

Guideline Concerning Protection of Personal Information

(Purpose)

Article 1.

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

(Definitions)

Article 2.

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

(1) **Personal Information**

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

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

In the case where any information about a deceased individual at the same time constitutes information about a living individual such as a surviving family member, such information constitutes information about the living individual.

Furthermore, although information about juridical person or any other group, such as a name of corporation, does not constitute "Personal Information" in principle, if a part of such information contains information about an individual such as a name of its officer, that part constitutes "Personal Information."

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

(2) **Individual Identification Code**

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

(3) **Personal Information Database, etc.**

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

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

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

(4) Personal Data

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

(5) Retained Personal Data

This refers to the Personal Data over which the relevant Regular Member or Electronic Public Offering Member has the entire authority to make its disclosure, to make correction or addition to or removal of its contents, to suspend its use, to make its deletion, or to suspend its provision to a third party, in response to a request made by Principal or his/her agent, except for the Personal Data set forth below:

- (a) Personal Data which, once its existence or nonexistence becomes known, is likely to result in giving rise to a threat to the life, body, or property of Principal or a third party;
- (b) Personal Data which, once its existence or nonexistence becomes known, is likely to result in promoting or inducing unlawful or unjust act;
- (c) Personal Data which, once its existence or nonexistence becomes known, is likely to result in endangering national security, damaging the relationship of trust with other nation or international organization, or causing disadvantage in negotiation with other nation or international organization; and
- (d) Personal Data which, once its existence or nonexistence becomes known, is likely to result in hindering prevention, suppression or investigation of crime, or hindering maintenance of public safety and order in other forms.

(6) Principal

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

(7) Special-Care-Required Personal Information

This refers to the Personal Information which contains the race, belief, social status, medical history, criminal record or fact of having been victimized of a crime, in

respect of Principal, or other descriptions, etc. prescribed in Article 2 of Enforcement Order as descriptions, etc. requiring special care in handling so as not to give rise to unjust discrimination, prejudice or other disadvantages against Principal.

(8) Personally Referable Information

This refers to the information which is related to a living individual and does not fall under Personal Information, Pseudonymously Processed Information or Anonymously Processed Information.

(9) Personally Referable Information Database, etc.

This refers to a collective body of information comprising Personally Referable Information which has been systematically organized so as to be able to search using a computer for specific Personally Referable Information or similar others prescribed by Enforcement Order as systematically organized so as to be able to search easily for specific Personally Referable Information.

(10) Personally Referable Information Handling Business Operator

This refers to the Personally Referable Information Handling Business Operator prescribed in Article 16, Paragraph 7 of Protection Act.

(Specifying Purpose of Use)

Article 3.

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

4. In the case where the purpose of use of any specific Personal Information is restricted by laws and regulations, etc., the relevant Regular Member or Electronic Public Offering Member must clearly indicate such fact.

(Form of “Consent”)

Article 4.

When procuring the consent of Principal prescribed in the following Article, Article 13, Article 14 or Article 16-2 (limited to the case where the relevant Regular Member or Electronic Public Offering Member is to receive provision of Personally Referable Information from Personally Referable Information Handling Business Operator pursuant to the provisions of the said Article and procure it as Personal Data), each Regular Member and Electronic Public Offering Member must procure it in writing (which includes the form of electromagnetic record; the same shall apply hereinafter) as a general rule. In such cases as that Principal does not possess the ability to make judgment regarding the consequences which could arise from giving consent to the handling of Personal Information because the Principal is a minor, adult ward, person under curatorship or under assistance, it becomes necessary to procure consent of a person who has parental authority, is a statutory agent or has authority equivalent thereto in respect of such Principal.

(Restriction Based on Purpose of Use)

Article 5.

1. Regular Member and Electronic Public Offering Member must not handle Personal Information beyond the scope necessary for achieving the purpose of use which was specified pursuant to Article 3 without procuring prior consent of Principal; provided, however, that use of Personal Information to procure prior consent of Principal (e.g., transmitting e-mail or making telephone call) does not constitute unintended use even if such use is not described in the initially specified purpose of use.
2. In the event any Regular Member or Electronic Public Offering Member acquired Personal Information as a result of succeeding to a business of other “Personally Referable Information Handling Business Operator” because of a merger or any other reason, the relevant Regular Member or Electronic Public Offering Member must not, without procuring prior consent of Principal, handle such Personal Information beyond the scope necessary for achieving the purpose of use held by such other “Personally Referable Information Handling Business Operator” prior to the relevant succession;

provided, however, that use of Personal Information to procure prior consent of Principal does not constitute unintended use even if such use is not described in the purpose of use existed prior to the relevant succession.

3. The provisions of the preceding two Paragraphs shall not apply to the following cases:
 - (1) In the case it is based on any law or regulation;
 - (2) In the case it is necessary for protecting person's life, body or property (including juridical person's property), and it is difficult to procure the consent of Principal;
 - (3) In the case it is particularly necessary for improving public health or promoting sound growth of children, and it is difficult to procure the consent of Principal; and
 - (4) In the case it is necessary to cooperate in the execution of work, which is prescribed by any law or regulation, by any national government organ, local government or person entrusted by any of the foregoing, and procuring the consent of Principal is likely to hinder the execution of such work.
 - (5) In the case it is to provide Personal Data to an Academic Research Institution, etc. (referring to a university, other institution or organization having an objective of performing academic researches, or a person belonging thereto; the same shall apply hereinafter) where it is necessary for the Academic Research Institution, etc. to handle the relevant Personal Data for the purpose of using it for an academic research (hereinafter referred to as "Academic Research Purpose") (including the case where a part of the purpose of handling the relevant Personal Data is Academic Research Purpose, and excluding the case where there is a possibility that a personal right or interest may be wrongfully infringed).

(Sensitive Information)

Article 6.

1. Regular Member and Electronic Public Offering Member must not acquire, use or provide to a third party Special-Care-Required Personal Information, or information (excluding the information falling under Special-Care-Required Personal Information) regarding membership in labor union, family origin, registered domicile, health care or sex life (excluding the information which has been published by Principal, national government organ, local government, Academic Research Institution, etc. or any person stipulated in any Item of Paragraph 1 of Article 57 of Protection Act or in any Item of Article 6 of Enforcement Rules, and the information which is obvious in appearance and acquired by looking at or taking picture of Principal; hereinafter referred to as "Sensitive Information") except in the cases provided below:
 - (1) In the case it is based on any law or regulation;
 - (2) In the case it is necessary for protecting person's life, body or property;

- (3) In the case it is particularly necessary for improving public health or promoting sound growth of children;
 - (4) In the case it is necessary to cooperate in the execution of work, which is prescribed by any law or regulation, by any national government organ, local government or person entrusted by any of the foregoing;
 - (5) In the case the Sensitive Information is to be acquired under the situation prescribed in Article 20, Paragraph 2, Item 6 of Protection Act; in the case the Sensitive Information is to be used under the situation prescribed in Article 18, Paragraph 3, Item 6 of the said Act; or in the case the Sensitive Information is to be provided to a third party under the situation prescribed in Article 27, Paragraph 1, Item 7 of the said Act;
 - (6) In the case Sensitive Information regarding employee, etc. such as affiliation with or membership in political or religious organization or labor union is to be acquired, used or provided to a third party to the extent necessary for executing the work of collecting withholding tax or the like;
 - (7) In the case Sensitive Information is to be acquired, used or provided to a third party to the extent necessary for the execution of transfer, etc. of rights and obligations under an inheritance procedure;
 - (8) In the case Sensitive Information is to be acquired, used or provided to a third party—on the ground of the necessity for securing appropriate business operation of Self-Offering and Other Transactions, etc. conducted by the relevant Regular Member or Electronic Public Offering Member—based on the consent of Principal, to the extent necessary for the execution of the business; and
 - (9) In the case biometric authentication information, which falls under Sensitive Information, is to be used for identity verification based on the consent of Principal.
2. When acquiring, using, or providing to a third party Sensitive Information under any of the cases set forth in the preceding Paragraph, the relevant Regular Member or Electronic Public Offering Member must handle it especially carefully so as not to make such acquisition, use or provision to a third party in deviation from the conditions set forth in the preceding Paragraph.
 3. When acquiring, using, or providing to a third party Sensitive Information under any of the cases set forth in Paragraph 1, the relevant Regular Member or Electronic Public Offering Member must act appropriately in accordance with the laws and regulations, etc. related to protection of Personal Information.

4. When providing Sensitive Information to a third party, the relevant Regular Member or Electronic Public Offering Member must not apply the provision of Article 27, Paragraph 2 (opt out) of Protection Act.

(Prohibition of Inappropriate Utilization)

Article 6-2.

Regular Member and Electronic Public Offering Member must not utilize Personal Information using a method that has the possibility of fomenting or prompting unlawful or unfair act.

(Appropriate Acquisition of Personal Information)

Article 7.

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

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

Article 8.

1. When having acquired Personal Information, the relevant Regular Member or Electronic Public Offering Member must promptly notify the purpose of its use to Principal or publish it, unless such purpose of use has already been published. In such case, the relevant “notice” must be made in writing as a general rule, and the relevant “publication” must be made in an appropriate manner—such as publishing it on the Internet website, etc., or displaying or making available document at a counter, etc. of its business office—in accordance with its mode of business such as its method of selling financial instruments.
2. Notwithstanding the provision of the preceding Paragraph, when Personal Information described in a written agreement or other document is to be acquired as a result of concluding agreement with Principal, the relevant Regular Member or Electronic

Public Offering Member must expressly indicate the purpose of its use to the Principal in advance; provided, however, that the foregoing does not apply to the case where the Personal Information is needed urgently in order to protect the life, body or property of a person.

3. When any Regular Member or Electronic Public Offering Member has changed the purpose of use, it must notify to Principal, or publish, the changed purpose of use.
4. The provisions of the preceding three Paragraphs shall not apply to the following cases:
 - (1) In the case notifying to Principal, or publishing, the purpose of use is likely to result in harming the life, body, property or any other right or interest of the Principal or a third party;
 - (2) In the case notifying to Principal, or publishing, the purpose of use is likely to result in harming the right, or just and proper interest, of the relevant Regular Member or Electronic Public Offering Member;
 - (3) In the case it is necessary to cooperate in the execution of work, which is prescribed by any law or regulation, by any national government organ or local government, and notifying to Principal, or publishing, the purpose of use is likely to result in hindering the execution of such work; and
 - (4) In the case the purpose of use is deemed to be clear in the light of the circumstances of the acquisition.

(Securing Accuracy of Data)

Article 9.

Each Regular Member and Electronic Public Offering Member must strive to maintain Personal Data accurate and up-to-date to the extent necessary for achieving the purpose of use, through such means as developing the procedure to collate and verify Personal Data at the time of inputting it in Personal Information Database, etc., developing the procedure for making correction, etc. upon finding error, etc., updating recorded matters and establishing the retention period. It is not necessary to make the retained Personal Data to be updated uniformly or constantly, and it shall be sufficient if its accuracy and recency is secured in accordance with the corresponding purpose of use and to the extent necessary for such purpose.

Furthermore, each Regular Member and Electronic Public Offering Member must prescribe retention period for retained Personal Data in accordance with the purpose of use by, for example, setting the retention period for Personal Data regarding customers, etc. to

be of such length so that it expires within a certain period of time after the termination of the relevant agreement, and must delete the retained Personal Data after the lapse of the relevant period.

However, the foregoing shall not apply to the case where the retention period is prescribed under any law, regulation, etc.

(Security Control Measures)

Article 10.

1. Each Regular Member and Electronic Public Offering Member must take necessary and appropriate measures—such as developing fundamental policy/handling rules, etc. on security control, and developing a system for implementing security control measures—for the purpose of preventing Leakage, etc. in respect of Personal Data it handles and other security control for Personal Data. The necessary and appropriate measures must include “Systematic Security Control Measures,” “Human Security Control Measures,” “Physical Security Control Measures,” “Technological Security Control Measures” and “Comprehension of External Environment” for each stage of acquisition, use, retention, etc. of Personal Data.

The measures must be prepared in consideration of the extent of infringement of rights and interests that will be suffered by Principal if Leakage, etc. occurs in respect of Personal Data, and must be corresponding to the risks attributable to such factors as the scale and nature of the business, the condition of handling Personal Data (including the nature and volume of Personal Data being handled), and the nature of the medium which records Personal Data. The definitions of the terms used in this Article are as set forth below:

- (1) Systematic Security Control Measures

This refers to the development of systems and implementation of measures by each Regular Member and Electronic Public Offering Member, which consist of the following acts among others: defining the responsibilities and authorities of officers and employees (referring to those who are within the organization of the relevant Regular Member or Electronic Public Offering Member, directly or indirectly subject to the instructions and supervision of the relevant Regular Member or Electronic Public Offering Member and engaged in the business conducted by the relevant Regular Member or Electronic Public Offering Member, and they are not limited to the employees (full-time employees, contract employees, part-time employees, part-timers, nonregular workers, etc.) having employment relationship

with the relevant Regular Member or Electronic Public Offering Members, but also include those who do not have employment relationship with the relevant Regular Member or Electronic Public Offering Member (including the directors, accounting advisors (in the case where the accounting advisor is a corporation, its employees who perform such duties), company auditors, executive officers, temporary workers sent from temp agencies, etc.); the same shall apply hereinafter) concerning security control measures for Personal Data; preparing and operating rules, etc. on security control; and checking and inspecting their implementation status.

(2) Human Security Control Measures

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

(3) Physical Security Control Measures

This refers to the physical measures concerning security control of Personal Data, such as management of the areas where Personal Data is handled, prevention of theft of equipment and electronic media, etc., prevention of Leakage, etc. when electronic media are being carried about, and disposition of equipment and electronic media, etc.

(4) Technological Security Control Measures

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

(5) Comprehension of External Environment

This refers to the comprehension of the systems, etc. for the protection of Personal Information in the relevant foreign country when Personal Data is to be handled in a foreign country.

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

(1) Development of rules, etc.

- (a) Development of fundamental policy on security control for Personal Data;
- (b) Development of handling rules on security control for Personal Data;
- (c) Development of rules on checking and inspecting the condition of handling Personal Data; and

- (d) Development of rules on outsourcing.
- (2) Handling rules on security control at each control stage
 - (a) Handling rules for the acquisition and input stage;
 - (b) Handling rules for the use and processing stage;
 - (c) Handling rules for the safekeeping and retention stage;
 - (d) Handling rules for the transfer/transmission stage;
 - (e) Handling rules for the deletion/disposition stage; and
 - (f) Handling rules for the stage of dealing with Leakage, etc. Incident (referring to the incident where Leakage, etc. has occurred or may have occurred; the same shall apply hereinafter).
- 3. Each Regular Member and Electronic Public Offering Member must implement the following “Systematic Security Control Measures,” “Human Security Control Measures,” “Physical Security Control Measures” and “Technological Security Control Measures” for the development of systems of implementing security control for Personal Data.
 - (1) Systematic Security Control Measures
 - (a) Appointing a person who is responsible for managing Personal Data;
 - (b) Enhancing the work rules, etc. with security control measures;
 - (c) Operating in accordance with the handling rules on security control for Personal Data;
 - (d) Developing the method to check the condition of handling Personal Data;
 - (e) Developing and implementing systems to check and inspect the condition of handling Personal Data; and
 - (f) Developing system to deal with Leakage, etc. Incident.
 - (2) Human Security Control Measures
 - (a) Concluding agreement regarding nondisclosure of Personal Data, etc. with the officers and employees;
 - (b) Clarifying the roles, responsibilities, etc. of the officers and employees;
 - (c) Making security control measures thoroughly known to the officers and employees, and providing education and training for the officers and employees on such measures;
 - (d) Checking the status of compliance with Personal Data control procedures by the officers and employees.
 - (3) Physical Security Control Measures
 - (a) Management of Personal Data handling areas, etc.;

- (b) Prevention of theft, etc. of equipment and electronic media, etc.;
 - (c) Prevention of Leakage, etc. when electronic media, etc. are to be carried about; and
 - (d) Deletion of Personal Data and disposition of equipment and electronic media, etc.
- (4) Technological Security Control Measures
- (a) Identifying and authenticating users of Personal Data;
 - (b) Establishing demarcations of Personal Data for control, and controlling access to Personal Data;
 - (c) Managing the authority to access Personal Data;
 - (d) Personal Data Leakage, etc. preventive measures;
 - (e) Recording and analyzing access to Personal Data;
 - (f) Recording and analyzing the condition of operation of the information system handling Personal Data; and
 - (g) Monitoring and inspecting the information system handling Personal Data.

(Supervision Over Officers and Employees)

Article 11.

1. Each Regular Member and Electronic Public Offering Member must, in making its officers and employees handle Personal Data, establish appropriate internal control system and exercise necessary and appropriate supervision over such officers and employees so that security control will be exerted for the relevant Personal Data. Such supervision must be exercised by taking into consideration the extent of infringement of rights and interests which will be suffered by Principal if Leakage, etc. occurs in respect of the Personal Data, and must be corresponding to the risks attributable to such factors as the nature of business and the condition of handling Personal Data.
2. Each Regular Member and Electronic Public Offering Member must exercise the “necessary and appropriate supervision” over its officers and employees provided for in the preceding Paragraph by developing the following systems, etc.:
 - (1) Concluding with officers and employees at the time of hiring, etc. an agreement, etc. prohibiting the relevant officer or employee, while he/she is with the relevant Regular Member or Electronic Public Offering Member and after he/she left such Member, from allowing a third party to know and from using for any purpose other than the intended purpose of use, Personal Data which he/she has come to know in

relation to the Self-Offering and Other Transactions, etc. conducted by such Member;

- (2) Clearly defining the roles and responsibilities of officers and employees through establishing handling rules for appropriate handling of Personal Data, making security control obligation thoroughly known to officers and employees, and providing education and training for officers and employees regarding such obligation; and
- (3) Developing system to check, among others, the status of compliance with the matters prescribed under internal security control measures, and system to check and inspect the protection of Personal Data by officers and employees, for the purpose of preventing officers and employees from taking out Personal Data.

(Supervision Over Entrusted Party)

Article 12.

1. When entrusting handling of Personal Data in whole or in part (which includes all agreements, regardless of their forms or types, under which the relevant Regular Member or Electronic Public Offering Member causes other person to handle the whole or part of Personal Data), the relevant Regular Member or Electronic Public Offering Member must exercise necessary and appropriate supervision over the entrusted party in order to ensure that security control for the Personal Data the handling of which was entrusted is exerted. The supervision must be exercised by taking into consideration the extent of infringement of rights and interests which will be suffered by Principal if Leakage, etc. occurs in respect of the Personal Data, and must be corresponding to the risks attributable to such factors as the scale and nature of the entrusted operation and the condition of handling Personal Data.
2. Each Regular Member and Electronic Public Offering Member must, when it is to entrust operation to other party, select a party which can be recognized as handling Personal Data properly, and, in order to ensure that security control measures will be exerted for the Personal Data entrusted, must secure measures of security control for Personal Data also at the party which is to be entrusted with operation (in the case where operation is to be entrusted through two or more steps, supervision must be exercised also to check whether the business operator, which is the party entrusted with the operation initially, is exercising sufficient supervision over the business operators to which the operation was re-entrusted, etc.). To be more specific, for example, the following measures, among others, must be taken.

- (1) In order to secure security control for Personal Data, prescribe in the criteria for selecting the party to be entrusted with operation details of such matters as the development of organizational system and the formulation of fundamental policy/handling rules on security control at the party to be entrusted with operation, and review such criteria on a regular basis. In selecting the party to be entrusted with operation, it is desirable to have such persons as those who are responsible for managing Personal Data make assessments appropriately after checking by the method of visiting (including the method of utilizing a video conference system (referring to the method by which a person can recognize such other party's conditions through transmission and reception of image and sound)), if necessary, the site where Personal Data will be handled, or by other reasonable alternative method.
- (2) Include in the relevant entrustment agreement the security control measures which consist of the following: entrusting party's authorities regarding supervision, inspection and collection of reports; prohibition of leakage, unauthorized use, alteration and use for any purpose other than the intended purpose of use, of the Personal Data at the party entrusted with operation; the terms and conditions for re-entrustment; and the responsibility of the party entrusted with operation in the event of occurrence of Leakage, etc. Incident. And by such means as regularly performing inspection, check the status of compliance with the security control measures prescribed in the relevant entrustment agreement on a regular basis or at any time and review the security control measures.

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

If the party entrusted with operation intends to re-entrust the operation to other party, it is desirable that the relevant Regular Member or Electronic Public Offering Member sufficiently checks—by such means as requiring the party entrusted with operation to present report or complete approval procedure in advance and also regularly performing inspection, directly or through the party entrusted with operation, on such matters as the party to be re-entrusted with operation, details of the operation to be re-entrusted, and the method of handling Personal Data by the party to be re-entrusted with operation—to make sure, just

like when making the initial entrustment, that the party entrusted with the operation appropriately exercises the supervision, which is referred to in this Article, over the party re-entrusted with the operation and that the party re-entrusted with the operation implements the security control measures pursuant to Article 23 of Protection Act. The foregoing matters concerning re-entrustment shall also apply to any further re-entrustment made by the party re-entrusted with operation and by any subsequent party.

(Restriction of Provision to a Third Party)

Article 13.

1. Regular Member and Electronic Public Offering Member must not provide Personal Data to a third party (referring to any person, regardless of whether it is a natural person, juridical person or any other organization, other than the relevant Regular Member or Electronic Public Offering Member intending to provide the Personal Data, and the Principal who is the subject of the relevant Personal Data; the same shall apply hereinafter except for the following Article through Article 16-2) without procuring the consent of Principal in advance, except in the cases set forth below. In procuring such consent, the relevant Regular Member or Electronic Public Offering Member must clearly indicate to reasonable and appropriate extent the details that are deemed necessary, in the light of such factors as the scale and nature of the business and the condition of handling Personal Data (including the nature and volume of the Personal Data handled), for Principal to make decision regarding the consent.
 - (1) In the case it is based on any law or regulation;
 - (2) In the case it is necessary for protecting person's life, body or property (including juridical person's property), and it is difficult to procure the consent of Principal;
 - (3) In the case it is particularly necessary for improving public health or promoting sound growth of children, and it is difficult to procure the consent of Principal; and
 - (4) In the case it is necessary to cooperate in the execution of work, which is prescribed by any law or regulation, by any national government organ, local government or person entrusted by any of the foregoing, and procuring the consent of Principal is likely to hinder the execution of such work.
 - (5) In the case the third party is an Academic Research Institution, etc. and it is necessary for the third party to handle the relevant Personal Data for Academic Research Purpose (including the case where a part of the purpose of handling the relevant Personal Data is Academic Research Purpose, and excluding the case

where there is a possibility that a personal right or interest may be wrongfully infringed).

2. With regard to Personal Data that is to be provided to a third party, in the case where provision to a third party of Personal Data which can identify Principal has been suspended in accordance with the request of the Principal, if the relevant Regular Member or Electronic Public Offering Member has in advance notified the Principal of the matters set forth below or placed these matters under such condition so that the Principal can easily know them, and also notified these matters to Personal Information Protection Commission, it may provide the relevant Personal Data to a third party notwithstanding the provision of the preceding Paragraph. The relevant Regular Member or Electronic Public Offering Member must also publish the contents of such notification to Personal Information Protection Commission through use of the Internet or any other appropriate method.
 - (1) Name, address, and the individual name of the representative, of the relevant Regular Member or Electronic Public Offering Member;
 - (2) Provision to a third party shall be made a purpose of use;
 - (3) Items of Personal Data to be provided to a third party;
 - (4) Method of acquiring Personal Data to be provided to a third party;
 - (5) Method of provision to a third party;
 - (6) Provision to a third party of Personal Data which can identify Principal will be suspended in accordance with a request of Principal;
 - (7) Method of receiving the request of Principal;
 - (8) Method of updating Personal Data which is to be provided to a third party; and
 - (9) Scheduled date of commencing the provision to a third party of Personal Data pertaining to the notification.
3. When any of the matters set forth in Item (1) of the preceding Paragraph was changed or when provision of Personal Data pursuant to the preceding Paragraph was terminated, without delay, and when any of the matters set forth in Item (3), (4), (5), (7) or (8) of the preceding Paragraph is to be changed, in advance, the relevant Regular Member or Electronic Public Offering Member must notify Principal to such effect or place the matter under such condition so that Principal can easily know it, and also notify Personal Information Protection Commission to such effect.

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

4. The person who receives provision of the relevant Personal Data in the cases set forth below does not fall under a third party:
 - (1) In the case Personal Data is provided as a result of entrustment by the relevant Regular Member or Electronic Public Offering Member of the entire or a part of handling of Personal Data within the extent necessary for achieving the purpose of use;
 - (2) In the case Personal Data is provided as a result of succession of a business because of a merger or any other reason (limited to the case where the Personal Data continues to be used, even after the succession of the business, within the scope of the purpose of use which existed prior to its provision resulting from the relevant succession of the business); and
 - (3) In the case Personal Data, which is to be used jointly with other specific persons, is provided to such specific persons, and such fact, the items of Personal Data to be used jointly, the scope of such joint users, the users' purpose of use, the individual name or name of the person responsible for the management of the relevant Personal Data (referring to the person who is primarily responsible for receiving and processing complaint, for making disclosure, correction, etc., for making decisions on such matters as suspension of use, and for security control, at such joint users; such person being referred to as "Control Manager" in Paragraph 6) and the individual name of the representative if it is a juridical person (if it is an organization which does not have legal personality but has its designated representative or manager, such representative or manager; the same shall apply in this Article, Article 16, Paragraph 1, Item (1) and Article 17, Paragraph 1, Item (1)) have already been notified to Principal or placed under such condition so that Principal can easily know them.
5. The notification to be made by the relevant Regular Member or Electronic Public Offering Member pursuant to the provision of Item (3) of the preceding Paragraph shall be in writing as a general rule. With regard to the notification, etc. concerning "the scope of such joint users," the relevant Regular Member or Electronic Public Offering Member must strive to individually list each of such joint users.
6. When the individual name, name or address of Control Manager provided for in Item (3) of Paragraph 4, or the individual name of the representative if it is a juridical person, was changed, without delay, and when the user's purpose of use provided for in the same Item or the person with the responsibility is to be changed, in advance, the relevant Regular Member or Electronic Public Offering Member must notify Principal

to such effect or place the matter under such condition so that Principal can easily know it.

7. The provision of Paragraph 2 does not apply to the case where Personal Data to be provided to a third party is Sensitive Information, was obtained in violation of the provision of Paragraph 1 of Article 20 of Protection Act, or was provided by other “Personally Referable Information Handling Business Operator” pursuant to the provision of the main text of Paragraph 1 (including its entire or partial copy and processed data).

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

Article 14.

1. If Regular Member or Electronic Public Offering Member is to provide Personal Data to a third party (excluding those which have developed a system conforming to the standards prescribed in Enforcement Rules that are considered to be necessary for continuously implementing the measures equivalent to the measures which “Personally Referable Information Handling Business Operator” is required to implement for handling of Personal Data (hereinafter referred to as “Equivalent Measures”); the same shall apply hereafter in this Paragraph, Paragraphs 2 through 4 and Article 16-2, Paragraph 1, Item (2)) in a foreign country (referring to any nation or region outside the territory of Japan; the same shall apply hereinafter) (excluding those that are prescribed in Enforcement Rules as a country having a system for protecting Personal Information which is recognized to be at the level equivalent to that of Japan in terms of protection of personal rights and interests; the same shall apply hereafter in this Article, the following Article and Article 16-2, Paragraph 1, Item (2)), it must procure the consent of Principal to the provision to a third party in a foreign country in advance, except in the cases set forth in each Item of Paragraph 1 of the preceding Article. In such case, the provisions of the said Article shall not apply.
2. When Regular Member or Electronic Public Offering Member is to procure the consent of Principal pursuant to the provision of the preceding Paragraph, it must provide in advance the Principal with the information described below; provided, however, that if the information described in Item (3) cannot be provided, information regarding such fact and the reason therefor must be provided.
 - (1) Name of the relevant foreign country;
 - (2) Information on the system for protecting Personal Information in the relevant foreign country which was obtained through an appropriate and reasonable method;

- (3) Information on the measures to be implemented by the relevant third party for the protection of Personal Information;
 - (4) The third party to which Personal Data is to be provided;
 - (5) Purpose of use by the third party to which Personal Data is to be provided; and
 - (6) Items of Personal Data to be provided to the third party.
3. Notwithstanding the provisions of the preceding Paragraph, if the foreign country where the third party to which Personal Data is to be provided is located cannot be identified at the time Regular Member or Electronic Public Offering Member attempts to procure the consent of Principal, it must provide the Principal with the information described below; provided, however, that the information described in Item (2) shall be provided only if it is possible to provide such information.
 - (1) The fact that it cannot be identified and the specific reason therefor (including the necessity to procure the consent of Principal before the third party to which Personal Data is to be provided is determined); and
 - (2) Information which should serve as reference for Principal in place of the name of the foreign country where the third party to which Personal Data is to be provided is located.
 4. In the case of the situation set forth in the preceding Paragraph, if the relevant Regular Member or Electronic Public Offering Member was able to identify the foreign country where the third party to which Personal Data is to be provided is located thereafter, it must provide Principal with the information described in Items (1) through (3) of Paragraph 2 in accordance with a request made by Principal. Furthermore, the relevant Regular Member or Electronic Public Offering Member must make Principal recognize, by the statements in the written document used to procure its consent, that it can make such a request for provision of information, and also publish such fact as an integral part of "Declaration of Protection of Personal Information" prescribed in Article 26 through such means as keeping it posted on its Internet website, or posting it or making it available at a counter of its business office, etc; provided, however, that even if Principal has made a request for provision of information, in such cases as where proper execution of the operation of the relevant Regular Member or Electronic Public Offering Member is likely to be significantly hindered as a result of providing the information, it is allowed not to provide the whole or a part of the information. In such event, the relevant Regular Member or Electronic Public Offering Member must notify such fact and explain the reason therefor to Principal without delay.
 5. When Regular Member or Electronic Public Offering Member is to provide Personal Data to a third party in a foreign country (limited to those which have developed the system prescribed in Paragraph 1; the same shall apply hereafter in this Paragraph and Paragraphs 6 and 7), it must check, through an appropriate and reasonable method, whether a system exists in the relevant foreign country which is likely to affect the execution of Equivalent Measures by the third party and the details thereof, and in the

case such a system exists, the possibility to secure execution of Equivalent Measures by the third party.

6. In the case where Regular Member or Electronic Public Offering Member has provided Personal Data to a third party pursuant to the provision of the preceding Paragraph, it must implement the following measures as the measures that are necessary to secure continuous execution of Equivalent Measures by the third party:
 - (1) Periodically check, through an appropriate and reasonable method, the status of execution of Equivalent Measures by the third party, and whether a system exists in the relevant foreign country which is likely to affect the execution of the relevant Equivalent Measures, and the details thereof; and
 - (2) If a problem concerning the execution of Equivalent Measures by the third party has occurred, implement necessary and appropriate measures, and in the case securing continuous execution of the relevant Equivalent Measures has become difficult, suspend provision of Personal Data to the third party.
7. In the case where Regular Member or Electronic Public Offering Member has provided Personal Data to a third party pursuant to the provision of Paragraph 5, if it has received a request from Principal, it must provide the Principal with the information described below without delay. Furthermore, the relevant Regular Member or Electronic Public Offering Member must publish the fact that such request for provision of information can be made, through such means as keeping it posted on its Internet website, or posting it or making it available at a counter of its business office, etc., as an integral part of “Declaration of Protection of Personal Information” prescribed in Article 26, provided, however, that if proper execution of the operation of the relevant Member is likely to be significantly hindered as a result of providing the information, it is allowed not to provide the whole or a part of the information. In such event, the relevant Regular Member or Electronic Public Offering Member must notify such fact and explain the reason therefor to the Principal without delay.
 - (1) Method by which the third party in a foreign country develops the system prescribed in Paragraph 1;
 - (2) Outline of Equivalent Measures to be executed by the third party in a foreign country;
 - (3) Method and the frequency of checking the status of execution of Equivalent Measures by the third party in a foreign country, whether a system exists in the relevant foreign country which is likely to affect the execution of the relevant Equivalent Measures, and the details thereof;
 - (4) Name of the relevant foreign country;
 - (5) Whether a system exists in the relevant foreign country which is likely to affect the execution of Equivalent Measures by the third party in a foreign country, and the outline thereof;
 - (6) Whether there is any obstacle to the execution of Equivalent Measures by the third party in a foreign country, and the outline thereof; and

- (7) Outline of the measures to be implemented by the Regular Member or Electronic Public Offering Member that is the provider, if a problem concerning the execution of Equivalent Measures by the third party in a foreign country occurred, in order to resolve or improve the problem.

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

Article 15.

1. The relevant Regular Member or Electronic Public Offering Member must, when it provided Personal Data to a third party (excluding those set forth in each Item of Paragraph 2 of Article 16 of Protection Act; the same shall apply in this Article and the following Article (including the case of mutatis mutandis application by operation of Paragraph 3 of Article 16-2)), prepare record of the date on which the relevant Personal Data was provided, the individual name or name of the relevant third party, and all other matters prescribed in Enforcement Rules; provided, however, that the foregoing shall not apply if the relevant provision of Personal Data falls under any Item of Paragraph 1 or any Item of Paragraph 4 of Article 13 (or, in the case of provision of Personal Data under the provision of Paragraph 1 of the preceding Article, any Item of Paragraph 1 of Article 13).
2. The relevant Regular Member or Electronic Public Offering Member must retain the record stipulated in the preceding Paragraph during the period prescribed in Enforcement Rules from the date of the preparation of such record.

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

Article 16.

1. The relevant Regular Member or Electronic Public Offering Member must confirm the matters set forth below when it receives provision of Personal Data from a third party; provided, however, that the foregoing shall not apply if the relevant provision of Personal Data falls under any Item of Paragraph 1 or any Item of Paragraph 4 of Article 13.
 - (1) The relevant third party's individual name, name, address, and if it is a juridical person, the individual name of its representative; and
 - (2) The circumstances leading to the acquisition of such Personal Data by the relevant third party.
2. The relevant Regular Member or Electronic Public Offering Member must, when it made the confirmation pursuant to the provision of the preceding Paragraph, prepare record of the date on which it received provision of the relevant Personal Data, the

matters pertaining to the relevant confirmation, and all other matters prescribed in Enforcement Rules, and retain such record during the period prescribed in Enforcement Rules from the date of the preparation of such record.

(Restriction on Third Party Provision of Personally Referable Information)

Article 16-2.

1. If a third party is expected to procure Personally Referable Information (limited to the information comprising Personally Referable Information Database, etc.; the same shall apply hereafter in this Article) as Personal Data, Regular Member or Electronic Public Offering Member must not provide the relevant Personally Referable Information to the third party without confirming in advance the matters described below, except in the cases set forth under each Item of Paragraph 1 of Article 13.
 - (1) The Principal's consent to the effect that he or she approves that the third party acquires Personally Referable Information as Personal Data that can identify the Principal by receiving the provision of Personally Referable Information from Personally Referable Information Handling Business Operator, has been obtained.
 - (2) For a provision to a third party in a foreign country, in case of intending to obtain the Principal's consent referred to in the preceding Item, information on the Personal Information protection system of the foreign country, on the action the third party takes for the protection of Personal Information, and other information that is to serve as a reference to the Principal, have been provided in advance to the Principal.
2. When Regular Member or Electronic Public Offering Member attempts to procure the consent of Principal for procuring Personally Referable Information as Personal Data by receiving its provision from Personally Referable Information Handling Business Operator (including the case where it makes Personally Referable Information Handling Business Operator which is the provider procure the consent on its behalf), it must provide the Principal with the information described below.
 - (1) Items of the subject Personally Referable Information; and
 - (2) Purpose of use of Personally Referable Information after it procured it as Personal Data by receiving provision of Personally Referable Information.
3. The provision of Paragraph 6 of Article 14 shall be applied mutatis mutandis to the case where Regular Member or Electronic Public Offering Member provides Personally Referable Information pursuant to the provision of Paragraph 1.
4. The provision of Paragraph 2 of the preceding Article shall be applied mutatis mutandis to the case where Regular Member or Electronic Public Offering Member makes the confirmation pursuant to the provision of Paragraph 1.

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

Article 17.

1. With regard to Retained Personal Data, each Regular Member and Electronic Public Offering Member must place the matters set forth below under such condition so that Principal can know them (which includes making reply without delay in response to a request made by Principal). If the purpose of use includes provision to a third party, the relevant Regular Member or Electronic Public Offering Member must describe such fact as a matter set forth in Item (2).
 - (1) Name, address, and the individual name of the representative, of the Regular Member or Electronic Public Offering Member;
 - (2) Purpose of use of all Retained Personal Data (except for the cases which fall under any of Items (1) through (3) of Paragraph 4 of Article 8);
 - (3) Procedures to respond to the request referred to in the following Paragraph or to the demand referred to in Paragraph 1 of the following Article (including the case of mutatis mutandis application by operation of Paragraph 3 of the said Article), Paragraph 1 of Article 19, or Paragraphs 1 through 3 of Article 20 (if the amount of handling fee has been prescribed pursuant to the provision of Article 23, including the amount of handling fee);
 - (4) Measures implemented for safety management of Retained Personal Data (excluding those that are likely to cause hindrance to safety management of the relevant Retained Personal Data if they are placed under such condition so that Principal can know them (which includes the case of making reply without delay in response to a request made by Principal));
 - (5) The section of the relevant Regular Member or Electronic Public Offering Member which has been designated to receive complaint regarding handling of Retained Personal Data; and
 - (6) Name of Accredited Personal Information Protection Organization and its section to file a request for resolving complaint.
2. Each Regular Member and Electronic Public Offering Member must, when it was requested by Principal to notify the purpose of use of Retained Personal Data which can identify the Principal, notify the Principal of it without delay; provided, however, that the foregoing shall not apply if the situation falls under either of the Items set forth below:
 - (1) If the purpose of use of Retained Personal Data which can identify the Principal is clear as a result of the provision of the preceding Paragraph; or
 - (2) If the situation falls under any of Items (1) through (3) of Paragraph 4 of Article 8.

3. If the relevant Regular Member or Electronic Public Offering Member has decided not to notify the purpose of use of Retained Personal Data requested as referred to in the preceding Paragraph, it must notify the Principal to such effect without delay.

(Disclosure)

Article 18.

1. Each Regular Member and Electronic Public Offering Member must, when it received from Principal a demand to disclose Retained Personal Data which can identify the Principal (including a demand to notify non-existence of such data if such data does not exist), disclose to the Principal the relevant Retained Personal Data without delay through the method demanded by the Principal (if disclosure by such method would require a large amount of expense or disclosure by such method is otherwise difficult, by means of delivering document); provided, however, that if disclosure would result in a situation which falls under any of the Items set forth below, the relevant Regular Member or Electronic Public Offering Member may decide not to disclose all or a part of such data.
 - (1) It is likely to result in harming the life, body, property or any other right or interest of the Principal or a third party;
 - (2) It is likely to cause serious hindrance to appropriate execution of the business of the relevant Regular Member or Electronic Public Offering Member; or
 - (3) It will result in a violation of other law or regulation.
2. If the relevant Regular Member or Electronic Public Offering Member has decided not to disclose all or a part of Retained Personal Data pertaining to the demand referred to in the provision of the preceding Paragraph, if no such Retained Personal Data exists, or if disclosure through the method demanded by the Principal under the provision of the preceding Paragraph is difficult, it must notify the Principal to such effect without delay. If disclosure through the method demanded by the Principal is difficult, the disclosure must be made by means of delivering document after such fact is notified to the Principal.
3. The provisions of the preceding two Paragraphs shall be applied mutatis mutandis to the third-party records pertaining to Personal Data which can identify Principal that are retained pursuant to the provisions of Paragraph 2 of Article 15 or Paragraph 2 of Article 16 (excluding those prescribed by Enforcement Order that will harm the public interest or other interest once their existence or nonexistence becomes known).

(Correction, etc.)

Article 19.

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

(Suspension of Use, etc.)**Article 20.**

1. When any Regular Member or Electronic Public Offering Member received a demand from Principal to suspend use of or delete (hereinafter referred to as “Suspension of Use, etc.”) Retained Personal Data which can identify the Principal, on the ground that the relevant Retained Personal Data was handled in violation of the provisions of Article 5 or Article 6-2, or that such data was obtained in violation of the provisions of Article 7, if such demand is found to have a valid ground, it must effect Suspension of Use, etc. of the relevant Retained Personal Data without delay to the extent necessary to cure the violation; provided, however, that the foregoing shall not apply to the case where it would require a large amount of expense to effect Suspension of Use, etc. of the relevant Retained Personal Data, nor to the case where it would be otherwise difficult to effect the Suspension of Use, etc., if an alternative measure necessary to protect the rights and interests of the Principal is implemented.
2. When any Regular Member or Electronic Public Offering Member received a demand from Principal to suspend provision to a third party of Retained Personal Data which can identify the Principal on the ground that the relevant Retained Personal Data is being provided to a third party in violation of the provisions of Paragraph 1 of Article 13 or Article 14, if such demand is found to have a valid ground, it must suspend provision to a third party of the relevant Retained Personal Data without delay; provided, however, that the foregoing shall not apply to the case where it would

require a large amount of expense to suspend provision of the relevant Retained Personal Data to a third party, nor to the case where it would be otherwise difficult to suspend the provision to a third party, if an alternative measure necessary to protect the rights and interests of the Principal is implemented.

3. When any Regular Member or Electronic Public Offering Member received a demand from Principal to effect Suspension of Use, etc. of Retained Personal Data on the ground that the need for the relevant Regular Member or Electronic Public Offering Member to use Retained Personal Data which can identify the Principal ceased to exist, or that Leakage, etc. Incident prescribed in Paragraph 1 of Article 25 has occurred in respect of Retained Personal Data which can identify the Principal, or that the rights or legitimate interests of the Principal are otherwise likely to be harmed as a result of the handling of Retained Personal Data which can identify the Principal, and if such demand is found to have a valid ground, it must effect without delay Suspension of Use, etc., or suspension of provision to a third party, of the relevant Retained Personal Data to the extent necessary to prevent infringement of the rights and interests of the Principal; provided, however, that the foregoing shall not apply to the case where it would require a large amount of expense to effect Suspension of Use, etc. of the relevant Retained Personal Data, nor to the case where it would be otherwise difficult to effect Suspension of Use, etc., if an alternative measure necessary to protect the rights and interests of the Principal is implemented.
4. When the relevant Regular Member or Electronic Public Offering Member effected Suspension of Use, etc. of Retained Personal Data pertaining to the demand referred to in the provision of Paragraph 1 or the preceding Paragraph, or made decision not to effect such Suspension of Use, etc., or when it suspended provision to a third party of all or a part of Retained Personal Data pertaining to the demand referred to in the provision of Paragraph 2 or the preceding Paragraph, or made decision not to suspend such provision to a third party, it must notify the Principal to such effect (including details of the measures if measures different from those requested by the Principal are to be implemented) without delay.

(Explanation of Reason)

Article 21.

When the relevant Regular Member or Electronic Public Offering Member notifies Principal—pursuant to the provisions of Paragraph 3 of Article 17, Paragraph 2 of Article 18 (including the case of mutatis mutandis application by operation of Paragraph 3 of the

said Article), Paragraph 2 of Article 19, Paragraph 3 of the preceding Article, or Paragraph 4 of the said Article—of its decision not to implement all or a part of the measures, or decision to implement measures entirely or partially different from the measures requested or demanded by the Principal, and explains the reasons therefor to the Principal, it must indicate the grounds for the decision not to implement the measures or for the decision to implement different measures, as well as the facts constituting such grounds.

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

Article 22.

1. With regard to the request referred to in the provision of Paragraph 2 of Article 17, or the demand referred to in the provision of Paragraph 1 of Article 18 (including the case of mutatis mutandis application by operation of Paragraph 3 of the said Article), Paragraph 1 of Article 19, or Paragraphs 1 through 3 of Article 20 (hereinafter referred to as “Demand, etc. for Disclosure, etc.”), each Regular Member and Electronic Public Offering Member may prescribe the procedures to receive such request or demand as set forth below. In such case, the relevant Regular Member or Electronic Public Offering Member must keep posting on its Internet website, or must post or make available at a counter of its business office, etc., such procedures together with Declaration of Protection of Personal Information prescribed in Article 26.
 - (1) Its section to which Demand, etc. for Disclosure, etc. should be made;
 - (2) Forms of documents to be submitted when making Demand, etc. for Disclosure, etc., and any other formalities of Demand, etc. for Disclosure, etc.;
 - (3) Method of identity-verification of the person making Demand, etc. for Disclosure, etc.;
 - (4) The amount of and the method of collecting the handling fee provided for in Article 38, Paragraph 1 of Protection Act (which includes the case where no fee is charged);
 - (5) Matters that are necessary for identifying the Retained Personal Data or the third-party provision record which is the subject of Demand, etc. for Disclosure, etc.; and
 - (6) Method of making reply to Demand, etc. for Disclosure, etc.
2. As a procedure for the case in which an agent (referring to the agent prescribed in Article 11 of Enforcement Order; the same shall apply in this Paragraph) makes Demand, etc. for Disclosure, etc., each Regular Member and Electronic Public Offering Member must prescribe the following matters in addition to each Item of the preceding Paragraph. Making disclosure, etc. directly to the Principal only is not

prevented when responding to Demand, etc. for Disclosure, etc. made by the agent prescribed in Article 11, Item 2 of Enforcement Order.

- (1) Method of identity-verification of the agent; and
 - (2) Method of confirming the agent's authority to represent.
3. In prescribing the procedures for Demand, etc. for Disclosure, etc. pursuant to the provisions of the preceding two Paragraphs, each Regular Member and Electronic Public Offering Member must be considerate so that they will not become excessively burdensome to Principal.

(Handling Fee)

Article 23.

1. Each Regular Member and Electronic Public Offering Member may, when it received a demand for notification of the purpose of use referred to in Paragraph 2 of Article 17 or for disclosure referred to in Paragraph 1 of Article 18 or Paragraph 3 of the said Article, charge handling fee for the execution of the relevant measures.
2. When the relevant Regular Member or Electronic Public Offering Member is to charge handling fee pursuant to the provision of the preceding Paragraph, it must determine the amount of handling fee within the range which can be recognized as reasonable in the light of the actual cost.

(Complaint Processing by Regular Member and Electronic Public Offering Member)

Article 24.

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

(Dealing with Leakage, etc. Incident regarding Personal Information, etc.)

Article 25.

1. Upon becoming aware of the situation prescribed under any Item of Article 7 of Enforcement Rules, the relevant Regular Member or Electronic Public Offering Member must report it to Personal Information Protection Commission (in the event

the authority to receive the report has been delegated to Commissioner of the Financial Services Agency, etc. pursuant to the provision of Article 147 of Protection Act, to the Commissioner of the Financial Services Agency, etc., and in the event a head of a local government, etc. is to administer, pursuant to the provision of Article 165 of Protection Act, the affairs which belong to the authority to receive the report belongs, to the head of the local government, etc.) and the Association in accordance with 3-5-3 of the Guideline for the Act on the Protection of Personal Information (General Rules). Furthermore, upon becoming aware of an occurrence of Leakage, etc. of Personal Data regarding individual customers, etc. handled by itself, or of a situation where such Leakage, etc. may have occurred, the relevant Regular Member or Electronic Public Offering Member must report it to the competent authorities and the Association in accordance with the relevant laws and regulations.

2. Upon becoming aware of the situation described below (excluding the situations prescribed in the preceding Paragraph), the relevant Regular Member or Electronic Public Offering Member must report it to the competent authorities and the Association by applying the provision of the preceding Paragraph.
 - (1) Situation where Leakage, etc. of Personal Information handled by itself has occurred or may have occurred; or
 - (2) Situation where leakage of the deletion information, etc. pertaining to Pseudonymously Processed Information (as for the information regarding the method of processing performed pursuant to the provision of Paragraph 1 of Article 41 of Protection Act, it is limited to the information whose use can restore the Personal Information used for preparing Pseudonymously Processed Information; the same shall apply in the following Paragraph) or of the information on processing method, etc. pertaining to Anonymously Processed Information handled by itself has occurred or may have occurred.
3. Upon becoming aware of the situation prescribed under any Item of Article 7 of Enforcement Rules, the relevant Regular Member or Electronic Public Offering Member must perform, among others, notification to the Principal in accordance with 3-5-4 of the Guideline for the Act on the Protection of Personal Information (General Rules). In addition, also upon becoming aware of the situation described below (excluding the situation prescribed under each Item of Article 7 of Enforcement Rules), the relevant Regular Member or Electronic Public Offering Member shall perform, among others, notification to the Principal by applying the same.

- (1) Situation where Leakage, etc. of Personal Data (excluding Personal Data that is Pseudonymously Processed Information) handled by itself has occurred or may have occurred;
 - (2) Situation where Leakage, etc. of Personal Information (excluding Personal Information that is Pseudonymously Processed Information) handled by itself has occurred or may have occurred; or
 - (3) Situation where leakage of the deletion information, etc. pertaining to Pseudonymously Processed Information or of the information on processing method, etc. pertaining to Anonymously Processed Information handled by itself has occurred or may have occurred.
4. When any of the situations prescribed in Paragraph 1 or Paragraph 2 has been detected, the relevant Regular Member or Electronic Public Offering Member must implement measures that are necessary for the matters described below in accordance with the details, etc. of the relevant situation.
- (1) Reporting within the business establishment and prevention of expansion of damage;
 - (2) Investigation of the facts and clarification of the cause;
 - (3) Identification of the extent of the impact; and
 - (4) Examination and execution of recurrence preventive measures.
- In addition, in accordance with the details, etc. of the relevant situation, the facts of the relevant situation and the recurrence preventive measures, etc. shall be promptly published from the perspectives of prevention of secondary damage and avoidance of an occurrence of a similar incident, etc.
5. Other particulars not discussed above shall be governed by the Guideline for the Act on the Protection of Personal Information (General Rules) (limited to those related to each Item of Article 7 of Enforcement Rules).

(Preparation of Declaration of Protection of Personal Information)

Article 26.

1. Each Regular Member and Electronic Public Offering Member must, in consideration of the importance of providing in advance explanation on its policy of dealing with Personal Information in an easily understandable manner, prepare and publish a declaration regarding the business operator's approach and policy on protection of Personal Information (so-called "privacy policy," "privacy statement," etc.; hereinafter referred to as "Declaration of Protection of Personal Information").

2. Declaration of Protection of Personal Information shall include, for example, the matters set forth below:
 - (1) Declaration of the policy of dealing with protection of Personal Information, such as to comply with applicable laws and regulations, not to use Personal Information for anything other than the intended purpose of use, and to appropriately engage in complaint processing;
 - (2) Easily understandable explanation on the procedures of notification, publication, etc. of the purpose of use provided for in Article 21 of Protection Act;
 - (3) Easily understandable explanation on various procedures regarding handling of protection of Personal Information, such as the procedures for disclosure, etc. provided for in Article 32 of Protection Act; and
 - (4) Section to contact for inquiries and complaint processing regarding handling of Personal Information.
3. Each Regular Member and Electronic Public Offering Member must strive to include as much as possible in Declaration of Protection of Personal Information statements which take into account the following points from the perspective of protection of rights and interests of Principal such as consumers in the light of the characteristics, scale and actual condition of the business activities:
 - (1) If Principal him/herself makes a request regarding Retained Personal Data, the relevant Regular Member or Electronic Public Offering Member is to voluntarily accommodate request for suspension of use, etc., such as suspension of sending direct mail;
 - (2) The relevant Regular Member or Electronic Public Offering Member is to improve transparency of entrustment process by, for example, clarifying existence or nonexistence of entrustment and details of the operation to be entrusted;
 - (3) The relevant Regular Member or Electronic Public Offering Member is to make the purpose of use clearer for Principal by, for example, indicating the purpose of use by limiting it according to each different type of customers based upon reflection on details of its business, or voluntarily engaging in limiting the purpose of use based on elections made by Principal; and
 - (4) The relevant Regular Member or Electronic Public Offering Member is to expressly state the source of Personal Information or the method of its procurement (type of the source of information, etc.) as concretely as possible.

(Report to the Association)

Article 27.

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

Supplementary Provisions (May 20, 2011)

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

Supplementary Provisions (May 26, 2015)

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

(Note) Amended provisions are as follows:

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

Article 21; Paragraphs 1 through 3 of Article 22; Paragraph 1 and Item (3) of Paragraph 3 of Article 23; and Paragraphs 1 and 2 of Article 24.

Supplementary Provisions (August 26, 2015)

This amendment shall become effective from August 26, 2015.

(Note) Amended provisions are as follows:

- (1) Amended Paragraph 1 of Article 1; the main text of Paragraph 1 of Article 10 and Item (3) of Paragraph 3 of the said Article; Paragraph 1 of Article 11; Paragraph 1 of Article 12; and the main text and Items (1) and (2) of Paragraph 2 of the said Article; and
- (2) Newly added Paragraph 2 of Article 7.

Supplementary Provisions (April 28, 2017)

This amendment shall become effective from May 30, 2017.

(Note) Amended provisions are as follows:

- (1) Amended Paragraphs 1 and 2 of Article 1;
- (2) Amended Item (1) of Paragraph 1 of Article 2; newly added Item (2) of the said Paragraph, and moved down former Item (2) of the said Paragraph by one item so that it has become Item (3), and amended the said Item; moved down former Items (3) through (5) by one item each; and newly added Item (7) of the said Paragraph;
- (3) Amended Paragraphs 3 and 4 of Article 3; Article 4; Paragraphs 1 and 2 of Article 5; the main text of Paragraph 1, and Paragraphs 2 through 4 of Article 6; Paragraphs 1 and 2 of Article 8; Article 9; and the main text of Paragraph 1 of Article 10;
- (4) Amended the main text of Paragraph 1, and the main text and Item (3) of Paragraph 2 of Article 13, and newly added Item (5) of the said Paragraph; and amended Paragraph 3, Items (1) through (3) of Paragraph 4, and Paragraph 5 of the said Article;
- (5) Newly added Articles 14 through 16;

- (6) Moved down former Article 14 to become Article 17; and amended Items (2) and (3) of Paragraph 1, and the main text of Paragraph 2 of the said Article;
- (7) Moved down former Article 15 to become Article 18; and amended the main text of Paragraph 1, and Paragraph 2 of the said Article;
- (8) Moved down former Article 16 to become Article 19; and amended Paragraphs 1 and 2 of the said Article;
- (9) Moved down former Article 17 to become Article 20; and amended Paragraphs 1 through 3 of the said Article;
- (10) Moved down former Article 18 to become Article 21 and amended the said Article;
- (11) Moved down former Article 19 to become Article 22; and amended the headword, the main text and Items (1) through (6) of Paragraph 1, the main text of Paragraph 2, and Paragraph 3 of the said Article;
- (12) Moved down former Article 20 to become Article 23; and amended Paragraphs 1 and 2 of the said Article;
- (13) Moved down former Article 21 to become Article 24; and amended Paragraph 1 of the said Article;
- (14) Moved down former Article 22 to become Article 25; and amended the headword and Paragraphs 1 through 3 of the said Article;
- (15) Moved down former Article 23 to become Article 26; and amended Paragraph 1, and Items (2) and (3) of Paragraph 2 of the said Article; and
- (16) Moved down former Article 24 to become Article 27.

Supplementary Provisions (March 4, 2022)

This amendment shall become effective from April 1, 2022.

(Note) Amended provisions are as follows:

- (1) Amended Paragraphs 1 and 2 of Article 1;
- (2) Amended Items (3) and (5) of Article 2; and newly added Items (8) through (10) of the said Article;
- (3) Amended Article 4;
- (4) Newly added Item (5) of Paragraph 3 of Article 5;

- (5) Amended the main text of Paragraph 1 of Article 6; newly added Item (5) of the said Paragraph; and moved down former Items (5) through (8) of the said Paragraph to become Items (6) through (9); and amended Paragraph 4;
- (6) Newly added Article 6-2;
- (7) Amended the main text of Paragraph 1 of Article 10; newly added Items (3) and (5) of the said Paragraph; moved down former Item (3) of the said Paragraph to become Item (4); amended Sub-item (f) of Item (2) of Paragraph 2 and the main text of Paragraph 3 of the said Article; newly added Item (3) of the said Paragraph; and moved down former Item (3) of the said Paragraph to become Item (4);
- (8) Amended Paragraph 1 of Article 11;
- (9) Amended Paragraph 1 and Items (1) and (2) of Paragraph 2 of Article 12;
- (10) Newly added Item (5) of Paragraph 1 of Article 13; amended the main text of Paragraph 2 of the said Article; newly added Items (1), (4), (8) and (9) of the said Paragraph; moved down former Items (1) and (2) of the said Paragraph by one item each; moved down former Items (3) through (5) of the said Paragraph by two items each; amended Paragraph 3, Item (3) of Paragraph 4 and Paragraph 6 of the said Article; and newly added Paragraph 7 of the said Article;
- (11) Amended Paragraph 1 of Article 14; and newly added Paragraphs 2 through 7 of the said Article;
- (12) Amended Paragraph 1 of Article 15;
- (13) Amended Item (1) of Paragraph 1 of Article 16;
- (14) Newly added Article 16-2;
- (15) Amended Items (1) and (3) of Paragraph 1 of Article 17; newly added Item (4) of the said Paragraph; and moved down former Items (4) and (5) of the said Paragraph by one item each;
- (16) Amended the main text of Paragraph 1 and Paragraph 2 of Article 18; and newly added Paragraph 3 of the said Article;

- (17) Amended Paragraphs 1 and 4 of Article 20; and newly added Paragraph 3 of the said Article;
- (18) Amended Article 21;
- (19) Amended the main text and Items (4) and (5) of Paragraph 1 of Article 22;
- (20) Amended Paragraph 1 of Article 23;
- (21) Amended Paragraphs 1 through 3 of Article 25; and newly added Paragraphs 4 and 5 of the said Article; and
- (22) Amended Items (2) and (3) of Paragraph 2 of Article 26.

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.