Guidelines for Protection of Personal Information

Established on March 18, 2005
Revised on September 21, 2007
Revised on March 21, 2008
Revised on March 19, 2009
Revised on December 17, 2009
Revised on December 20, 2012
Revised on October 15, 2015
Revised on February 18, 2016
Revised on April 20, 2017
Revised on July 15, 2021

Article 1. Purpose

1. In accordance with the Act on the Protection of Personal Information (Act No. 57 of 2003; hereinafter referred to as the "Protection Act"), the Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003; hereinafter referred to as the "Enforcement Order"), the Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3 of 2016; hereinafter referred to as the "Enforcement Rules"), the Basic Policy on the Protection of Personal Information (Cabinet Decision on April 2, 2004), the Guidelines on the Act on the Protection of Personal Information (Volume on General Rules) (Notification of the Personal Information Protection Commission No. 6 of 2016), (Volume on Provision to a Third Party in a Foreign Country) of the said guidelines (Notification of the Personal Information Protection Commission No. 7 of 2016), (Volume on Confirmation and Record-Keeping Obligations upon Third-Party Provision) of the said guidelines (Notification of the Personal Information Protection Commission No. 8 of 2016), (Volume on Anonymously Processed Information) of the said guidelines (Notification of the Personal Information Protection Commission No. 9 of 2016), the Guidelines for the Protection of Personal Information in the Finance Sector (Notification of the Personal Information Protection Commission, Financial Services Agency No. 1 of 2017) and the Practical Guideline on the Security Control Actions under the Guidelines for Protection of Personal Information in the Finance Sector (Notification of the Personal Information Protection Commission, Financial Services Agency No. 2 of 2017), and others (hereinafter referred to as the "Laws and Regulations on Protection of Personal Information"), these guidelines provide for specification of utilization purposes, security control actions and other matters related to personal information as well as specific actions to be taken by Full Members (meaning Full Members specified in Article 7, Paragraph 1, Item 1 of the Articles of Incorporation; the same shall apply hereinafter) of the Investment Trusts Association, Japan (hereinafter referred to as the "Association") in order to ensure the proper handling of personal information in business operations related to the investment management business (meaning operations set forth in Article 2, Paragraph 8, Item 12 (a) and Item 14 of the same paragraph of the Financial Instruments and Exchange Act (Act No 25 of 1948; hereinafter referred as the "FIEA") including business operations incidental thereto) operated by Full Members and business operations related to investment trust managed without instructions from the settlor, and business operations set forth in Article 2, Paragraph 8, Item 7 of the FIEA in association with beneficiary certificates, etc. (meaning beneficiary certificates (including book-entry transfer beneficial

interest in an investment trust), investment corporation bond certificates (including book-entry transfer investment equity) or investment corporation bond certificates (including book-entry transfer investment corporation bonds)).

2. In order to prevent divulgation, unauthorized leakage, or any other similar incident involving personal information, it is necessary for Full Members to develop systems for appropriate control of personal information in accordance with Laws and Regulations on Protection of Personal Information as well as related laws and regulations and guidelines, etc.

Article 2. Definition

In the Guidelines, the terms set forth in the following items are as defined in the respective items.

(1) Personal Information

This term refers to any information relating to a living person that is capable of identifying a specific person (including any information that can be readily collated with other information and thereby can identify a specific individual) or which contains a personal identification code.

"Information Relating to an Individual" is not limited to information identifying an individual such as name, address, gender, date of birth and face image, and is all information representing facts, judgment, and evaluation with respect to attributes such as body, property, occupation and title of an individual, which also includes evaluation information, information made public by publications, etc., and information in the form of image or voice, whether or not such information is concealed by encryption, etc. If the above-mentioned "Information Relating to an Individual," combined with names, etc., "can identify a specific individual," it becomes "Personal Information."

If Information Relating to a non-living Individual is simultaneously Information Relating to a living Individual such as bereaved family members, the information shall be regarded as Information Relating to the living Individual.

In addition, information relating to corporations and other organizations, such as company name, does not basically fall under the category of "Personal Information"; however, when Information Relating to an Individual, such as names of officers, is included in the information, such part of the information falls under the category of "Personal Information."

Furthermore, "individuals" naturally include foreign nationals.

(1-2) Personal Identification Codes

This term refers to letters, numbers, symbols, and other codes specified in Article 1 of the Enforcement Order as those that can identify a specific individual from the information alone.

(2) Personal Information Database, etc.

This term refers to a collection of information including Personal Information listed below; provided, however, that this shall exclude those that are unlikely to damage rights and interests of individuals in light of the method of use.

(a) Database, etc. systematically arranged so that specific Personal Information can be searched by using a computer

(b) In addition to those described in (a) above, database, etc. systematically arranged so that specific

Personal Information can be easily searched by organizing personal information in accordance with certain rules, which are placed in such a state that it can be easily searched with a table of contents, index, codes, etc.

(3) Personal Data

This term refers to Personal Information constituting a Personal Information Database, etc.

(4) Personal Information Handling Business Operators

This term refers to a person providing a Personal Information Database, etc. for use in business; however, excluding central government organizations, local governments, incorporated administrative agencies, etc. set forth by the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003), and local incorporated administrative agencies set forth by the Local Incorporate Administrative Agencies Act (Act No. 118 of 2003).

The term "business" used herein in reference to "for use in business" means similar acts that are repeatedly and continuously carried out for a certain purpose and deemed to be business under normal social conventions, whether for profit or non-profit.

In addition, any person providing a Personal Information Database, etc. for use in business is deemed to be a Personal Information Handling Business Operator, regardless of the number of specific individuals identified by Personal Information constituting the Personal Information Database, etc.

Even a non-juridical association (voluntary organization) or an individual with no capacity of right shall be deemed to be a Personal Information Handling Business Operator if the association or individual provides a Personal Information Database, etc. for use in business.

(5) Principal

The term refers to a specific person identified by Personal Information.

(6) Retained Personal Data

This term refers to any Personal Data for which a Full Member has all authority to disclose, correct, add to or delete from the contents, to discontinue use, to erase, or to discontinue provision to any third party at the request of a Principal or his/her representative, other than the following Personal Data.

(a) Personal Data that are likely to harm the life, body, or property of a Principal or a third party if their presence or absence is made known

(b) Personal Data that are likely to promote or induce illegal or unjust acts if their presence or absence is made known

(c) Personal Data that are likely to impair the safety of Japan, impair trust relationship with other countries or international organizations, or suffer disadvantages in negotiations with other countries or international organizations if their presence or absence is made known

(d) Personal Data that are likely to interfere with the prevention, suppression, or investigation of crimes or the maintenance of public safety and order if their presence or absence is made known

(e) Personal data to be deleted (except for renewal) within six (6) months

(7) Special Care-required Personal Information

The term refers to Personal Information comprising certain descriptions, etc. as those whose handling requires special care so as not to cause unfair discrimination, prejudice, or other disadvantages.

(8) Sensitive Information

In the finance sector, this term refers to Special Care-required Personal Information and information relating to individuals' membership in a labor union, family origin, registered domicile, healthcare, and sex life (among these, excluding the matters falling under the category of the Special Care-required Personal Information) (excluding any information made public by the Principal or by a national government organ, local public entity, or any of those set forth in the items of Article 76, Paragraph 1 of the Protection Act, or the items of Article 6 of the Enforcement Rules, or seemingly clear information acquired by visual observation, filming, or photographing of the Principal).

(9) Anonymously Processed Information

This term refers to Information Relating to an Individual that can be produced from processing Personal Information so as to neither be able to identify a specific individual by taking action prescribed in accordance with the divisions of Personal Information nor be able to restore the Personal Information.

Article 3. Specification of Purpose of Use

1. A Full Member must, in handling Personal Information, specify in what kind of business the Personal Information is provided for use and for what purpose it is used as explicitly as possible so that the Principal can reasonably anticipate them.
2. When a utilization purpose in the preceding paragraph is specified, abstract expressions such as "to be used for a purpose required by the company" are not considered to satisfy the requirement of "as explicitly as possible." Therefore, a Full Member must make efforts to specify the utilization purpose by indicating the financial instruments or services to be provided.
3. When utilization purposes of specific Personal Information are limited by laws and regulations, etc., a Full Member is to clearly indicate that fact.
4. A Full Member must, in case of altering utilization purpose, not do so beyond "the scope recognized reasonably relevant to the pre-altered utilization purpose" stipulated in Article 15, Paragraph 2 of the Protection Act.

Article 4. Format of Consent

When obtaining the consent of a Principal specified in the next article, Article 13 and Article 13-2, a Full Member is to do so in writing (including an electromagnetic record; the same shall apply hereinafter) in principle.

In the case where the Principal is a minor, adult ward, person under curatorship, or person under assistance and does not have the ability to judge results of the consent to the handling of Personal Information, and other cases, consent must be obtained from a person with parental authority or legal representative, etc.

Article 5. Restriction due to a Utilization Purpose

1. A Full Member must not handle Personal Information without obtaining in advance a Principal's consent beyond the necessary scope to achieve a utilization purpose specified in Article 3.

However, use of Personal Information (such as sending an e-mail or making a telephone call) to obtain a

Principal's consent in advance shall not be deemed as a utilization for unintended purposes even if it is not included the utilization purposes as originally specified.

2. A Full Member must, in case of having acquired Personal Information as a result of succession of a business from another Personal Information Handling Business Operator because of a merger or other reason, not handle the Personal Information without obtaining in advance a Principal's consent beyond the necessary scope to achieve the pre-succession utilization purpose of the said Personal Information.

   In addition, when personal information is handled within the necessary scope to achieve the pre-succession utilization purpose, it shall not be deemed as a utilization for unintended purposes, and a Principal's consent does not need to be obtained.

3. The preceding two paragraphs shall not apply to any of the following cases.
   (1) Cases based on laws and regulations
   (2) Cases in which there is a need to protect a human life, body, or property, and when it is difficult to obtain a Principal's consent
   (3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a Principal's consent
   (4) Cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a Principal's consent would interfere with the performance of the said affairs

Article 6. Handling of Sensitive Information

1. A Full Member shall not acquire, use, or provide to a third party any Sensitive Information, except for the following cases.
   (1) Cases based on laws and regulations, etc.
   (2) Cases in which there is a need to protect a human life, body, or property
   (3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children
   (4) Cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations
   (5) Cases in which there is a need to acquire, use, or provide to a third party any Sensitive Information of its employees, etc. concerning their affiliation to or membership in a political or religious group or labor union within the scope necessary for the performance of affairs relating to withholding taxes, etc.
   (6) Cases in which any Sensitive Information is acquired, used, or provided to a third party to the extent necessary for performing the transfer of rights and obligations arising from inheritance procedures
   (7) Cases in which a Full Member acquires, uses, or provides to a third party any Sensitive Information based on the consent of a Principal to the extent necessary for performing its services from the necessity to ensure appropriate operation of its businesses run by the Full Member
   (8) Cases in which biometric information, which falls under the category of Sensitive Information, is used based on a Principal's consent for the purpose of identity verification

2. When a Full Member acquires, uses, or provides to a third party any Sensitive Information in the case set forth in the preceding paragraph, the Full Member shall handle the information with extreme caution so as to avoid acquisition, use, or provision to a third party of the information beyond the grounds set forth in the same paragraph.
3. When a Full Member acquires, uses, or provides to a third party any Sensitive Information in the cases set forth in Paragraph 1 of this article, the Full Member must make a response appropriately in accordance with Laws and Regulations on Protection of Personal Information.
4. Article 23, Paragraph 2 of the Protection Act (opt-out provision) is not to apply to the case where a Full Member provides Sensitive Information to a third party.

Article 7. Proper Acquisition of Personal Information

1. A Full Member must not acquire Personal Information by deceit or other improper means. In addition, a Full Member must not unjustifiably infringe interests of a Principal in acquiring Personal Information from a third party.
2. When acquiring Personal Information through provision from a third party, a Full Member shall confirm the status of compliance with laws and regulations of the provider and also confirm that the Personal Information has been lawfully acquired.

Article 8. Notification, Public Disclosure, Clear Indication, etc. of a Utilization Purpose When Acquiring Personal Information

1. A Full Member must, in case of having acquired Personal Information except in cases where a utilization purpose has been disclosed in advance to the public, promptly inform a Principal of, or disclose to the public, the utilization purpose. In this case, the method to "inform" is to be in writing, in principle, and as for the method to "disclose to the public," a Full Member must employ appropriate methods, such as making the relevant matters public on its website, etc. or posting or keeping the document at a counter of the head office or any other business office, etc., depending on the sales method of its financial instruments or other mode of business.
2. A Full Member must, notwithstanding the provisions of the preceding paragraph, in cases where it acquires the Principal's Personal Information stated in a written contract or other document as a result of conclusion of a contract with a Principal, state the utilization purpose explicitly to the said Principal in advance. This, however, shall not apply in cases where there is an urgent need to protect a human life, body, or property.
3. A Full Member must, in case of altering a utilization purpose, inform a Principal of, or disclose to the public, the post-altered utilization purpose.
4. The preceding three paragraphs shall not apply to any of the following cases.
   (1) Cases in which there is a possibility that informing a Principal of, or disclosing to the public, a utilization purpose would harm a Principal or third party's life, body, property, or other rights and interests
   (2) Cases in which there is a possibility that informing a Principal of, or disclosing to the public, a utilization purpose would harm the rights or legitimate interests of the Full Member
   (3) Cases in which there is a need to cooperate with a central government organization or a local government

performing affairs prescribed by laws and regulations, and when there is a possibility that informing a Principal of, or disclosing to the public, a utilization purpose would interfere with the performance of the said affairs

(4) Cases in which it can be recognized, judging from the acquisitional circumstances, that a utilization purpose is clear

Article 9. Assurance, etc. about the Accuracy of Data Contents

A Full Member must endeavor to keep Personal Data accurate and up-to-date within the necessary scope to achieve a utilization purpose by establishing procedures for collation and confirmation at the time of inputting Personal Information into a Personal Information Database, etc., establishing procedures for correction, etc. in the event of discovery of errors, etc., renewing record matters, setting a retention period, etc.

It should be noted that it is not necessary to update the Personal Data held in a single uniform way or at all times, and it is sufficient to ensure accuracy and recency within the necessary scope in accordance with the respective utilization purposes.

In addition, a Full Member must endeavor to delete Personal Data without delay when utilization of the data has become unnecessary, such as cases where the utilization purpose has been achieved and there is no longer reasonable reason to hold such Personal Data in relation to the purpose, and where the business constituting the premise for the purpose has been discontinued although the utilization purpose has not been achieved. However, this shall not apply to cases where the retention period, etc. is stipulated by laws and regulations.

Article 10. Security Control Action

1. A Full Member must take necessary and appropriate action, such as establishment of basic policies and handling rules for security control and development of a system for security control measures, for the security control of Personal Data including preventing the leakage, loss, or damage of its handled Personal Data. In addition, necessary and appropriate action must include “Institutional Security Control Measures,” “Human Security Control Measures,” and “Technological Security Control Measures” in accordance with each stage of acquisition, utilization and preservation, etc. of Personal Data. These actions shall be those corresponding to risks arising from the scale and nature of the business, the handling status of Personal Data (including the size and volume of its handled Personal Data; the same shall apply hereinafter), the nature of the medium in which Personal Data is recorded and other factors, in consideration of the significance of infringement and rights and interests that may be suffered by the Principal in the event of a leakage, loss, or damage of Personal Data.
2. The definition of terms in this article is as follows.

(1) Institutional Security Control Measures

This term means measures for system development and actions to be taken by Full Member for security control of Personal Data, such as to clearly determine the responsibility and authority of each officer and employee (meaning persons engaging in the business of a Full Member within its organization under direct or indirect control and supervision of the Full Member, not limited to employees having an employment relationship (regular employees, contract employees, fixed-term employees, part-timers, and

casual staff, etc.), but including those without an employment relationship with the Full Member (directors, accounting advisors (when an accounting advisor is a corporation, employees who are to perform the duties thereof), company auditors, executive officers, or temporary staff; the same shall apply hereinafter), establish and implement rules on security control, and inspect and audit the implementation status.

(2) Human Security Control Measures

This term means to conclude a non-disclosure contract with officers and employees and provide them with education and training, thereby supervising officers and employees so as to ensure security control of Personal Data.

(3) Technological Security Control Measures

This term means technological measures concerning security control of Personal Data, such as to limit access to Personal Data and the information system handling such data, and to monitor that information system.

3. A Full Member must take the following Institutional Security Control Measures for establishing basic policies and handling rules for security control of Personal Data.

(1) Development of rules, etc.

(a) Development of basic policies for security control of Personal Data

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

(c) Development of rules for inspection and audit of the handling status of Personal Data

(d) Development of rules for outsourcing

(2) Handling rules for safety control at each stage

(a) Handling rules at the stage of acquisition and input of data

(a) Handling rules at the stage of use and processing of data

(a) Handling rules at the stage of preservation and retention of data

(d) Handling rules at the stage of transfer and sending of data

(e) Handling rules at the stage of deletion and disposal of data

(f) Handling rules at the stage of responding to information leakage or other incidents

4. A Full Member must take the following Institutional Security Control Measures, Human Security Control Measures and Technological Security Control Measures for developing a system for security control of Personal Data.

(1) Institutional Security Control Measures

(a) Appointment of employees responsible for the management of Personal Data, etc. (a person responsible for Personal Data management who is the overall person in charge of execution of operations relating to security control of Personal Data, persons responsible for Personal Data management in each division handling Personal Data)

(b) Development of security control actions in rules of employment, etc.

(c) Operation in line with the handling rules for security control of Personal Data

(d) Development of means to check the handling status of Personal Data

(e) Development and implementation of a system for inspection and audit of the handling status of

Personal Data

(f) Development of a system for responding to information leakage or other incidents

(2) Human Security Control Measures

(a) Conclusion of a non-disclosure contract, etc. concerning Personal Data with officers and employees

(b) Clarification of roles, responsibilities, etc. of officers and employees

(c) Thorough dissemination of security control actions to officers and employees and their education and training

(d) Checking of compliance with predetermined Personal Data management procedures by officers and employees

(3) Technological Security Control Measures

(a) Identification and authentication of Personal Data users

(b) Setting of management categories of Personal Data and access control

(c) Management of authority to access Personal Data

(d) Measures to prevent the leakage, damage, etc. of Personal Data

(e) Recording and analysis of access to Personal Data

(f) Recording and analysis of operation of the information systems handling Personal Data

(g) Monitoring and audit of the information system handling Personal Data

Article 11. Supervision over Officers and Employees

1. A Full Member must, in having its officers and employees handle Personal Data, establish an appropriate internal management system and exercise necessary and appropriate supervision over the officers and employees so as to seek the security control of the Personal Data. The supervision shall correspond to risks arising from the nature of the business, the handling status of Personal Data and other factors, in consideration of the significance of infringement of rights and interests that may be suffered by the Principal in the event of a leakage, loss, or damage of Personal Data.
2. A Full Member is to exercise the "necessary and appropriate supervision" over the officers and employees in the preceding paragraph by establishing the following systems, etc.

(1) To conclude a contract, etc. upon recruiting an officer or employee to ensure that the officer or employee will not disclose to a third party any Personal Data that the person has come to know in relation to businesses operated by the Full Member or use such data for unintended purposes while being employed and after resigning from the job

(2) To clarify the roles and responsibilities of officers and employees through establishing handling rules to ensure proper handling of Personal Data, and thoroughly disseminate the obligation to ensure security control among its officers and employees and provide them with education and training

(3) To develop a system for checking compliance of its officers and employees with the matters specified in internal security control rules and inspecting and auditing their attitudes toward the protection of Personal Data in order to prevent them from taking out any Personal Data.

Article 12. Supervision over Outsourcees

1. When a Full Member outsources the partial or entire handling of Personal Data (including the entirety of outsourcing contracts, irrespective of the form or type thereof, under which a Full Member has another entity carry out the whole or part of the handling of Personal Data), the Full Member must exercise necessary and appropriate supervision over the relevant outsourcee so as to ensure security control of the outsourced Personal Data. The supervision shall correspond to risks arising from the scale and nature of the outsourced business, the handling status of Personal Data and other factors, in consideration of the significance of infringement of rights and interests that may be suffered by the Principal in the event of a leakage, loss, or damage of Personal Data.
2. A Full Member must select an entity that is found to be properly handling Personal Data as an outsourcee and secure measures for security control of Personal Data also at that outsourcee so that security control measures are taken for the outsourced Personal Data (in the case where an outsourcee further outsources personal information-related duties, the Full Member shall also supervise whether the outsourcee sufficiently supervises the sub-outsourcees). Specifically, a Full Member must make the following responses, etc. for example.
   (1) Specify the requirements to develop an organizational system and establish basic policies and handling rules for security control as the criteria for selecting outsourcees and review those criteria regularly in order to ensure the security control of the Personal Data.

   When selecting an outsourcee, it is desirable that the Full Member checks the candidate's capabilities by visiting the place where Personal Data is handled, as necessary, or by other reasonable methods and has its person responsible for the management of Personal Data make an evaluation of the candidate appropriately.

   (2) Incorporate in an outsourcing contract specific security control actions that clarify the authority on the supervision and audit of and the collection of reports from the outsourcee, prohibition of the leakage of, stealing and alteration, and the utilization of Personal Data for unintended purposes by the outsourcee, conditions concerning sub-outsourcing and the responsibility of the outsourcee in the event of information leakage, etc., and at the same time, check the outsourcee's compliance with the security control actions incorporated in the outsourcing contract, regularly or as needed, and review those measures through conducting audits regularly or taking other actions.

   It is desirable that the person responsible for Personal Data management, etc. review the security control actions incorporated in the outsourcing contract and appropriately evaluate the outsourcee's compliance therewith.

   When an outsourcee intends to outsource the relevant duties to another entity, it is desirable that the Full Member sufficiently confirms that the outsourcee appropriately supervises the sub-outsourcee of this article and that the sub-outsourcee takes security control actions based on Article 20 of the Protection Act, as in the case with the outsourcee, by such means as requesting the outsourcee to make a report on the sub-outsourcee, the content of duties to the sub-outsourced, and sub-outsourcee's method of handling Personal Data in advance and go through prior approval process or implementing regular audits by themselves or making the outsourcee do so. The same shall apply to cases of further

sub-outsourcing.

Article 13. Restriction on Third-Party Provision

1. A Full Member must not provide Personal Data to a third party (meaning those who do not fall under any of the categories of a Full Member attempting to provide the Personal Data and a Principal relating to the Personal Data, regardless of whether the party is an individual, corporation or any other organization; the same shall apply except for Articles 13-2 through 13-5) without obtaining in advance a Principal's consent. In obtaining consent, the Full Member must clearly indicate the content within a reasonable and appropriate scope that is considered necessary for the Principal to make a judgment on the consent in accordance with the scale and nature of the business, the handling status of Personal Data and other factors.

   If provision of Personal Information to a third party is assumed in advance, a Full Member must specify the fact in the utilization purpose.

   However, in any of the following cases, a Principal's consent is unnecessary in the provision of Personal Data to a third party.

   (1) Cases based on laws and regulations

   (2) Cases in which there is a need to protect a human life, body, or property, and when it is difficult to obtain a Principal's consent

   (3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a Principal's consent

   (4) Cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a Principal's consent would interfere with the performance of the said affairs

2. A Full Member, with regard to Personal Data provided to a third party (excluding Sensitive Information; the same shall apply in this paragraph) may, in cases where it is set to cease in response to a Principal's request a third-party provision of Personal Data that can identify the Principal and when it has in advance informed a Principal of those matters set forth in the following or put them into a state where a Principal can easily know, and notified them to the Personal Information Protection Commission, provide the said Personal Data to a third party notwithstanding the provisions of the preceding paragraph.

   In addition, a Full Member itself shall also disclose the content of the notification by using the Internet or other appropriate methods.

   Sensitive Information may not be provided to a third party due to an opt-out policy.

   (1) To set a third-party provision as a utilization purpose

   (2) The categories of Personal Data provided to a third party

   (3) Means or method of a third-party provision

   (4) To cease, in response to a Principal's request, a third-party provision of Personal Data that can identify the Principal

   (5) Method of receiving a Principal's request

3. A Full Member must, in case of altering those matters set forth in item (2), item (3), or item (5) of the preceding paragraph, in advance inform a Principal of the contents to be altered or put them into a state

where a Principal can easily know and notify them to the Personal Information Protection Commission.

In addition, when notifying the contents to be altered to the Personal Information Protection Commission pursuant to this paragraph, a Full Member itself shall also disclose the content.

4. In any of the following cases, a person receiving the provision of the Personal Data does not fall under a third party.
   (1) Cases in which Personal Data is provided as a result of a Full Member's outsourcing of the whole or part of the handling of the Personal Data within the necessary scope to achieve a utilization purpose.
   (2) Cases in which Personal Data is provided as a result of business succession caused by a merger or other reason (limited to cases where Personal Data is used even after the succession of the business within the scope of the utilization purpose before the Personal Data is provided due to the business succession)
   (3) Cases in which Personal Data to be jointly utilized by a specified person is provided to the specified person, and when a Principal has in advance been informed or a state has been in place where a Principal can easily know to that effect as well as of the categories of the jointly utilized Personal Data, the scope of a jointly utilizing person, the utilization purpose of the utilizing person, and the name or appellation of the person responsible for controlling the said Personal Data (meaning a person who primarily accepts and processes complaints, makes decisions on disclosure, correction, etc. and utilization cease, etc., and has responsibilities for security control in the jointly utilizing person; hereinafter referred to as the "Control Manager" in Paragraph 6)
5. Any notification given by a Full Member pursuant to the provisions of item (3) of the preceding paragraph is to be in writing in principle. With regard to a notification, etc. concerning "the scope of a jointly utilizing person," a Full Member must make efforts to list jointly utilizing persons individually.
6 A Full Member must, in case of altering a utilization purpose for a utilizing person or the name or appellation of the Control Manager set forth in Paragraph 4, item (3), in advance inform a Principal of the contents to be altered or put them into a state where a Principal can easily know.

Article 13-2. Restriction on Provision to a Third Party in a Foreign Country

A Full Member, except in those cases set forth in each item of Paragraph 1 of the preceding article, must, in case of providing Personal Data to a third party (excluding a person establishing a system conforming to standards prescribed by the Enforcement Rules as necessary for continuously taking action equivalent to the one that a Personal Information Handling Business Operator shall take concerning the handling of Personal Data; hereinafter the same shall apply in this article) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same shall apply) (excluding those prescribed in the Enforcement Rules as a country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests; hereinafter the same shall apply in this article and the next article), in advance obtain a Principal's consent to the effect that he or she approves for the provision to a third party in a foreign country. In this case, the provisions of the same article shall not apply.

Article 13-3. Keeping, etc. of a Record on a Third-Party Provision

A Full Member must, when having provided personal data to a third party (excluding a person set forth in each item of Article 2, Paragraph 5 of the Protection Act; the same shall apply in this article through Article 13-5), keep a record of the date of the Personal Data provision, the name or appellation of the third party, and other matters prescribed in the Enforcement Rules.

However, when providing Personal Data to a third party in Japan, keeping of records shall be unnecessary if the case falls under any of items (1) through (7) below.

In addition, in the provision to a third party in a foreign country, keeping of records shall be unnecessary if the case falls under any of items (1) through (4), or if the third party meets standards stipulated in the Enforcement Rules and the case falls under each item of Article 23, Paragraph 5 of the Protection Act.

(1) Cases based on laws and regulations

(2) Cases in which there is a need to protect a human life, body, or property, and when it is difficult to obtain a Principal's consent

(3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a Principal's consent

(4) Cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a Principal's consent would interfere with the performance of the said affairs

(5) Cases in which Personal Data is provided as a result of a Full Member's outsourcing of the whole or part of the handling of the Personal Data within the necessary scope to achieve a utilization purpose.

(6) Cases in which Personal Data is provided as a result of business succession caused by a merger or other reason.

(7) Cases in which Personal Data to be jointly utilized by a specified person is provided to the specified person, and when a Principal has in advance been informed or a state has been in place where a Principal can easily know to that effect as well as of the categories of the jointly utilized Personal Data, the scope of a jointly utilizing person, the utilization purpose of the utilizing person, and the name or appellation of the person responsible for controlling the said Personal Data

Article 13-4. Confirmation, etc. when Receiving a Third-Party Provision

A Full Member, when receiving the provision of Personal Data from a third party, confirm the name or appellation and address of the third party and, for a corporate body, the name of its representative (for non-corporate body having appointed a representative or administrator, the said representative or administrator), and process of acquisition of the personal information by the third party, and keep a record of matters stipulated in Article 26, Paragraph 3 of the Protection Act, except in the following cases.

However, the confirmation and record-keeping obligations shall not apply to any case that is not a provision by a "provider" substantially.

(1) Cases based on laws and regulations

(2) Cases in which there is a need to protect a human life, body, or property, and when it is difficult to obtain a Principal's consent

(3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a Principal's consent

(4) Cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a Principal's consent would interfere with the performance of the said affairs

(5) Cases in which Personal Data is provided as a result of a Full Member's outsourcing of the whole or part of the handling of the Personal Data within the necessary scope to achieve a utilization purpose.

(6) Cases in which Personal Data is provided as a result of business succession caused by a merger or other reason.

(7) Cases in which Personal Data to be jointly utilized by a specified person is provided to the specified person, and when a Principal has in advance been informed or a state has been in place where a Principal can easily know to that effect as well as of the categories of the jointly utilized Personal Data, the scope of a jointly utilizing person, the utilization purpose of the utilizing person, and the name or appellation of the person responsible for controlling the said Personal Data

Article 13-5. Retention Period for Keeping Records upon Third-Party Provision

Records made in accordance with Article 13-3 and Article 13-4 must be kept for the period specified in the Enforcement Rules from the date of creating these records.

Article 14. Public Disclosure, etc. on Matters Relating to Retained Personal Data

1. A Full Member must, concerning its Retained Personal Data, put the following matters into a state where a Principal can know (including those cases in which it, at the request of a Principal, responds without delay). When the utilization purpose includes provision of information to a third party, the fact must be clearly stated as the content in Item (2).

(1) Appellation of the Full Member

(2) Utilization purpose of all Retained Personal Data (excluding those cases falling under Article 8, Paragraph 4, Item (1) through Item (3))

(3) Procedures for responding to a request pursuant to the provisions of Paragraph 1 of the succeeding paragraph or a demand pursuant to the provisions of Article 15, Paragraph 1, Article 16, Paragraph 1, or Article 17, Paragraph 1 or Paragraph 2 (including the amount of a fee when it is prescribed pursuant to the provisions of Article 20)

(4) In-house contact point to which a complaint is to be filed in regard to handling of Retained Personal Data

(5) Appellation of the accredited personal information protection organization and contact point to which resolution of its complaint is to be filed

2. A Full Member must, when requested by a Principal to get informed of a utilization purpose of Retained Personal Data that can identify the Principal, inform the said Principal thereof without delay. This, however, shall not apply in those cases falling under any of the following items.

(1) Cases in which the utilization purpose of Retained Personal Data that can identify the said Principal is clear pursuant to the provisions of the preceding paragraph

(2) Cases falling under Article 8, Paragraph 4, Items (1) through Item (3)

3. A Full Member must, when having been requested based on the provisions of the preceding paragraph but deciding not to inform a Principal of the utilization purpose of Retained Personal Data, inform the Principal to that effect without delay.

Article 15. Disclosure

1. A Full Member must, when having received a demand of disclosing Retained Personal Data that can identify a Principal (when such data does not exist, including informing a Principal thereof) from the Principal, disclose the Retained Personal Data to the Principal without delay by means of issuing a document (when there is a method agreed by the person demanding the disclosure, that method). However, in cases where disclosing such data falls under any of the following cases, the whole or part thereof may not be disclosed.
   (1) Cases in which there is a possibility of harming a Principal or third party's life, body, property, or other rights and interests
   (2) Cases in which there is a possibility of interfering security with the said Full Member implementing its business properly
   (3) Cases of violating other laws or regulations
2. A Full Member must, when having decided not to disclose the whole or part of Retained Personal Data in connection with a demand pursuant to the provisions of the preceding paragraph or when the Retained Personal Data does not exist, inform a Principal thereof without delay. The reasons for the decision shall be explained by showing the provisions of the law supporting the decision and facts that are the basis of the decision.

Article 16. Correction, etc.

1. In case of having received a demand made by a Principal for making a correction, addition, or deletion (hereinafter referred to as a "Correction, etc.") of the contents of Retained Personal Data that can identify the Principal by reason that the data are neither correct nor factual, a Full Member must conduct a necessary investigation, such as confirmation of facts, without delay to the extent necessary to achieve a utilization purpose and, based on the result thereof, make a Correction, etc. of the contents of the Retained Personal Data in principle.
2. A Full Member must, when having made a Correction, etc. on the whole or part of the contents of the Retained Personal Data in connection with a demand specified in the preceding paragraph or when having made a decision not to make a Correction, etc., inform a Principal without delay to that effect (including, when having made a Correction, etc., the contents thereof). If a Full Member does not make a Correction, etc., the Full Member is to explain the reasons by presenting grounds for the decision not to make a Correction, etc. and facts supporting the decision.

Article 17. Utilization Cease, etc.

1. In case of having received a demand made by a Principal for a utilization use or deletion (hereinafter referred to as a "Utilization Cease, etc.") of Retained Personal Data that can identify the Principal by reason that the

Retained Personal Data has been handled in violation of the provisions of Article 5 or has been acquired in violation of the provisions of Article 7 and when it has become clear that there is a reason in the demand, a Full Member must fulfill a Utilization Cease, etc. of the said Retained Personal Data to the extent necessary to redress a violation without delay. This, however, shall not apply in case where a Utilization Cease, etc. of the said Retained Personal Data requires a large expense or other cases where it is difficult to fulfill a Utilization Cease, etc. and when necessary alternative action is taken to protect a Principal's rights and interests.

2. In case of having received a demand made by a Principal for ceasing a third-party provision of Retained Personal Data that can identify the Principal by reason that the Retained Personal Data are being provided to a third party in violation of the provisions of Article 13, Paragraph 1 and when it has become clear that there is a reason in the demand, a Full Member must cease the third-party provision of the Retained Personal Data without delay in principle. This, however, shall not apply in cases where ceasing the third-party provision of the said Retained Personal Data requires a large expense or other cases where it is difficult to cease the third-party provision and when necessary alternative action is taken to protect a Principal's rights and interests.
3. A Full Member must, when having fulfilled a utilization cease etc. or decided not to fulfill a Utilization Cease, etc. of the whole or part of Retained Personal Data in connection with a demand pursuant to the provisions of Paragraph 1, or when having ceased a third-party provision or decided not to cease a third party provision of the whole of Retained Personal Data in connection with a demand pursuant to the provisions of the preceding paragraph, inform a Principal to that effect (including, when taking a measure that is different from the action requested by the Principal, the contents of the measure) without delay.

Article 18. Explanation of Reason

In case of informing a Principal to the effect that, as regards the whole or part of action requested or demanded by the Principal pursuant to the provisions of Article 14, Paragraph 3, Article 15, Paragraph 2, Article 16, Paragraph 2, and Paragraph 3 of the preceding article, the action will not be taken, or to the effect that different action from the said action will be taken, when explaining a reason therefor to the said Principal, a Full Member is to present grounds for the decision not to take the action or to take a different action and facts supporting the decision.

Article 19. Procedures for Responding to Demand, etc. for Disclosure, etc.

1. A Full Member may, as regards a request pursuant to the provisions of Article 14, Paragraph 2 or a demand pursuant to the provisions of Article 15, Paragraph 1, Article 16, Paragraph 1, Article 17, Paragraph 1 or Paragraph 2 (hereinafter referred to as a "Demand, etc. for Disclosure, etc."), decide on a method of receiving a request or demand. In this case, a Full Member is to regularly post that method on its website together with the Pronouncement Concerning Protection of Personal Information as specified in Article 23, or regularly posting or keeping it at a business office counter, etc.
   (1) Contact point to which a Demand, etc. for Disclosure, etc. is to be made
   (2) Form of documents to be submitted at the time of a Demand, etc. for Disclosure, etc. and other methods

of receiving Demand, etc. for Disclosure, etc.

(3) Method of confirming that a person who makes a Demand, etc. for Disclosure, etc. is the Principal or a representative (meaning a legal representative for a minor or adult ward, or a representative entrusted by the Principal; the same shall apply in this article)

(4) Amount of the fee in Article 33, Paragraph 1 of the Protection Act and method for collection thereof (including the case where such a demand, etc. is free of charge)

(5) Matters necessary to identify Retained Personal Data that are subject to a Demand, etc. for Disclosure, etc.

(6) Method of replying to a Demand, etc. for Disclosure, etc.

2. A Full Member shall decide on the following matters in addition to each item of the preceding paragraph as the procedures for cases where a representative makes a Demand, etc. for Disclosure, etc. A Full Member shall not be precluded from disclosing the relevant personal data directly only to the Principal in response to a Demand, etc. for Disclosure, etc. made by a representative.

(1) Method for identity verification of a representative

(2) Method to confirm a representative's authority of representation

3. A Full Member must, in establishing a procedure for Demand, etc. for Disclosure, etc. based on the provisions of the preceding two paragraphs, give consideration so as not to impose excessive burden on a Principal.

Article 20. Fees

1. A Full Member may, when having been requested to inform of a utilization purpose pursuant to the provisions of Article 14, Paragraph 2 or when having received a demand for disclosure pursuant to the provisions of Article 15, Paragraph 1, collect a fee in relation to taking such action.
2. A Full Member must, in case of collecting a fee pursuant to the provisions of the preceding paragraph, decide on the amount of the fee within a range recognized as reasonable considering actual expenses.

Article 21. A Full Member's Dealing with a Complaint

1. A Full Member must strive to deal appropriately and promptly with a complaint about the handling of Personal Information.
2. A Full Member must strive to establish the system necessary to achieve a purpose under the preceding paragraph through setup of a contact point for receiving complaints, formulation of procedures for dealing with complaints, provision of sufficient education and training to officers and employees engaging in dealing with complaints, and other means.

Article 22. Response to Personal Information Leakage or Other Incidents

1. In the event of the leakage of any Personal Information or the leakage of information concerning descriptions, etc. and Personal Identification Codes deleted from Personal Information used to produce Anonymously Processed Information and information relating to a processing method carried out pursuant to the provisions of Article 36, Paragraph 1 of the Protection Act (hereinafter referred to as "Personal Information Leakage or

Other Incidents"), a Full Member is to immediately report that incident to the Financial Services Agency and the Association. If, in addition to Personal Information Leakage or Other Incidents, leakage of specific personal information specified in Article 2, Paragraph 8 of the Act on the Uses of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 27 of 2013) occurs, a Full Member shall also report the incident to the Personal Information Protection Commission.

2. In the event of any of Personal Information Leakage or Other Incidents, a Full Member is to disclose the facts concerning the incident and preventive measures to the public without delay from the perspective of preventing secondary damage or the occurrence of any similar incidents.
3. In the event of any of Personal Information Leakage or Other Incidents, a Full Member is to promptly inform the Principal involved in the relevant incident of the facts concerning the incident.

Article 23. Formulation of the Pronouncement Concerning Protection of Personal Information

1. In consideration of the significance of explaining policies related to Personal Information in advance in an easy-to-understand manner, a Full Member is to formulate the pronouncement concerning its ideas and policies concerning protection of Personal Information (so-called privacy policy or privacy statement, etc.; hereinafter referred to as the "Pronouncement Concerning Protection of Personal Information") and disclose it to the public.
2. For example, the Pronouncement Concerning Protection of Personal Information is to include the following matters.
   (1) Pronouncement of policies concerning protection of Personal Information, such as the compliance with related laws and regulations, etc., prohibition of utilization of Personal Information for unintended purposes and proper processing of complaints
   (2) Simple explanation of procedures for notification and public disclosure of the utilization purposes of personal information under Article 18 of the Protection Act
   (3) Simple explanation of procedures for disclosure, etc. under Article 27 of the Protection Act or other various procedures for handling of Personal Information
   (4) Contact information on offices processing inquiries and complaints concerning handling of Personal Information
3. A Full Member shall strive to incorporate as many descriptions as possible in consideration of the following points, depending on the characteristics, scale, and actual status of business activities, from the perspective of protecting rights and interests of a Principal, including general consumers, in the Pronouncement Concerning Protection of Personal Information.
   (1) When a Principal makes a request, a Full Member is to suspend sending of direct email or otherwise voluntarily cease the utilization of the Retained Personal Data.
   (2) A Full Member is to endeavor to increase transparency regarding outsourcing, such as clarifying whether it outsources any business or the content of outsourced business if any.
   (3) A Full Member is to devise means to clarify utilization purposes for the respective Principal, through efforts such as presenting limited utilization purposes separately by the type of customers in consideration of the business contents or voluntarily endeavoring to limit utilization purposes based on

each choice by a Principal.

(4) A Full Member is to indicate sources and methods of acquiring Personal Information (types of information sources, etc.) as concretely as possible.

Article 24. Review of the Guidelines

The Guidelines shall be reviewed as necessary.

Article 25. Report to the Association, etc.

1. The Association may request a Full Member to make a report where appropriate to confirm the Full Member's compliance with the Guidelines.
2. The Association shall provide guidance and recommendations and take other measures necessary to have Full Members comply with the Guidelines.
3. A Full Member must comply with the Guidelines and follow necessary guidance and recommendations provided, and other measures taken by the Association.

Supplementary Provision

The Guidelines shall come into force on April 1, 2005.

Supplementary Provision

This amendment shall come into force on 30 September 2007.

Supplementary Provision

This amendment shall come into force on March 21, 2008.

Supplementary Provision

This amendment shall come into force on March 19, 2009.

Supplementary Provision

This amendment shall come into force on December 17, 2009.

Supplementary Provision

This amendment shall come into force on January 4, 2013.

Supplementary Provision

This amendment shall come into force on October 15, 2015.

* The amended provisions, etc. are as follows:

- Amendment of Articles

Articles 1 through 3, Article 7, Articles 10 through 12, Article 22

- Revision of explanations

  Articles 1 through 3, Articles 5 through 10, Article 12, Article 13, Article 15, Article 19, Article 22, Article 23

- Revision of reference provisions

  Articles 1 through 3, Article 5, Article 7, Articles 9 through 13, Article 16

Supplementary Provision

This amendment shall come into force on February 18, 2016.

* The amended provisions, etc. are as follows:

  - Explanation and reference provisions of Article 7
  - Article 22, Paragraph 1 and explanation

Supplementary Provision

This amendment shall come into force on 30 May, 2017.

* The amended provisions, etc. are as follows:

  - Amendment of provisions, etc.

    Articles 1 through 23 and 25 have been amended and Articles 13-2 through 13-5 have been newly added.

  - Amendment of explanation and reference provisions, etc.

    The explanation and reference provisions for each provision have been transferred to the newly established “Explanation on the Guidelines for Protection of Personal Information,” and deleted. The explanation and reference provisions have also been amended in accordance with the amended provisions.

Supplementary Provision

This amendment shall come into force on July 15, 2021.

* The amended provisions, etc. are as follows:

  - Article 1.
  - Amendment of explanation and reference provisions, etc.

    Articles 2 through 4, 7, 8, 10, 13, 13-2, and 23 have been amended.

    Supplementary provisions are newly added.