or property of a person.

3. When having changed the purpose of use, an Association Member must notify the purpose of use changed to the Person or publicize it.

4. The provisions of preceding three Paragraphs shall not apply to the cases set forth below:

(1) In case notification to the Person or publication of the purpose of use may harm the life, body, or property of the Person or a third party;

(2) In case notification to the Person or publication of the purpose of use may harm the rights or fair interest of an Association Member;

(3) In case such action is necessary to cooperate with a state organ or a government in executing the operations prescribed in laws and regulations, and notification to the Person or publication of the purpose of use may impede the execution of such operations;

(4) In case the purpose of use is clear in consideration of the circumstances of the acquisition.

(Maintenance of the Accuracy of Data)

Article 10 An Association Member must endeavor to maintain Personal Data accurate and up-to-date within the scope that is necessary to achieve the purpose of use. For this purpose, then Association Member shall prescribe the retention period of the Personal Data held depending on the purpose of use such as retaining the Personal Data of customers, etc. only for a certain period of time after the termination of a contract. Provided however that, this provision shall not apply if a retention period is prescribed under laws and regulations.

(Security Control Measures)

Article 11 An Association Member must take necessary and appropriate measures such as the establishment of basic policy/ handling rules on security control and a system pertaining to security control measures for the purpose of preventing leakage, loss, or damage of the Personal Data handled and other measures for security control of the Personal Data. The necessary and appropriate measures must include "Systematic Security Control Measures," "Human Security Control Measures," and "Technological Security Control Measures" which are laid out according to the respective stages of acquisition, use, and retention of the Personal Data. The measures shall be prepared in consideration of the extent of infringement of rights and interests incurred on the Person at the time of leakage, loss, or damage of the Personal Data, and shall be based on the risks attributable to the nature of business, handling status of Personal Data, and the nature of the medium that records the Personal Data, etc. The definition of the terms in this Article shall be as follows:

(1) "Systematic Security Control Measures";
The establishment of systems and implementation of measures by an Association Member such as defining the responsibilities and authorization of officers and employees (a person who is within an organization of an Association Member, directly or indirectly receives an instruction and is under supervision of the Association Member, and is engaged in the business conducted by the Association Member, not limited to such employee who has an employment relationship with the Association Member (regular staff, contract staff, or part-time staff) but also including a person who does not have an employment relationship with the Association Member (director, accounting

counselor, (in the case where an accounting counselor is a juridical person, an employee who performs such duties), auditor, operating officer, or temporary staff); the same shall apply hereinafter) for the security control measures of the Personal Data, preparing and operating the rules on security control, and checking and inspecting the implementation status;

(2) Human Security Control Measures;
To execute a non-disclosure agreement on the Personal Data with officers and employees, to give education and training for officers and employees, and to supervise officers and employees for ensuring the security control of the Personal Data; and

(3) Technological Security Control Measures;
Technological measures for security control of the Personal Data such as access control to an information system that handles the Personal Data, and monitoring of information systems.

2. An Association Member must take the following "Systematic Security Control Measures" for the establishment of basic policy and handling rules on security control of the Personal Data:

(1) Establishment of rules, etc.;

(i) Establishment of basic policy on security control of the Personal Data;

(ii) Establishment of handling rules on security control of the Personal Data;

(iii) Establishment of rules on check and inspection of handling status of the Personal Data; and

(iv) Establishment of rules on outsourcing.

(2) Handling rules on security control in respective control stages;

(i) Handling rules at the acquisition and input stages;

(ii) Handling rules at the use and processing stages;

(iii) Handling rules at the custody and retention stage;

(iv) Handling rules at the transfer and transmission stages;

(v) Handling rules at the deletion and disposition stages; and

(vi) Handling rules in a stage of responding to an event such as leakage.

3. An Association Member must take the following "Systematic Security Control Measures," "Human Security Control Measures" and "Technological Security Control Measures" for the development of an implementation system pertaining to the security control of the Personal Data:

(1) Systematic Security Control Measures;

(i) Appointment of a person who is responsible for managing the Personal Data;

(ii) Establishment of security control measures in the working rules;

(iii) Operation in accordance with the handling rules on security control of the Personal Data;

(iv) Preparation of a method to check the handling status of the Personal Data;

(v) Establishment and implementation of a check and inspection system of the handling status of the Personal Data; and

(vi) Development of a system to respond to events such as leakage.

(2) Human Security Control Measures;

(i) Execution of an agreement on non-disclosure, etc. of the Personal Data with officers and employees;

(ii) Clear definition of roles and responsibilities of officers and employees;

(iii) Thorough dissemination, education, and training in security control measures for officers and employees; and

(iv) Checking of compliance with Personal Data control procedures taken by officers and employees.

(3) Technological Security Control Measures;

(i) Identification and authentication of users of the Personal Data;

(ii) Establishment of control stages and control of access to the Personal Data;

(iii) Management of access right to the Personal Data;

(iv) Measures to prevent leakage and damage of the Personal Data;

(v) Recording and analysis of access to the Personal Data;

(vi) Recording and analysis of information system operations that handle the Personal Data; and

(vii) Monitoring and inspection of information systems that handle the Personal Data.

(Supervision of Officers and Employees)

Article 12 When an Association Member has its officers and employees handle the Personal Data, the Association Member must establish an appropriate internal administration system to ensure the security control of the Personal Data, and exercise necessary and appropriate supervision of such officers and employees. The supervision shall be conducted in consideration of the extent of infringement of rights and interests incurred on the Person at the time of leakage, loss, or damage of the Personal Data, and shall be based on the risks attributable to the nature of business and handling status of Personal Data, etc.

2. An Association Member shall exercise the "Necessary and Appropriate Supervision" to officers and employees set forth in the preceding Paragraph by developing the following systems, etc.:

(1) Conclude an agreement with officers and employees at the time of employment, etc. that prohibits officers and employees from informing a third party of the Personal Data or using it for any purpose other than the purpose of use that is known by the officers and employees through the securities business operations of an Association Member during and after their service to the Association Member;

(2) Clearly define the roles and responsibilities of officers and employees through the establishment of handling rules for proper handling of the Personal Data, and thorough disseminate, and give education and training regarding duties for security control; and

(3) An Association Member shall develop a system to confirm the compliance with matters that are prescribed in internal security control measures and to check and inspect the Personal Data protection by officers and employees for the purpose of preventing officers and employees from

taking out the Personal Data.

(Supervision over Entrusted Party)

Article 13 When entrusting the handling of Personal Data in whole or in part (including all agreements that include entrustment of the whole or part of the Personal Data handling to others, regardless of the form or type of the agreement), an Association Member must exercise Necessary and Appropriate Supervision over the entrusted party to ensure security control of the entrusted Personal Data handling. The supervision shall be conducted in consideration of the extent of infringement of rights and interests incurred on the Person at the time of leakage, loss, or damage of the Personal Data, and shall be based on the risks attributable to the scale and nature of the services entrusted and the status of handling Personal Data, etc.

2. An Association Member shall select and entrust the business to a party who can be recognized to handle the Personal Data properly and must confirm that the entrusted party takes the security control measures for the Personal Data for the purpose of ensuring that the security control measures are taken for the Personal Data entrusted (in case the business is re-entrusted to two or more parties, the Association Member shall supervise the entrusted party in exercising sufficient supervision of re-entrusted parties). More concretely, for example, the following measures among others, must be taken.

(1) Prescribe the details of establishment of organizational systems of an entrusted party and its basic policy and handling rules on the security control as the criteria to select the entrusted party, and review the criteria on a regular basis
On the occasion of selecting an entrusted party, the Association Member is encouraged to have a person responsible for managing the Personal Data or other person carry out an appropriate evaluation process, where necessary, after confirmation through entry and inspection of the site where the Personal Data will be handled or by other reasonable alternative method.

(2) Include the security control measures that cover the authority to supervise, inspect, and collect a report from a entrusted party, prohibition of leakage, piracy, falsification, and use other than the purpose of use of the Personal Data at the site of entrusted party, the terms and conditions for re-entrustment, and the responsibility of the entrusted party at the time of leakage and other events in the entrustment agreement, check the compliance with the security control measures prescribed in the entrustment agreement on a regular basis or from time to time by such means as regular auditing, and review the security control measures
With regard to compliance with the security control measures, etc. prescribed in the entrustment agreement, the Association Member is encouraged to have a person responsible for managing the Personal Data or other person carry out an appropriate evaluation process, which process may include review of the security control measures, etc.
If an entrusted party intends to re-entrust its entrusted services, the Association Member is encouraged, in the same way as in the case of the entrustment from the Association Member to its first-tier entrusted party, to obligate the first-tier entrusted party to make an advance report to the Association Member or obtain the approval of the Association Member, and to audit the re-entrusted party directly or through the first-tier entrusted party on a regular basis, in connection with the re-entrusted party, the scope of services to be re-entrusted, the re-entrusted party's method of handling Personal Data, and other service details, thereby obtaining adequate confirmation in order to ensure that the first-tier entrusted party will properly supervise the re-entrusted party in accordance with the conditions of this Article and that the re-entrusted party will implement security control measures based on Article 20 of the Protection Act. The foregoing shall apply to any further entrustment to a lower-tier entrusted party.

(Restriction of Provision to a Third Party)

Article 14 An Association Member must not provide the Personal Data to a third party (a person other than the Association Member who intends to provide the Personal Data and the Person concerning the Personal Data, regardless of natural person, juridical person or other body; the same shall apply hereinafter) without obtaining the prior consent of the Person except for the cases set forth below:

(1) In case it is required by laws and regulations;

(2) In case it is necessary for protecting the life, body, or property of a person (including property of a juridical person) and it is difficult to obtain the consent of the Person;

(3) In case it is specifically necessary for improving the public health or promoting sound growth of children, and it is difficult to obtain consent of the Person; and

(4) In case it is necessary for cooperating with a state organ, a local government, or a person or entity entrusted by either of such bodies in executing the operations prescribed in laws and regulations, and obtaining consent of the Person may impede the execution of the operations concerned.

2. Regarding the Personal Data that is to be provided to a third party and in case the Person requests to suspend the provision of the Personal Data to a third party that can identify the Person, notwithstanding the preceding Paragraph, an Association Member may provide the Personal Data to a third party if the Association Member notifies the following matters to the Person or renders the following matters in a state where the Person can easily know it:

(1) The purpose of use is to provide to a third party;

(2) Matters of the Personal Data that are to be provided to a third party;

(3) Means or method to provide to a third party; and

(4) Providing the Personal Data that can identify the Person to a third party is to be suspended upon request of the Person.

3. When changing the matters set forth in the provision of the preceding Paragraph, Item 2 or 3, an Association Member shall notify such changes to the Person in advance or render such changes in a state where the Person can easily know it.

4. In the following cases, a person who is provided the Personal Data is not regarded as a third party:

(1) In case an Association Member entrusts the handling of the whole or part of the Personal Data within the scope that is necessary to achieve the purpose of use;

(2) In case the Personal Data are provided as a result of taking over the business of another entity in a merger and other reasons associated with such take-over; and

(3) In case the Personal Data are shared with specific persons and such fact, the matters of the Personal Data that are shared, the scope of the persons who share the Personal Data, the purpose of use of the persons who share the Personal Information, and the name of the persons responsible for the control of such Personal Data (for the persons who share the Personal Information, this means a person who primarily receives and handles claims, decides on the disclosure, correction, and suspension of use, and is responsible for the security control; referred to as "Person responsible for the control" in Paragraph 6) are notified to the Person in advance, or are in a state where the Person can easily know it.

5. An Association Member shall in principle make the notice prescribed in the provision of the preceding Paragraph, Item 3 in writing. An Association Member must endeavor to individually list "the scope of the persons who share the Personal Data" in the notice.

6. When changing the purpose of use by persons who share the Personal Data or the name of the Person responsible for the control that are prescribed in the provision of Paragraph 4, Item 3, an Association Member must notify such changes to the Person in advance, or render them in a state where the Person can easily know it.

(Publication, Etc. of Matters pertaining to the Retained Personal Data)

Article 15 An Association Member must render the following matters in a state where the Person can easily know it (including the case the Association Member replies without delay in response to a request from the Person) regarding its Retained Personal Data. In case the purpose of use includes the provision to a third party, the Association Member must describe so as a matter set forth in Item 2:

(1) Name of the Association Member;

(2) Purpose of use of all the Retained Personal Data (however, excluding the cases subject to Article 9, Paragraph 4, Item 1 through 3);

(3) Procedures required under the provision of the next Paragraph, next Article, Paragraph 1, Article 17, Paragraph 1, or Article 18, Paragraph 1 or 2 (including the amount of fee if it is determined pursuant to the provision of Article 21);

(4) The section in charge of receiving a complaint on the handling of Retained Personal Data within the company; and

(5) Name of the Authorized Personal Information Protection Organization and the contact information of such organization for submitting a complaint.

2. When requested by the Person to notify the purpose of use of its Retained Personal Data that can identify the Person, an Association Member must notify it to the Person without delay. Provided however that, this provision shall not apply to either of the cases set forth in the Items below:

(1) In case the purpose of use of the Retained Personal Data that can identify the Person is clear due to the provision of the preceding Paragraph; or

(2) In case falling under Article 9, Paragraph 4, Item 1 through 3.

3. When having decided not to inform the purpose of use of the Retained Personal Data pursuant to the provision of the preceding Paragraph, an Association Member must notify so to the Person without delay.

(Disclosure)

Article 16 When requested by the Person to disclose the Retained Personal Data that can identify the Person, an Association Member must disclose such Retained Personal Data without delay by delivering a document or in a method agreed with the person who requested the disclosure. However, if the disclosure may fall under any of the following, the Association Member may avoid disclosing the whole or party of such data:

(1) In case it may pose a threat to the life, body, or property of the Person or a third party;

(2) In case it may significantly hinder the proper conduct of business by the Association Member; or

(3) In case it breaches other laws and regulations.

2. When having decided not to disclose the whole or part of the Retained Personal Data pursuant to the provision of the preceding Paragraph, an Association Member must notify the Person of it without delay. The Association Member shall also endeavor to explain the reason by indicating the ground provision of laws and the standard fact to make such a decision.

(Correction, Etc.)

Article 17 When requested by the Person to correct, add, or delete (hereinafter referred to as "Correction,

etc.") the Retained Personal Data for the reason that the content of the Retained Personal Data that can identify the Person is incorrect, an Association Member must conduct a necessary investigation such as confirming the fact without delay within the scope necessary for the achievement of the purpose of use, and make the Correction, etc. on such Retained Personal Data based on the result of the investigation.

2. When having made the Correction etc. on the whole or party of the Retained Personal Data upon request pursuant to the provision of the preceding Paragraph, or decided not to make the Correction, etc., an Association Member must notify the Person of it (including what is changed in case the Correction, etc. is made) without delay. In case an Association Member does not make the Correction, etc. the Association Member shall endeavor to indicate the reason why the member would not make the Correction, etc., and the fact that can be a ground for such decision, and explain the reason.

(Suspension of Use, Etc.)

Article 18 When requested by the Person to stop using or to erase the Retained Personal Data (hereinafter referred to as "Suspension of Use, etc.") for the reason that the Retained Personal Data that can identify the Person are handled in breach of the provision of Article 6 or that it was obtained in breach of the provision of Article 8, and it is found that the request is reasonable, an Association Member must implement the Suspension of Use, etc. of such Retained Personal Data within the scope that is necessary to correct such breach, without delay. Provided however that, this provision shall not apply if implementing the Suspension of Use, etc. is prohibitively expensive, or it is difficult to implement the Suspension of Use, etc. due to other reasons, and the Association Member takes an alternative measure to protect the rights and interest of the Person.

2. When requested by the Person to suspend the provision of the Retained Personal Data to a third party due to the reason that the Retained Personal Data that can identify the Person is provided to a third party in breach of the provision of Article 14, Paragraph 1, and it is found that such request is reasonable, an Association Member must stop providing the Retained Personal Information to a third party without delay. Provided however that, this provision shall not apply if implementing the Suspension of Use, etc. is prohibitively expensive, or it is difficult to implement the Suspension of Use, etc. due to other reasons, and the Association Member takes an alternative measure to protect the rights and interest of the Person.

3. When having done or decided not to implement the Suspension of Use, etc. of the whole or part of the Retained Personal Data as requested pursuant to the provision of Paragraph 1, or decided not to suspend, or stopped providing or decided not to provide the whole or part of the Retained Personal Data to a third party as requested pursuant to the provision of the preceding Paragraph, an Association Member must notify the Person of it (including measures if the Association Member takes the measures that are different from the one requested by the Person) without delay.

(Explanation of Reason)

Article 19 Under the provisions of Paragraph 3 of Article 15, , Paragraph 2 of Article 16, Paragraph 2 of Article 17, and Paragraph 3 of the preceding Article, in case an Association Member notifies that the Association Member decides not to take the whole or part of measures requested by the Person, or the Association Member takes measures that are different from the one requested by the Person, the Association Member must endeavor to indicate the reason why it decides not to take the measures, or to take different measures and the fact that is a ground for such decision, and explain the reason.

(Procedures to Respond to the Request for Disclosure, Etc.)

Article 20 Regarding the request pursuant to the provision of Paragraph 2 of Article 15, Paragraph 1 of Article 16, Paragraph 1 of Article 17, and Paragraph 1 or 2 of Article 18, (hereinafter referred to as "Request for Disclosure"), an Association Member may prescribe how to receive such request as follows. In this case, an Association Member shall endeavor to keep posting them on its internet website, or indicating or placing them on a counter of its business office combined with its Statement of Personal Information Protection as prescribed in the provision of the Article 24.

(1) Where to apply the Request for Disclosure, etc.;

(2) A form of document that should be submitted at the time of the Request for Disclosure, etc. and other means to make the Request for Disclosure, etc.;

(3) How to identify the Person who makes the Request for Disclosure, etc.;

(4) The amount of fee prescribed in the provision of the next Article and how to collect it (including the case of free of charge);

(5) Matters that are necessary to specify the Retained Personal Data that are subject to the Request for Disclosure, etc.; and

(6) How to respond to the Request for Disclosure, etc.

2. An Association Member shall prescribe the following matters in addition to those prescribed in the respective Items of the preceding Paragraph for procedures that an agent (legal agent for minors, legal agent under adult guardianship, or voluntary agent appointed by the Person; the same shall apply to this Paragraph) makes the Request for Disclosure, etc. The Request for Disclosure, etc. by an agent shall not hinder the Association Member from making the disclosure, etc. directly to the Person.

(1) How to identify an agent; and

(2) How to confirm the power of attorney held by an agent.

3. When prescribing the procedure for the Request for Disclosure, etc. pursuant to the provisions of the preceding two Paragraphs, an Association Member must consider that such procedure would not impose an excessive burden on the Person.

(Fee)

Article 21 When requested to notify the Purpose of Use pursuant to the provision of Article 15, Paragraph 2, or to make disclosure pursuant to the provision of Article 16, Paragraph 1, an Association Member may charge a fee for the conduct of such measures.

2. When charging a fee pursuant to the provision of the preceding Paragraph, an Association Member must determine the amount of fee within the scope that can be recognized to be reasonable in consideration of the actual cost. In such case, the Association Member shall endeavor to calculate the reasonable amount of fee based on the estimate of averaged actual cost, etc. of a similar disclosure procedure.

(Dealing with Complaints by an Association Member)

Article 22 When having received a complaints regarding the handling of the Personal Information, an Association Member shall investigate the details, and shall endeavor to process it properly and promptly within a reasonable period of time.

2. An Association Member must endeavor to establish a necessary system that enables it to process complaints properly and promptly by preparing a complaints processing procedure, establishing a section to receive complaints, and giving sufficient education and training to officers and employees who process complaints.

(Response to an Incident such as Leakage)

Article 23 When an incident such as leakage of the Personal Information occurs, an Association Member shall immediately report it to the Financial Services Agency and the Association; provided, however, that the occurrence of leakage of any Specific Personal Information shall be reported to the Personal Information Protection Commission, in addition to the foregoing.

2. When an incident such as leakage of the Personal Information occurs, an Association Member shall immediately publicize the fact of such leakage and preventive measures from a viewpoint to prevent secondary damage from occurring and a similar incident from reoccurring, etc.

3. When an incident such as leakage of the Personal Information occurs, an Association Member shall immediately notify the Person who is subject to such leakage of such leakage and other facts.

(Preparation of Statement of Personal Information Protection)

Article 24 Given the importance to explain in advance a handling policy on Personal Information in an easy-to-understand manner, an Association Member shall prepare and publicize the statement of its concept and policy on the Personal Information protection (a so-called privacy policy or privacy statement, etc.; hereinafter referred to as "Statement of Personal Information Protection").

2. The Statement of Personal Information Protection shall include, for example, the following matters:

(1) Statement of the handling policy on the Personal Information Protection such as compliance with applicable laws and regulations, non-use of the Personal Information other than the Purpose of Use, and proper handling of complaints;

(2) Easy-to-understand explanation of procedures to notify and publicize, etc. the Purpose of Use under the provisions of Article 18 of the Protection Act;

(3) Easy-to-understand explanation of various procedures for the Personal Information Protection such as the procedures for disclosure, etc. under the provisions of Article 24 of the Protection Act; and

(4) Who receives an inquiry and complaints on the handling of the Personal Information.

3. The statement of Personal Information protection shall include descriptions considering the following matters as much as possible in light of the features, scale, and actual condition of the business activity from a viewpoint of protecting rights and interests of the Person such as consumers, etc.:

(1) If the Person him/herself makes a request about his/her own Personal Data held by the Association Member, the Association Member shall voluntarily respond the request such as stop using the Personal Data, such as termination of sending a direct mail;

(2) The Association Member shall further enhance the transparency of entrusted business by disclosing the use/non-use of entrusted party and what business is entrusted;

(3) The Association Member shall endeavor to further clarify the Purpose of Use for the Person by indicating the limited Purpose of Use to each type of customer in consideration of its business and voluntarily limiting the Purpose of Use by customers' choice; and

(4) The Association Member shall concretely describe the source of Personal Information and how it was obtained (i.e., type of information sources) as much as possible.

(Report to the Association)

Article 25 The Association may request an Association Member to submit a report when necessary for the purpose of confirming compliance with the Guideline by the Association Member.

2. The Association gives to an Association Member an instruction and recommendation or takes measures that are necessary to make an Association Member comply with the Guideline.

SUPPLEMENTARY PROVISIONS [Omitted]

(Note) These Rules are based on the version in effect as of January 1, 2016.

This translation is solely for the convenience of those interested therein, and accordingly all questions that may arise with regard to the meaning of the words or expressions herein shall be dealt with in accordance with the original Japanese text.