GUIDELINE FOR PROTECTION OF PERSONAL INFORMATION

(March 21, 2017)

(Purpose)

Article 1 The purpose of the Guideline for Protection of Personal Information (hereinafter referred to as "Guideline") is to prescribe measures and other matters to specify the purpose of using the Personal Information and to securely control the Personal Information, as well as 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), (b) or (c) of the Articles of Association conducted by a Specified Business Member; and the Registered Financial Institution Business by a Special Member as prescribed 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 the Protection of Personal Information (hereinafter referred to as "Enforcement Order"), the Ordinance for Enforcement of the Act on the Protection of Personal Information (Rule No. 3 of the Personal Information Protection Commission in 2016; hereinafter referred to as the "Enforcement Ordinance"), the Basic Policy on the Protection of Personal Information (cabinet decision on April 2, 2004), the Guidelines for the Act on the Protection of Personal Information (General Rules; notice No. 6 of Personal Information Protection Commission in 2016), (Provision to a Third Party in a Foreign Country; notice No. 7 of Personal Information Protection Commission in 2016), (Obligation for Confirming and Recording in the Case of Providing to a Third Party; notice No. 8 of Personal Information Protection Commission in 2016), (Pseudonym Processed Information and Anonymously Processed Information; notice No. 9 of Personal Information Protection Commission in 2016), and (Certified Personal Information Protection Organization; notice No.7 of Personal Information Protection Commission in 2021), and the Guidelines for Personal Information Protection in the Financial Business (Notice No. 1 of Personal Information Protection Commission/Financial Services Agency in 2017), and the Practical Guide of Security Management Measures for the Guidelines for Personal Information Protection in the Financial Business (hereinafter collectively referred to as the "Laws and Regulations on Personal Information Protection").

2. An Association Member needs to establish a proper system to manage the Personal Information pursuant to the Laws and Regulations on Personal Information Protection and other relevant laws, regulations, and guidelines, etc. in order to prevent leakage, loss, or damage (hereinafter referred to as "Leakage, 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 that can identify the specific individual (including such information as will allow easy reference to other information and will thereby enable to identify the specific individual), or that includes an Individual Identification Code.

"Information about an Individual" shall mean not only information that enables to identify an individual such as name, address, gender, date of birth, and face image but also all information that indicates facts, judgment, and evaluation on personal attributes such as physical features, property, job type, and title, and shall include evaluation information, information that is publicly available, and video and voice information, regardless of whether or not its privacy is concealed by encryption,

etc. 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.

(1)-2 Individual Identification Code
Character, letter, number, symbol, or other code that are prescribed as items that can identify a specific individual from single information in Article 1 of the Enforcement Order.

(2) Personal Information Database, etc.
A set of information including the Personal Information set forth below (excluding those having little possibility of harming an individual's rights and interests considering their utilization method):

(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 principal 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 principal 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

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

(6) Special Care-required Personal Information
Personal Information including a specific description that requires special attention so as not to

cause unfair discrimination, prejudice, or other disadvantage.

(7) Sensitive Information
In the financial business field, the Special Care-required Personal Information, as well as information on the participation in a labor union, family origin, domicile of origin, healthcare, and sexual life (excluding that included in the Special Care-required Personal Information) (except for information that is disclosed by the Principal, a state agency, a local public body, an academic research institution, etc. or a person that falls under any of the items in Article 57, Paragraph 1 of the Protection Act or the items in Article 6 of the Enforcement Ordinance, or information that can be easily obtained from an external form when seeing the Principal or taking a picture or video of the Principal).

(8) Pseudonym Processed Information
Information about an Individual that is obtained by processing the Personal Information in such a way that prevents the individual from being identified, by means of taking measures prescribed depending on the type of the Personal Information, unless it is matched with other information.

(9) Anonymously processed information
Information about an Individual that is obtained by taking measures prescribed depending on the type of the Personal Information, for processing the Personal Information that disables to identify a specific individual, and reconstruction of which to enable to identify a specific individual is impossible after such processing.

(10) Individual-related Information
Information about a living individual that does not fall under Personal Information, Pseudonym Processed Information, and Anonymously Processed Information.

(11) Individual-related Information Database
A set of information including Individual-related Information set forth below:

(i) Information that is systematically arranged in such a way that specific Individual-related Information can be retrieved using a computer; or

(ii) In addition to what is listed in (i) above, information that is systematically arranged in such a way that specific Individual-related Information can be easily retrieved by organizing Individual-related Information based on certain rules and that is left in a state where it can be easily retrieved by means of a table of contents, index, code, etc.

(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 Principal 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 alters the purpose of use, such change must not exceed "the scope recognized reasonably relevant to the pre-altered the purpose of use" as prescribed in Article 17, Paragraph 2 of the Protection Act.

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 the case that an Association Member acquires Personal Information at the time of conducting a credit business such as a margin transaction, a when-issued transaction, or making a loan based on securities under custody as collateral (limited to the loan based on securities under custody as collateral by a Regular Member; the same shall apply to the next Paragraph) directly from the Principal with a written format, the Association Member must obtain the consent of the Principal and clearly describe the purpose of use under an agreement, etc. separately from other provisions in the agreement, etc.

2. In the case of the preceding Paragraph, an Association Member must not exploit its advantageous position in the transaction as a condition of allowing a customer to grant credit and must not force the Principal to agree to use the Personal Information that was obtained in the credit business for sending direct mail, etc. marketing for financial instruments that is not related to those business.

(Format of "Consent")

Article 5 When obtaining the consent of the Principal as prescribed in the provisions of the following Article, Article 14, Article 14-2, and Article 14-5 (limited to when the Association Member obtains Individual-related Information as Personal Data through the provision of such Individual-related Information by an Individual-related Information handling business operator based on the provision of the Article), an Association Member shall, in principle, obtain it in writing (including an electromagnetic record; the same shall apply hereinafter except for Article 16).
If the Principal 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 Principal.

Provided, however, if the Personal Information is used to obtain consent of the Principal in advance (such as sending an e-mail or making a call, etc.), 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 achieving the purpose of use of the Personal Information concerned before the take-over.

Provided, however, if handling the Personal Information within the scope necessary for achieving the purpose of use before the take-over, it does not fall under a use out of the purpose of use, and consent of the Principal is not required.

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 life, body, or property of a person (including property of a juridical person) and it is difficult to obtain consent of the Principal;

(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 Principal; 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 Principal may impede the execution of such operations.

(5) When providing an academic research institution, etc. (universities and other institutions or organizations that serve the purpose of academic research, or persons belonging to such institutions or organizations; the same shall apply hereinafter) with Personal Data, in case it is necessary for the said academic research institution, etc. to handle such Personal Data for the purpose of using it for academic research (hereinafter referred to as "Academic Research Purpose") (including cases where part of the purpose of handling the said Personal Data is for Academic Research Purpose, but excluding cases where there is a risk of unjustifiable infringement of an individual's rights and/or interests).

(Handling of Sensitive Information)

Article 7 An Association Member shall not acquire, use, or provide to a third party the 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 in laws and regulations;

(5) In case any Sensitive Information is acquired under a case specified in Article 20, Paragraph 2, Item 6 of the Protection Act, is used under a case specified in Article 18, Paragraph 3, Item 6 of the Protection Act, or is provided to a third party under a case specified in Article 27, Paragraph 1, Item 7 of the Protection Act.

(6) 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.;

(7) 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;

(8) In case an Association Member acquires, uses, or provides to a third party the Sensitive Information based on the consent of the Principal 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

(9) 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 Principal.

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.

3. When an Association Member acquires, uses, or provides to a third party the Sensitive Information in the case set forth in Paragraph 1 of this Article, the Association Member must take a proper action pursuant to the Laws and Regulations on Personal Information Protection.

4. When an Association Member provides the Sensitive Information to a third party, the Association Member shall not apply the provision of Article 27, Paragraph 2 (Opt-out) of the Protection Act.

(Prohibition of Improper Use)

Article 7-2 No Association Member may use any Personal Information in a manner that is likely to encourage or induce any illegal or unjust act.

(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 Principal.

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 Principal, 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" must be made in a proper way; *e.g.,* by listing it on its web page on the Internet, etc., displaying or placing a document at a counter of the headquarters and other sales offices, depending on the nature of business, such as a marketing method of its own financial products.

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 Principal, an Association Member must expressly indicate the purpose of use to the Principal 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 Principal 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 Principal or publication of the purpose of use may harm the life, body, or property of the Principal or a third party;

(2) In case notification to the Principal or publication of the purpose of use may harm the rights or fair interest of the 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 Principal 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, Etc. of the Accuracy of Data)

Article 10 An Association Member must endeavor to maintain the Personal Data accurate and up-to-date within the scope that is necessary to achieve the purpose of use, by developing a procedure to check and confirm the Personal Information when inputting the Personal Information in the Personal Information Database, etc. and a system to correct, etc. the information when any error, etc. is found, and establishing

rules, etc. of update and retention period of the record.

In this case, it is not necessary to always or uniformly update all the Personal Data the Association Member retains, and the Association Member may update the Personal Information within the scope that is necessary to maintain the accuracy and the up-to-date status depending on the purpose of use.

If the Association Member no longer needs to use the Personal Data it retains; i.e. it has achieved the purpose of use and has no reasonable cause to retain such Personal Data in light of the relationship with such purpose of use, even if the purpose of use has not been achieved, the business that is the precondition of such purpose ceases, or other cases, the Association Member must endeavor to delete the Personal Data without delay. Provided, however, that this provision shall not apply if the retention period, etc. is prescribed by 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 **L**eakage, etc. 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," "Physical Security Control Measures," "Technological Security Control Measures," and "Understanding of External Environment" 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 Principal at the time of Leakage, etc. of the Personal Data, and shall be based on the risks attributable to the scale and nature of business, handling status of Personal Data (including the nature and volume of the Personal Data handled) 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) Physical Security Control Measures:
Physical measures for secure management of Personal Data, including management of the area where Personal Data is handled, prevention of theft of devices and electronic media, etc., prevention of Leakage, etc. in carrying electronic media, etc., and disposal of devices and electronic media, etc.

(4) 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.

(5) Understanding of External Environment
When handling Personal Data in a foreign country, this means to understand the system, etc. relating to the protection of personal information in that foreign country.

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 of Leakage, etc. (meaning Leakage, etc. or events with a risk thereof; the same shall apply hereinafter).

3. An Association Member must take the following "Systematic Security Control Measures," "Human Security Control Measures," "Physical 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 (supervisory manager of the Personal Data management who is a primary manager to conduct operations related to the security control of Personal Data, manager of Personal Data control in each section that handles 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, etc.

(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) Physical Security Control Measures:

(i) Management of the handling area, etc. of Personal Data;

(ii) Prevention of theft, etc. of devices and electronic media, etc.;

(iii) Prevention of Leakage, etc. in carrying electronic media, etc.; and

(iv) Deletion of Personal Data and disposal of devices, electronic media, etc.

(4) 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, etc. 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 Principal at the time of Leakage, etc. 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 Principal at the time of Leakage, etc. 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 for security control of the Personal Data.
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 (including a method of utilizing a video conference system or the like (meaning a method by which the communicating parties can mutually recognize each other by transmission of images and audio); the same shall apply hereinafter) 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, prevention of Leakage, etc. and prohibition of use other than the purpose of use of the Personal Data at the site of entrusted party, and the terms and conditions for re-entrustment, as well as the responsibility of the entrusted party in the event of Leakage, etc., 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 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 23 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 When an Association Member provides the Personal Data to a third party (a person other than the Association Member who intends to provide the Personal Data and the Principal concerning the Personal Data, regardless of natural person, judicial person or other body; the same shall apply hereinafter except for Articles 14-2 through 14-6), the Association Member must not provide the Personal Data without obtaining consent of the Principal. When obtaining consent, the Association Member must clearly indicate reasonable and proper details that are deemed necessary for the Principal to make a decision on whether or not to give consent, depending on the scale and nature of business and handling status of the Personal Data (including the nature and volume of the Personal Data handled).

If an Association Member expects in advance to provide the Personal Data to a third party, the Association Member must specifically describe such effect in the purpose of use.

Provided, however, that an Association Member is not required to obtain consent of the Principal if the Association Member provides the Personal Data to a third party in the following cases:

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

(2) In case a specific right or interest such as the life, body, or property of a person (including property of a juridical person) is likely to be damaged, and it is necessary for protecting them, and it is difficult to obtain the consent of the Principal;

(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 Principal; and

(4) In case it is necessary for cooperating with a state agency, 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 Principal may impede the execution of the operations concerned.

(5) When the third party is an academic research institution, etc., in case it is necessary for the third party to handle the Personal Data for Academic Research Purpose (including cases where part of the purpose of handling the said Personal Data is for Academic Research Purpose, but excluding cases where there is a risk of unjustifiable infringement of an individual's rights and/or interests).

2. Regarding the Personal Data that is to be provided to a third party, if the Principal requests to suspend the provision of the Personal Data to a third party that can identify the Principal, 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 Principal or renders the following matters in a state where the Principal can easily know them, and submits such facts to the Personal Information Protection Commission.

The Association Member shall publicize by itself the details of such submission by using the Internet or other proper method.
The Association Member is not allowed to provide the Sensitive Information or other Personal Data obtained through fraudulent or otherwise improper means to a third party using an opt-out method, or further provide opted-out Personal Data (including a reproduction of all or part of such data, or data created by processing all or part of such data) using an opt-out method.

(1) Name and address of the Association Member, and name of representative;

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

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

(4) Method of acquiring Personal Data provided to a third party;

(5) Means or method to provide to a third party;

(6) Providing the Personal Data that can identify the Principal to a third party is to be suspended upon request of the Principal;

(7) A method to receive a request from the Principal;

(8) Method of updating Personal Data provided to a third party; and

(9) Scheduled date to start the provision of Personal Data update to a third party for the submission.

3. When there has been any changes to the matters set forth in the preceding Paragraph, Item 1 or when stopping the provision of Personal Data pursuant to the provision of the same Paragraph, an Association Member must, without delay, notify the Principal to such effect or render such changes in a state where the Principal can easily know them. When changing the matters set forth in the same Paragraph, Items 3 to 5, Item 7 or 8, an Association Member must, in advance, notify the Principal to such effect or render such changes in a state where the Principal can easily know them. In either of the above cases, the Association Member must also report to the Personal Information Protection Commission.

When the Association Member submits the necessary matters to the Personal Information Protection Commission pursuant to this Paragraph, it shall publicize by itself such matters.

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

(1) In case the Personal Data is provided as a result of entrustment by an Association Member of 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 is provided as a result of taking over the business of another entity in a merger and other reasons associated with such take-over (only in the case that, after the take-over of the business, the Personal Data is used within the scope of the purpose of use that was the same as that before the provision of the Personal Data due to such take-over); and

(3) In case the Personal Data shared with specific persons is provided to such specific persons, and such fact, the items 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 Data, and the name (or business name) and address of the persons (in the case of corporations, the names of their respective representatives) responsible for the control of such Personal Data (among the persons who share the Personal Information, this means a person who primarily receives and handles complaints, 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 communicated to the Principal in advance, or are in a state where the Principal 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 there has been a change to the name, business name, or address of the person responsible for the control (in the case of a corporation, the name of its representative), as defined in Paragraph 4, Item 3, an Association Member must, without delay, notify the Principal to such effect or render such change in a state where the Principal can easily know it. When changing the purpose of use of the persons who share the Personal Data, as set forth in the same Item, or the said person responsible for the control, an Association Member must, in advance, notify the Principal to such effect or render such change in a state where the Principal can easily know it.

(Restriction on Provision to a Third Party Located in a Foreign Country)

Article 14-2 When an Association Member provides the Personal Data to a third party (excluding a person who has developed a system meeting the criteria prescribed in the Enforcement Ordinance that is necessary for continuously taking measures equivalent to those to be taken by the Personal Information Handling Entity for handling the Personal Data (hereinafter referred to as "Equivalent Measures"); the same shall apply hereinafter in this Paragraph to Paragraph 4, and Article 14-5, Paragraph 1, Item 2) that is located in a foreign country (a country or a region that is outside of Japan; the same shall apply hereinafter) (excluding a country that is listed in the Enforcement Ordinance as a country having a personal information protection system deemed equivalent to that in Japan in terms of protecting personal rights and interests; the same shall apply hereinafter in this Article, the following Article, and Article 14-5, Paragraph 1, Item 2), the Association Member must obtain consent of the Principal to provide the Principal's Personal Data to a third party located in a foreign country in advance, except for the cases as prescribed in each Item of the preceding Article, Paragraph 1. In such case, the provision of the preceding Article shall not apply.

2. When an Association Member intends to obtain the consent of the Principal pursuant to the provision of the preceding Paragraph, the Association Member must provide the following information to the Principal in advance. Provided, however, that if the information listed in Item 3 cannot be provided, the Association Member must provide information to that effect and the reason therefor.

(1) Name of the foreign country;

(2) Information on the system of protection of Personal Information in the foreign country obtained using an appropriate and reasonable method;

(3) Information on measures for the protection of Personal Information taken by the said third party;

(4) Third Party to whom Personal Data is provided;

(5) Purpose of use by the third party to which the information is provided; and

(6) Personal Data items provided to the third party.

3. Notwithstanding the provision of the preceding Paragraph, if an Association Member cannot identify, at the point of time when the Association Member intends to obtain the consent of the Principal pursuant to the provision of Paragraph 1, the foreign country in which the third party to which information is to be provided is located, the Association Member must provide the following information to the Principal. Provided, however, that the provision of the information set forth in Item 2 is limited to cases where such information can be provided.

(1) The fact that it cannot be identified and the specific reason therefor (including the need to obtain the Principal's consent before the recipient is identified); and

(2) Information to be used as a reference for the Principal in lieu of the name of the foreign country where the third party to which information is to be provided is located.

4. In the case set forth in the preceding Paragraph, an Association Member shall, at the request of the Principal, provide the information on the matters set forth in Paragraph 2, Items 1 and 2 if the foreign country in which the third party to which the information is to be provided is located can be subsequently identified, and must, at the request of the Principal, provide the information on the matters set forth in Item 3 of the same Paragraph if it becomes subsequently possible to provide the information on the measures for the protection of Personal Information taken by the third party to which the information is to be provided. The Association Member shall also make the Principal aware of the fact that such a request for provision of information may be made through a statement in writing at the time of providing consent, and after including it in the Statement on Personal Information Protection prescribed in Article 24, make the information public by permanently posting it on an Internet website or posting or placing it at a counter

of its office, etc. Provided, however, that even if the Principal requests the provision of information, the Association Member may choose not to provide all or part of the information if the provision of information is likely to significantly hinder the proper performance of the operation of the Association Member. In such a case, the Association Member shall notify the Principal to that effect without delay and explain the reason therefor.

5. Where an Association Member provides Personal Data to a third party in a foreign country (limited to those who have an established system as defined in Paragraph 1; the same shall apply hereinafter from this Paragraph to Paragraph 7), the Association Member shall check, at the time of the provision and using an appropriate and reasonable method, whether or not there is any system in the foreign country which is likely to affect the implementation of Equivalent Measures by the third party and the details thereof, and if there is any such system, whether or not it is possible to ensure the implementation of Equivalent Measures by the third party.

6. When an Association Member has provided Personal Data to a third party pursuant to the provision of the preceding Paragraph, the Association Member shall take the following measures as necessary measures to ensure the continued implementation of Equivalent Measures by the third party:

(1) To regularly check, using an appropriate and reasonable method, the status of the implementation of Equivalent Measures by the said third party, as well as whether or not there is a system in the said foreign country that is likely to affect the implementation of the said Equivalent Measures and the details thereof; and

(2) To take necessary and appropriate measures if any impediment arises in the implementation of Equivalent Measures by the third party, and to suspend the provision of Personal Data to the third party if it becomes difficult to ensure the continuous implementation of the said Equivalent Measures.

7. When an Association Member has provided Personal Data to a third party pursuant to the provision of Paragraph 5, the Association Member must provide the following information to the Principal without delay, at the request of the Principal. The Association Member shall also, after including in the Statement on Personal Information Protection defined in Article 24 the fact that making such a request for the provision of information is possible, make it public, by means of permanently posting it on an Internet website or posting or placing it at a counter in its office, etc. Provided, however, the Association Member may choose not to provide all or part of the information if the provision of information has the risk of significantly hindering the proper performance of the operation of the Association Member. In such a case, the Association Member shall notify the Principal to that effect without delay and explain the reason therefor.

(1) Method taken by the third party in a foreign country to develop the system set forth in Paragraph 1;

(2) Outline of Equivalent Measures implemented by the third party in a foreign country;

(3) Status of the implementation of Equivalent Measures by the third party in a foreign country and the method and frequency of checking whether or not there is a system that may affect the implementation of the said Equivalent Measures and the details thereof;

(4) Name of the foreign country;

(5) Whether or not there is a system in the foreign country where the third party is located that may affect the implementation of Equivalent Measures by the third party in the foreign country and the outline thereof;

(6) Whether there is any hindrance to the implementation of Equivalent Measures by the third party in a foreign country and the outline thereof; and

(7) In the case of any hindrance to the implementation of Equivalent Measures by the third party in a foreign country, an outline of the measures to be taken by the providing Association Member to

eliminate such hindrance or improve such situation.

(Keeping, Etc. of a Record about Provision to a Third Party)

Article 14-3 When an Association Member provides the Personal Data to a third party (excluding a person set forth in each Item of Article 16, Paragraph 2 of the Protection Act; the same shall apply from this Article to Article 14-5), the Association Member must keep a record that includes the date when the Personal Data is provided, the name of the third party, and other matters prescribed in the Enforcement Ordinance.
Provided, however, that when providing the Personal Data to a third party located in Japan, if it falls under any of the conditions set forth from Item 1 to 7 below, the Association Member shall not be required to keep the record.
When providing the Personal Data to a third party located in a foreign country, if it falls under any of the conditions set forth from Item 1 to 4, or if the third party satisfies the criteria prescribed in the Enforcement Ordinance and meets any of those set forth in each Item of Article 27, Paragraph 5 of the Protection Act, the Association Member shall not be required to keep the record.

(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 a juridical person) and it is difficult to obtain consent of the Principal;

(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 Principal;

(4) In case it is necessary for cooperating with a state agency, 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 Principal is likely to impede the execution of the operations concerned;

(5) In case the Personal Data is provided as a result of entrustment by an Association Member of the handling of the whole or part of the Personal Data within the scope that is necessary to achieve the purpose of use;

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

(7) In case the Personal Data shared with specific persons is provided to such 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 Data, and the name of the persons responsible for the control of such Personal Data are notified to the Principal in advance, or are in a state where the Principal can easily know them.

(Confirmation, Etc. in the Case of Receiving the Personal Data from a Third Party)

Article 14-4 When an Association Member receives the Personal Data from a third party, except in the cases listed below, the Association Member must confirm the name and address of the third party, the name of the representative of the third party if it is a juridical person (in the case of an entity that is not a juridical person but has a representative or a manager, the name of such representative or a manager), and how the third party obtained the Personal Data, and keep a record about the matters prescribed in Article 30, Paragraph 3 of the Protection Act.
Provided, however, that if the Personal Data is substantially not provided by a “Provider,” the obligation to confirm and keep a record shall not apply.

(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 a juridical person) and it is difficult to obtain consent of the Principal;

(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 Principal;

(4) In case it is necessary for cooperating with a state agency, 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 Principal is likely impede the execution of the operations concerned;

(5) In case the Personal Data is provided as a result of entrustment by an Association Member of the handling of the whole or part of the Personal Data within the scope that is necessary to achieve the purpose of use;

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

(7) In case the Personal Data shared with specific persons is provided to such specific persons, and such fact, the items 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 Data, and the name or business name of the persons responsible for the control of such Personal Data are communicated to the Principal in advance, or are in a state where the Principal can easily know them.

(Restriction on the Provision of Individual-related Information to a Third Party)

Article 14-5 When a third party is expected to acquire Individual-related Information (limited to such that comprises the Individual-related Information Database, etc. defined in Article 2, Item 11; the same shall apply hereinafter in this Article) as Personal Data, an Association Member shall not provide the said Individual-related Information to the said third party without confirming in advance the following matters, except in the cases listed in each item of Article 14, Paragraph 1:

(1) Principal's consent is obtained to allow the said third party to receive the provision of Individual-related Information from the Association Member and acquire it as Personal Data by which the Principal can be identified; and

(2) When providing information to a third party in a foreign country, to obtain the consent of the Principal under the preceding item, information on the system for the protection of Personal Information in the foreign country, information on measures for the protection of Personal Information taken by the third party, and other information that would serve as a reference for the Principal are provided to the Principal in advance.

2. When an Association Member intends to obtain the Principal's consent upon receiving the provision of Individual-related Information from an Individual-related Information handling business operator (including cases where the Association Member has the Individual-related Information handling business operator providing the information obtain consent on behalf of the Association Member) and acquiring it as Personal Data, the Association Member shall provide the Principal with the following information:

(1) Relevant Individual-related Information items;

(2) Purpose of use after the acquisition of Personal Data upon receiving the provision of Individual-related Information;

3 The provision of Article 14-2, Paragraph 6 shall apply *mutatis mutandis* to cases where an Association Member provides Individual-related Information pursuant to the provision of Paragraph 1; and

4 The provision on the obligation to keep records set forth in the preceding Article shall apply *mutatis mutandis* to cases where an Association Member seeks confirmation pursuant to the provision of Paragraph 1.

(Retention Period of a Record about Provision to a Third Party)

Article 14-6 When the Association Member keeps the record pursuant to Articles 14-3, 14-4 and 14-5, the Association Member must retain it during a period prescribed in the Enforcement Ordinance from the date when such record is kept.

(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 Principal can easily know it (including the case the Association Member replies without delay in response to a request from the Principal) regarding its Retained Personal Data. In case the purpose of use includes the provision to a third party, the Association Member must clarify it as a matter set forth in Item 2:

(1) Name and address of the Association Member, and name of representative;

(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, or claimed under the provisions of the next Article, Paragraph 1 (including when applied *mutatis mutandis* pursuant to Paragraph 3 of the same Article), Article 17, Paragraph 1, or Article 18, Paragraphs 1 to 3 (including the amount of fee if it is determined pursuant to the provision of Article 21);

(4) Measures taken for secure management of Retained Personal Data (excluding those that may hinder secure management of such Retained Personal Data by making them available to the person (this includes responding without delay at the request of the Principal));

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

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

2. When requested by the Principal to notify the purpose of use of its Retained Personal Data that can identify the Principal, an Association Member must notify it to the Principal 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 Principal is clear due to the provision of the preceding Paragraph; or

(2) In case of 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 Principal without delay.

(Disclosure)

Article 16 When claimed by the Principal to disclose the Retained Personal Data that can identify the

Principal (including the case to notify the fact that no Retained Personal Data exists), an Association Member must disclose such Retained Personal Data to the Principal without delay by means of providing electromagnetic records, delivering a document, or other method designated by the Association Member and claimed by the Principal (delivering a document is used as the method of disclosure in the case where this claimed method requires significant fee or is otherwise difficult to disclose by said method). However, if the disclosure may fall under any of the following, the Association Member may avoid disclosing the whole or part of such data:

(1) In case it may pose a threat to the life, body, or property of the Principal 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 that was in connection with the claim prescribed in the provision of the preceding Paragraph, or when no such Retained Personal Data exists, or when disclosure by the method claimed for by the Principal is difficult, an Association Member must notify the Principal of that without delay. If disclosure by the method requested by the Principal is not feasible, the Association Member shall notify the Principal to that effect and provide disclosure by delivering a document. The Association Member shall also explain the reason by indicating the grounds based on legal provisions and the facts used as basis for making such a decision.

3. The provisions of the preceding two Paragraphs shall apply *mutatis mutandis* to records of provision to a third party under the provisions of Articles 14-3 and 14-4 (excluding those specified by the Enforcement Order as those whose known presence or absence would harm public interest or other interests) relating to the Personal Data that can identify the Principal.

(Correction, Etc.)

Article 17 When claimed by the Principal to make correction, addition, or deletion (hereinafter referred to as "Correction, etc.") in regard to the contents of the Retained Personal Data for the reason that the Retained Personal Data that can identify the Principal has an error and 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 in principle.

2. When having made the Correction etc. on the whole or part of the Retained Personal Data in connection with the claim prescribed in the provision of the preceding Paragraph, or decided not to make the Correction, etc., an Association Member must notify the Principal 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 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 claimed by the Principal 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 Principal are handled in breach of the provision of Article 6 or Article 7-2 or that it was obtained in breach of the provision of Article 8, and it is found that such claim 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 Principal.

2. When claimed by the Principal 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 Principal is provided to a third

party in breach of the provision of Article 14, Paragraph 1, and it is found that such claim is reasonable, an Association Member must stop providing the Retained Personal Information to a third party without delay in principle. 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 Principal.

3. When the Principal claims for Suspension of Use, etc. or suspension of provision to a third party for the reason that the Retained Personal Data that can identify the Principal is no longer needed for use by the Association Member, that a situation such as Leakage, etc. set forth in Article 23, Paragraph 1 has occurred with regard to the Retained Personal Data that can identify the Principal, or that the handling of the Retained Personal Data that can identify the Principal may harm the Principal's rights or rightful interests, and it is found that such claim is reasonable, an Association Member must implement the Suspension of Use, etc. or the suspension of provision to a third party of such Retained Personal Data within the scope that is necessary to prevent infringements on the Principal's rights and interests, without delay. Provided however that, this provision shall not apply if implementing the Suspension of Use, etc. or suspension of provision to a third party is prohibitively expensive, or it is difficult to implement the Suspension of Use, etc. or suspension of provision to a third party due to other reasons, and the Association Member takes an alternative measure to protect the rights and interest of the Principal.

4. When having done or decided not to implement the Suspension of Use, etc. of the whole or part of the Retained Personal Data in connection with the claim prescribed in the provision of Paragraph 1 or the preceding Paragraph, 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 in connection with the claim prescribed in the provision of Paragraph 2 or the preceding Paragraph, an Association Member must notify the Principal of it (including measures if the Association Member takes the measures that are different from the one requested by the Principal) without delay.

(Explanation of Reason)

Article 19 In the case that, pursuant to the provisions of Paragraph 3 of Article 15, Paragraph 2 of Article 16 (including when applied *mutatis mutandis* pursuant to Paragraph 3 of the same Article), Paragraph 2 of Article 17, and Paragraph 3 and 4 of the preceding Article, an Association Member notifies that the Association Member decides not to take the whole or part of measures requested or claimed by the Principal, or the Association Member takes measures that are different from the one requested or claimed by the Principal, the Association Member shall 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, when explaining the reason thereof to the Principal.

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

Article 20 Regarding the claim pursuant to the provision of Paragraph 2 of Article 15, Paragraph 1 of Article 16 (including when applied *mutatis mutandis* pursuant to Paragraph 3 of the same Article), Paragraph 1 of Article 17, and Paragraph 1, 2 or 3 of Article 18, (hereinafter referred to as "Claim, etc. for Disclosure, etc."), an Association Member may prescribe how to receive such request as follows. In this case, an Association Member shall keep posting them on its internet website (this includes continuous displaying in the "Statement on Personal Information Protection" of a link that has been set to transition, with a single operation, to a screen that shows matters related to Retained Personal Data), indicating or placing them on a counter of its business office or otherwise combined with its Statement of Personal Information Protection as prescribed in the provision of the Article 24.

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

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

(3) How to identify the Principal or an agent (legal agent for minors, legal agent under adult

guardianship, or voluntary agent appointed by the Principal; the same shall apply to this Article) who makes the Claim, etc. for Disclosure, etc.;

(4) The amount of fee prescribed in Article 38, Paragraph 1 of the Protection Act and how to collect it (including the case of free of charge);

(5) Matters that are necessary to specify the Retained Personal Data or records of provision to a third party that are subject to the Claim, etc. for Disclosure, etc.; and

(6) How to respond to the Claim, etc. 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 makes the Claim, etc. for Disclosure, etc. The Claim, etc. for Disclosure, etc. by an agent shall not hinder the Association Member from making the disclosure, etc. directly to the Principal only.

(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 Claim, etc. 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 Principal.

(Fee)

Article 21 When requested to notify the Purpose of Use pursuant to the provision of Article 15, Paragraph 2, or claimed to make disclosure pursuant to the provision of Article 16, Paragraph 1 or 3, 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.

(Dealing with Complaints by an Association Member)

Article 22 An Association Member must endeavor to process complaints regarding the handling of the Personal Information properly and promptly.

2. An Association Member must endeavor to establish a necessary system for achieving the purpose prescribed in the preceding Paragraph by establishing a section to receive complaints, preparing a complaints processing procedure, and giving sufficient education and training to officers and employees who process complaints.

(Response to an Incident such as Leakage, etc. of Personal Information, etc.)

Article 23 If an Association Member becomes aware of any of the events specified in the items of Article 7 of the Enforcement Ordinance, the Association Member shall, in accordance with the Guidelines for the Act on the Protection of Personal Information (General Rules) 3-5-3 (“Reporting to the Personal Information Protection Commission”), report to the Personal Information Protection Commission (the Commissioner of the Financial Services Agency, etc., where the Commissioner of the Financial Services Agency, etc. has been delegated the authority to receive reports pursuant to the provision of Article 147 of the Protection Act, or the head of a local public entity, etc., where the head of a local public entity, etc. conducts the affairs that fall under the authority to receive reports pursuant to the provision of Article 165 of the Protection Act) and the Association. In addition, an Association member shall report to the Financial Services Agency and the Association if it becomes aware of a Leakage, etc. of Personal Data relating to individual customers, etc. handled by the Association member or a situation where such Leakage, etc.

may have occurred. If any Specific Personal Information that is prescribed in Article 2, Paragraph 8 of the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures is leaked, the Association Member shall also report it to the Personal Information Protection Commission, in addition to the foregoing.

2. An Association Member shall report to the Financial Services Agency and the Association pursuant to the provisions of the preceding paragraph if it becomes aware of any of the following circumstances (excluding the cases set forth in the preceding paragraph):

(1) A Leakage, etc. of the Personal Information handled by the Association Member has or may have occurred; or

(2) A leakage has or may have occurred of deleted information, etc. (in the case of information concerning the processing method used pursuant to the provision of Article 41, Paragraph 1 of the Protection Act, this shall be limited to information that can be used to restore the Personal Information used to produce the Pseudonym Processed Information; the same shall apply in the following Paragraph) pertaining to the Pseudonym Processed Information handled by the Association Member, or of processing method and other information pertaining to the Anonymously Processed Information handled by the Association Member.

3. If an Association Member becomes aware of any of the events specified in the items of Article 7 of the Enforcement Ordinance, it shall notify the Principal in accordance with the Guidelines for the Act on the Protection of Personal Information (General Rules) 3-5-4 ("Notification").
In addition, when an Association Member becomes aware of any of the following circumstances (excluding the cases specified in the items of Article 7 of the Enforcement Ordinance), it shall notify the Principal pursuant to the foregoing.

(1) A Leakage, etc. of the Personal Data handled by the Association Member (excluding Personal Data that is Pseudonym Processed Information) has occurred or may have occurred;

(2) A Leakage, etc. of the Personal Information handled by the Association Member (excluding Personal Information that is Pseudonym Processed Information) has occurred or may have occurred; or

(3) A leakage of deleted information, etc. pertaining to Pseudonym Processed Information or processing method and other information pertaining to Anonymously Processed Information handled by the Association Member has occurred or may have occurred.

4. If an event as set forth in Paragraphs 1 or 2 is found, an Association Member shall take necessary measures for the following matters according to the nature of the event:

(1) Reporting within sites and preventing damage from spreading;

(2) Investigation of facts and causes;

(3) Identification of the scope of impact; and

(4) Consideration and implementation of measures to prevent recurrence.
In addition, from the perspective of preventing secondary damage and similar incidents from occurring, the facts of the incident and measures to prevent recurrence shall be promptly publicized according to the details of the incident.

5. Matters other than the above are governed by the Guidelines for the Act on the Protection of Personal Information (General Rules) (limited to those related to the items of Article 7 of the Enforcement Ordinance).

(Application of the Guidelines to Pseudonym Processed Information)

Article 23-2 The application of the Guidelines to Pseudonym Processed Information (limited to Personal Information; the same shall apply hereinafter in this Paragraph) by an Association Member shall be as follows:

(1) Notwithstanding the provisions of Article 6, except in cases under laws and regulations, Pseudonym Processed Information shall not be handled beyond the extent necessary to achieve the purpose of use specified pursuant to the provision of Article 3, Paragraph 1.

(2) The provisions of Article 9 shall be applied to Pseudonym Processed Information upon replacing "notify the purpose of use to the Principal, or publicize it" in Paragraph 1 to "publicize the purpose of use" and "notify the purpose of use changed to the Principal or publicize it" in Paragraph 3 to "publicize the purpose of use changed," and "notification to the Principal or publication" in Paragraph 4, Items 1 to 3 of the same Article with "publication".

(3) When an Association Member no longer needs to use Personal Data and deleted information, etc. that is Pseudonym Processed Information, the Association Member shall endeavor to delete said Personal Data and deleted information, etc. without delay. In this case, the provision of Article 10 shall not apply.

(4) Notwithstanding the provisions of Article 14, Paragraphs 1 and 2, and Article 14-2, Paragraph 1, an Association Member shall not provide any Personal Data that is Pseudonym Processed Information to a third party, unless otherwise required by laws and regulations. In this case, the term "are communicated to the Principal in advance, or are in a state where the Principal can easily know it" in Article 14, Paragraph 4, Item 3 shall be replaced with "are publicized", "notify the Principal to that effect or render such change in a state where the Principal can easily know it" in Paragraph 6 of the same Article shall be replaced with "be publicized", "Provided, however, that when providing the Personal Data to a third party located in Japan, if it falls under any of the conditions set forth from Item 1 to 7 below, the Association Member shall not be required to keep the record. When providing the Personal Data to a third party located in a foreign country, if it falls under any of the conditions set forth from Item 1 to 4" in Article 14-3 shall be replaced with "In any of the cases listed in Item 1, or Items 5 to 7 below", and "except in the cases listed below" in Article 14-4 shall be replaced with "except in the cases listed in Item 1, or Items 5 to 7 below".

(5) The provisions of Article 3, Paragraph 3, Articles 15 through 21, and Article 23 shall not apply to any Pseudonym Processed Information, Personal Data that is Pseudonym Processed Information, and Retained Personal Data that is Pseudonym Processed Information.

2. The application of the Guidelines to Pseudonym Processed Information (excluding Personal Information; the same shall apply hereinafter in this Paragraph) shall be as follows:

(1) Unless otherwise provided by laws and regulations, an Association Member shall not provide any Pseudonym Processed Information to a third party.

(2) The provisions of Article 14, Paragraphs 4 and 6 shall apply *mutatis mutandis* to persons who receive Pseudonym Processed Information. In this case, the term "are communicated to the Principal in advance, or are in a state where the Principal can easily know it" in Paragraph 4, Item 3 of the same Article shall be replaced with "be publicized" and "notify the Principal to that effect or render such change in a state where the Principal can easily know it" in Paragraph 6 of the same Article shall be replaced with "be publicized".

(3) The provisions of Articles 11 to 13, and Article 22 shall apply *mutatis mutandis* to the handling of Pseudonym Processed Information by an Association Member.

(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 own

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 21 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 32 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 Principal:

(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 Principal 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.

4. It is desirable that the Statement on Personal Information Protection should be composed of indications, etc. that enable the Principal to appropriately understand the Statement and to exercise the opportunity to make a choice at his/her own discretion.

(Report to the Association, Etc.)

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.

3. An Association Member must comply with the Guideline and follow necessary instructions, recommendations, and other measures given or taken by the Association.

SUPPLEMENTARY PROVISIONS [Omitted]

(Note) This amendment comes into effect as of April 1, 2022.

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.