Procedural Guidelines on the Protection of Personal Information

March 23, 2005
Resolution of the Board of Directors
(Partially amended on October 24, 2007
Partially amended on February 24, 2010
Partially amended on September 16, 2015
Partially amended on December 16, 2015
Partially amended on May 24, 2017)

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(Purpose) Article 1 These Procedural Guidelines define concrete measures members shall take to ensure an appropriate handling of personal information in the investment management business or the investment advisory and agency business based on the Act on the Protection of Personal Information (hereinafter referred to as the "Protection Act"), Cabinet Order to Enforce the Act on the Protection of Personal Information (hereinafter referred to as the "Cabinet Order"), Enforcement Rules for the Act on the Protection of Personal Information (hereinafter referred to as the "Enforcement Rules"), Basic Policy on the Protection of Personal Information (hereinafter referred to as the "Basic Policy"), Guidelines on the Act on the Protection of Personal Information (Volume on General Rules)(hereinafter referred to as the "General Rules Guidelines"), other volumes of the Guidelines on the Act on the Protection of Personal Information, namely the Volume on Provision to a Third Party in a Foreign Country, the Volume on Confirmation and Record-keeping Obligations upon Third-Party Provision, and the Volume on Anonymously Processed Information, Guidelines for Protection of Personal Information in the Finance Sector (hereinafter referred to as the "Financial Sector Guidelines"), and the Operational Instructions on the Security Control Measures Based on the Guidelines for Protection of Personal Information in the Finance Sector.	When handling personal information in other businesses than the investment management business or investment advisory and agency business performed by members, guidelines on the protection of personal information set out by relevant accredited personal information protection organizations, etc. shall be complied with; in cases where no applicable guidelines, etc. are available, members shall ensure the proper handling of personal information in accordance with the objectives of these Procedural Guidelines. (Note) These Procedural Guidelines are not applicable to the following types of personal information: Personal information held for administrative purposes (including information on the employment of officers and employees by members and information on recruitment, wage, appraisal, and health examination) and personal information of members' shareholders.	Articles 1 and 53 of the Protection Act Article 1 of the Financial Sector Guidelines
(Definitions) Article 2 In these Procedural Guidelines, the definition of terms listed under the following items shall be as prescribed in those items: (i) Personal information Information about a living individual which can identify the specific individual (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual) or information containing an individual identification code. The term "information about an individual" refers not only to information that identifies a specific individual such as name, address, gender, date of birth or image of the face but also to any and all information that indicates a fact, judgement or evaluation concerning the bodily features, assets, type of business, title or other attributes of an individual, including evaluation information and information made public by public literature, etc. as well as information in the form of image or sound, whether protected by way of encryption or otherwise. The term "individual identification code" refers to characters, numbers, symbols, or other codes specified in Article 1 of the Cabinet Order as sufficient by itself to identify a specific individual. The "information about an individual" is regarded as "personal information" if it can identify a specific individual by being jointly used with name or other pieces of information. If a piece of information about a deceased individual is also information about a bereaved family or other living individual, the piece of information shall be regarded as information about the living individual. Company names and other types of information about corporations and other organizations do not fall under the category of personal information in principle; provided, however, that if the information contains officers' names and other information about individuals, such portions shall be regarded as personal information.	Unless otherwise specified, the terms used in these Procedural Guidelines shall have the same meaning as those used in the "General Rules Guidelines," etc. An example case where information can be readily collated with other information: A situation in which a person can, in ordinary course of his/her business, access a personal information database, etc. to collate the information; Cases that do not fall under the provision include situations in which the collation is difficult to perform as an inquiry to other business operators is required or the other information is held by a different department within the member's organization.	Article 2, paragraphs (1) and (2) of the Protection Act Article 1 of the Cabinet Order Articles 2 through 4 of the Enforcement Rules 2-1 and 2-2 of the General Rules Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
Furthermore, the term “individual(s)” shall also refer to foreigners. (ii) Personal information database, etc. Those set forth in the following which are a collective body of information comprising personal information (excluding those prescribed as having little possibility of harming an individual's rights and interests considering their utilization method): (a) Those systematically organized so as to be able to search for particular personal information using a computer; (b) Besides those set forth in (a), those to which a fixed set of rules is applied to arrange the personal information contained therein so that they are structurally organized to enable personal information to be easily retrieved from them, and which have a table of contents, an index, or anything else that aids in retrieval;	(1) Examples that fall under the definition of “personal information database, etc.” The following are the examples that fall under the definition: a. A database that is created by employees by inputting and organizing business card data on a business-use personal computer (regardless of owner) using spreadsheet software (item (ii) (a)); b. Customer management materials, etc. indexed and arranged in the order of the Japanese syllabary without using a computer (item (2) (b)). (2) Examples that do not fall under the definition of “personal information database, etc.” a. Business cards that are held in a business card box, etc. without being sorted; b. Questionnaire response cards that are left without being sorted by name, address, etc.; and c. Directory, corporate information, or other commercially available data, etc. that are kept intact and unprocessed.	Article 2, paragraph (4) of the Protection Act Article 3 of the Cabinet Order 2-4 of the General Rules Guidelines
(iii) Personal data Personal data means personal information constituting a personal information database, etc.	(1) Examples that fall under the definition of “personal data” The following are the examples that fall under the definition: a. Personal information downloaded from a personal information database, etc. to a recording medium; b. A hard copy output from a personal information database, etc. (or a photocopy thereof); c. Personal information constituting a personal information database that is not yet converted into an electronic format and held in a paper format such as a contract form, customer management material, etc., but is kept in a retrievable form by being arranged in the order of the Japanese syllabary, customer number, etc. (and therefore falls under the definition of “personal information database, etc.”); d. Personal information constituting a personal information database that omits name or other values so as not to allow a third party to identify specific individuals, but allows a member to identify specific personal information by collating with other information and is arranged in a format that allows users to readily retrieve specific personal information (and therefore falls under the definition of “personal information database, etc.”) (2) Examples that do not fall under the definition of “personal data” Personal information contained in a paper-based contract form, customer management material, etc., that is not yet converted into an electronic format and not kept in a retrievable form by being arranged in the order of the Japanese syllabary, customer number, etc. (and	Article 2, paragraph (6) of the Protection Act 2-6 of the General Rules Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
	therefore do not fall under the definition of “personal information database, etc.”).	
(iv) Personal data held by a member Personal data over which a member has the authority to, in response to a request from a principal or his/her agent, disclose, correct, add or delete the content, discontinue its utilization, erase, and discontinue its provision to a third party, excluding the data listed in the following:	(1) Examples that fall under the definition of “personal data held by a member” The following are the examples that fall under the definition: a. Personal information constituting a personal information database, etc. created and processed by a company (the company's database on its customers, etc., or documents and books concerning customers); b. If a member retains third-party company data, etc. in combination with its in-house data, the member is considered to have the authority to correct a database created and retained through such combination, and therefore the database falls under the definition of “personal data held.” (2) Examples that do not fall under the definition of “personal data held” For example, if a member acquires a database from another company, the database does not fall under the definition as the member does not have the authority to disclose the that do not have the authority over the database for disclose, etc. (In order to define personal data as “personal data held,” a member must have authority over the data to disclose, correct, add or delete, discontinue its utilization, erase, and discontinue its provision to a third party.)	Article 2, paragraph (7) of the Protection Act Articles 4 and 5 of the Cabinet Order 2-7 of the General Rules Guidelines
(a) Any personal data whose known presence or absence of a database is likely to threaten the life, body, or property of the identifiable person; (b) Those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would encourage or induce an illegal or unjust act;	Specific examples of item (iv) (b) a. Information on suspicious individuals, complainers, and corporate racketeers b. Information on antisocial forces such as organized crime groups	
(c) Any personal data whose known presence or absence of a database is likely to undermine national security, damage a relationship of confidence with a foreign country or international organization, or put the country at a disadvantage in negotiations with another country or with an international organization;	Specific examples of item (iv) (c) Information on VIPs’ schedule	
(d) Any personal data whose known presence or absence of a database is likely to interfere with crime prevention, crime control, or criminal investigations or with otherwise upholding public safety and order;	Specific examples of item (iv) (d) a. Information with regard to which a member received an inquiry from the police in the course of its investigations b. Information subject to the reporting of transactions suspected to be related to criminal proceeds (suspicious transactions)	
(e) Information that will be deleted within six months.		

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(v) Principal A principal means a specific individual identifiable by personal information.		Article 2, paragraph (8) of the Protection Act
(vi) Special care-required personal information Special care-required personal information means personal information of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.		Article 2, paragraph (3) of the Protection Act Article 2 of the Cabinet Order Article 5 of the Enforcement Rules 2-3 of the General Rules Guidelines
(vii) Anonymously processed information Information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each following item in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information.		Article 2, paragraph (9) of the Protection Act 2-8 of the General Rules Guidelines
(Specifying a Utilization Purpose) Article 3 (1) A member shall, in handling personal information, specify the purpose of utilizing the personal information as explicitly as possible, so as to enable the principal to reasonably expect how and for what purposes his/her personal information will be used in the business.	(1) Specific examples of the details of business a. Investment advisory business (investment advisory service) b. Business pertaining to discretionary investment contracts (2) Specific examples of the purpose of use The purpose of use shall be described specifically in a manner as follows, for example: a. To carry out administrative processes pertaining to investment advisory contracts (advisory services) or discretionary investment contracts with customers; b. To provide investment advisory services; c. To report investment results, balance of contract assets, etc. to customers; d. To make necessary contacts with customers, etc. and thereby provide services in an appropriate and smooth manner. Ambiguous expressions such as “for purposes necessary for the company,” “to use in our business activities,” or “to improve our service levels” do not meet the requirement for being “as explicitly as possible.”	Article 15, paragraph (1) of the Protection Act Article 2 of the Financial Sector Guidelines 3-1-1 of the General Rules Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(2) A member must, in case of altering a utilization purpose, not do so beyond the scope recognized reasonably relevant to the pre-altered utilization purpose.	(Example of acceptable alteration) From “to send product information, etc. by mail” to “to send product information, etc. via e-mail” (Example of unacceptable alteration) From “to use for the analysis of questionnaires” to “to use for the mailing of product information, etc.”	Article 15, paragraph (2) of the Protection Act 3-1-2 of the General Rules Guidelines
(3) When utilization purposes of specific personal information are limited by laws and regulations, a member shall state such effect explicitly.		Article 2, paragraph (2) of the Financial Sector Guidelines
(Restriction due to a Utilization Purpose) Article 4 (1) A member shall not handle personal information without obtaining in advance a principal’s consent beyond the necessary scope to achieve a utilization purpose specified pursuant to the provisions under the paragraph (1) of the preceding Article; provided, however, that using personal information to obtain a principal’s consent in advance does not fall under the category of unintended use, even if such use is not included in the initially specified use purposes.	A “principal’s consent” means the principal’s declaration of intent in which he/she agrees that his/her personal information is handled according to the method presented by the member (under the assumption that the person is already confirmed to be the principal concerned).	Article 16, paragraph (1) of the Protection Act 3-1-3 of the General Rules Guidelines
(2) A member shall, in case of having acquired personal information accompanied with succeeding a business from another personal information handling business operator, etc. 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; provided, however, that using personal information to obtain a principal’s consent in advance does not fall under the category of unintended use, even if such use is not included in the use purposes specified before the succession.		Article 16, paragraph (2) of the Protection Act 3-1-4 of the General Rules Guidelines
(3) The provisions under the preceding two paragraphs shall not apply to those cases set forth in the following: (i) Cases based on laws and regulations;	The following are the examples that fall under the definition: a. Article 56-2 (Collection of Reports and Inspections) of the Financial Instruments and Exchange Act b. Articles 210, 211, etc. (Investigation of Criminal Cases by Officials of Securities and Exchange Surveillance Commission) of the Financial Instruments and Exchange Act c. Article 8, paragraph (1) (“Reporting of Suspicious Transactions”) of the Act on Prevention of Transfer of Criminal Proceeds (hereinafter referred to as “Criminal Proceeds Transfer Prevention Act”) d. Articles 74-2 to 74-6 (“Right of Inquiries and Inspection of Tax Authority Officials”) of the Act on General Rules for National Taxes e. Article 1, etc. (Inspection of Criminal Cases by Tax Collectors or Voluntary Investigations of Criminal Cases by Tax Collectors or Local Tax Officials) of the National Tax Violations Control Act f. Article 72-63 (Right of Inquiries and Inspection Concerning Enterprise Tax of	Article 16, paragraph (3) of the Protection Act Article 4 of the Financial Sector Guidelines 3-1-5 of the General Rules Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
	Personnel of the Ministry of Internal Affairs and Communications) of the Local Tax Act g. Article 141 (Inquiries and Inspections) of the National Tax Collection Act h. Article 197 (Report on Particulars Relating to Investigations) of the Code of Criminal Procedure i. Article 218, paragraph (1) ("Seizure, Search, and Inspection upon Warrant") of the Code of Criminal Procedure j. Article 223 (Order to Submit Documents) of the Code of Civil Procedure k. Article 23-2, paragraph (2) (Request for Information) of the Attorney Act In the case where there are legal provisions to the effect that a third party may request the provision of personal information but that such request may be rejected for justifiable grounds, a member shall pay attention to making a response within the scope wherein the necessity and reasonableness of the information utilization for unintended purposes can be found in light of the purport of the relevant laws and regulations.	
(ii) Cases in which there is a need to protect a human life, body or fortune (including fortune of a juridical person), and when it is difficult to obtain a principal's consent;	The following are the examples that fall under the definition: a. When collecting information concerning illegal activities by antisocial groups including so-called corporate racketeers or organized crime groups, or their members, etc.; b. When providing family members' contact information, etc. to a medical institution to deal with sudden illnesses of a customer, etc.; c. Disclosure of the details of a contract, etc. to relatives of a principal in the event that the principal continues to be missing due to an earthquake, disaster, etc.; and d. When enterprises share information on antisocial forces such as organized crime groups and malicious persons who obstruct business operations.	
(iii) 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; and		
(iv) Cases in which there is a need to cooperate in regard to 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.	The following are the examples that fall under the definition: a. When responding to a voluntary investigation by tax authorities; b. When responding to a voluntary investigation by the police; and c. When responding to a general statistical survey. A member is to give consideration to making a response within the scope wherein the necessity and reasonableness of the utilization of the information for unintended purposes can be found in light of the purport of the relevant non-mandatory request.	
(Format of "Consent") Article 5 When obtaining the consent of the principal as specified in Articles 4, 13 and 13-2 hereof, a member shall do so in writing (including an electronic or magnetic record; the same applies hereinafter).	(1) Specific examples of methods to obtain "consent" The following are the examples of possible methods: a. The method to obtain consent from the principal by describing the utilization purposes on a	Article 3 of the Financial Sector Guidelines 2-12 of the General Rules

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
If the principal is a minor, adult ward, person under curatorship, or person under assistance, and has no ability to understand the consequence of the consent to the handling of personal information, it is necessary to obtain consent of a person who has parental authority or a statutory agent, etc.	document prepared to acquire personal information directly from the principal and by providing a check box (check column) in the document so that the principal can indicate his/her consent therein; and requesting the person's signature (or seal). b. The method to request a principal to manifest his/her consent (by clicking a consent button) on the Internet screen, etc., or to receive, from a principal, an e-mail, etc. that includes the principal's statement of consent. When the consent is obtained verbally using a non-face-to-face communication method (such as telephone) other than those described under a. and b. above, it is desirable to set up a system that provides an ex-post-facto verification capability, including the recording of customers' manifestation of consent. (2) Points to be noted when using pre-prepared consent forms It is desirable that the terms concerning the handling of personal information are indicated in a manner clearly distinguishable from other terms by such means as using larger fonts and different expressions so that the content thereof is explicitly understood by a person in question. Otherwise, it is desirable to confirm the principal's intent using a method in which his/her intention is clearly expressed, an example of which is preparing a check box in a pre-prepared consent form that the principal can fill in.	Guidelines
(Sensitive Information) Article 6 (1) A members is not to acquire, use or provide to a third party any personal information requiring special care and information on 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 personal information requiring special care) (excluding any information made public by the person in question themselves 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, and seemingly-clear information acquired by visual observation, filming or photographing of the person in question; hereinafter referred to as "sensitive information"), except for the following cases: (i) Cases in which the provision of personal information is based on laws and regulations	Publicly-known information provided in official gazettes or newspapers or reported on television, etc. does not fall under the sensitive information category. (Points of Attention) When a member receives from a customer a copy of driver's license, etc. bearing his/her registered domicile as a customer identification document, etc., on or after April 1, 2005, and if the registered domicile is blacked out immediately before the copy is filed (stored), it is not deemed as an "acquisition" of sensitive information. Attention shall be paid that, after April 1, 2005, a member may not use or provide to a third party any sensitive information (those that do not fall under any of items (i) to (v)) acquired before that day. Specific examples of "cases in which the provision of personal information is based on laws and regulations" Cases in which personal information is provided based on laws, Ministerial Orders, ordinances, treaties, cabinet decisions, and official documents issued by public agencies; for example, when a member receives information on antisocial behavior conducted by organized crime groups, antisocial groups, or their members described in documents, etc. at a meeting, etc. of the "Center for Removal of Criminal Organizations" based on the "Act on Prevention of Unjust Acts by Organized Crime Group Members".	Article 5, paragraph (1) of the Financial Sector Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(ii) Cases in which the provision of personal information is necessary for the protection of people's lives, bodies or property;	Specific examples of "cases in which the provision of personal information is necessary for the protection of people's lives, bodies or property" Cases in which a member acquires criminal information for the purpose of identifying antisocial groups (such as so-called corporate racketeers or organized crime groups) or their members;	
(iii) Cases in which the provision of personal information is especially necessary for the improvement of public hygiene and the promotion of the sound growth of children;		
(iv) Cases in which there is a need to offer cooperation to a national government organ, local public entity, or a person entrusted thereby in their performance of affairs prescribed in laws and regulations; and		
(v) Cases in which a member acquires, uses, or provides to a third party any sensitive information based on the consent of the principal to the extent necessary for performing its services from the necessity to ensure appropriate operation of its investment management business or investment advisory and agency business;		
(2) When a member acquires, uses, or provides to a third party any sensitive information in the cases set forth in the preceding paragraph, the member is to 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.		Article 5, paragraph (2) of the Financial Sector Guidelines
(3) When a member acquires, uses, or provides to a third party any sensitive information in the cases set forth in paragraph (1), the member must make a response appropriately in accordance with laws and regulations, etc. concerning the protection of personal information, such as the legal requirement to obtain the consent of the principal in advance upon obtaining personal information requiring special care pursuant to the provisions of Article 17, paragraph (2) of the Protection Act.		Article 5, paragraph (3) of the Financial Sector Guidelines
(4) Article 23, paragraph (2) of the Protection Act (opt-out provision) is not to be applied in the case where a member provides sensitive information to a third party.		Article 5, paragraph (4) of the Financial Sector Guidelines
(Proper Acquisition) Article 7 (1) A member must not acquire personal information by deceit or other improper means. When acquiring personal information from a third party, a member must neither unreasonably infringe the interest of the principal nor acquire personal information from a third party who commits unjust acts such as illegal acquisition of personal information, knowing that the information is leaked information.	Examples of cases falling under the definition of "improper means" The following are the examples that fall under the definition: a. When acquiring personal information from the principal while concealing or falsifying the purpose of collecting personal information; b. When acquiring personal information by forcing a violation of the restriction on third party provision stipulated in Article 23 of the Protection Act; and c. When instructing another business operator to acquire personal information by deceit means and acquiring personal information from that business operator.	Article 17, paragraph (1) of the Protection Act 3-2-1 of the General Rules Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(2) When acquiring any personal information provided by a third party, a member must check the status of regulatory compliance of the information provider and confirm that such personal information has been lawfully acquired.	(1) Specific methods to check the status of regulatory compliance of the provider For example, a member may check whether the provider discloses its opt-out policy, utilization purposes, disclosure procedures, and contact for inquiries and complaints. (2) A member may confirm that the provided personal information was lawfully acquired by using, for example, any one of the following methods: a. Inspection of contracts or other documents showing the process of acquisition; b. Acceptance of a confirmation letter stating that the information was legitimately acquired; and c. Verbal confirmation of legitimacy and keeping of appropriate internal records. If a member may not confirm that the personal information provided is acquired legitimately, it is desirable to consider careful measures, including refraining from acquiring the information.	
(Notification, Announcement, and Explicit Statement of a Utilization Purpose when Acquiring) Article 8 (1) A member shall, 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 such case, the "notice" shall, in principle, be made in writing, and the "publication" shall be made in a proper way depending on the way in which the business is conducted, including the manner of solicitation activities.	(1) The term "notification" refers to informing a principal directly. In principle, a "notification" is to be given in writing. The following are the examples of possible methods: a. Delivering documents by hand; b. Sending e-mails and facsimiles; and c. Sending documents by mail (2) The term "publication" refers to informing an unspecified number of people. The following are the examples of possible methods: a. Posting and keeping documents, etc.; b. Describing in, and delivery of, pamphlets; c. Posting on the website; d. Posting posters, etc. at sales offices, etc. (Note) The provisions under Article 18 of the Protection Act do not apply to any personal information that has been retained since before the enforcement of the Act as no acts of acquisition were performed at the time of enforcement.	Article 17, paragraph (1) of the Protection Act 2-10 and 2-11 of the General Rules Guidelines
(2) Notwithstanding the provisions of the preceding paragraph, a member shall, in cases where it acquires, as a consequence of concluding a contract with a principal, the principal's personal information stated in a written contract or other document, explicitly state the utilization purposes in advance to the principal. This, however, shall not apply in cases where there is an urgent need to protect a human life, body, or fortune.	(1) Example cases where information is acquired in a written form directly from the principal The following are example cases: a. When receiving, from the principal, a document associated with an investment advisory contract or a discretionary investment contract; b. When acquiring personal information described in a reply card or questionnaire form directly from the principal; When a member concludes a contract with a corporation and receives a contract form or other documents containing personal information of the corporation's representative, it shall be deemed that the member "acquires the principal's personal information stated in a written contract or other document."	Article 18, paragraph 2 of the Protection Act, 3-2-3 and 3-2-4 of the General Rules Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
	(2) Specific methods to "state explicitly" The following are the examples of possible methods: a. Using a document describing utilization purposes; b. Describing utilization purposes on the contract form, etc. when concluding a contract; c. Stating utilization purposes explicitly by posting posters, etc.; d. Stating utilization purposes explicitly by distributing pamphlets, leaflets, etc.; and e. In the case of online transactions, using a screen to be filled by, or an e-mail to be sent to, customers. (3) Matters, etc. to be stated explicitly a. The matters to be stated explicitly are the purposes of utilizing personal information acquired. The explicit statement shall be made either by stating only the personal information utilization purposes described in the document or by stating all or part of the comprehensive utilization purposes specified in accordance with Article 3. b. When the comprehensive utilization purposes were stated explicitly at the time of concluding a contract, etc., and the personal information utilization purposes described in the document are within the scope of the comprehensive utilization purposes stated explicitly at the time of concluding the contract, etc., a member is not required to state the utilization purposes explicitly each time it acquires personal information using the document.	
(3) A member shall, in case of altering a utilization purpose, inform a principal of, or disclose to the public, a post-altered utilization purpose.		Article 18, paragraph (3) of the Protection Act 3-1-2 of the General Rules Guidelines
(4) The provisions of the preceding paragraphs shall not apply in those cases set forth in the following:		Article 18, paragraph (4) of the Protection Act 3-2-5 of the General Rules Guidelines Article 6, paragraph (3) of the Financial Sector Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(i) 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, fortune or other rights and interests;	Specific example of paragraph (4), item (i) For example, when there is a risk that undue resentment is directed against persons who provide: information on antisocial forces such as organized crime groups; information subject to suspicious transaction reporting; and information on malicious persons who are engaged in the obstruction of business.	
(ii) 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 said personal information handling business operator;	Specific examples of paragraph (4), item (ii) The following are the examples that fall under the definition: a. A case in which notification, etc. of the utilization purpose results in disclosing a new service or business know-how under development, thereby hindering sound competition of the company; b. A case in which there is a possibility that provision of information on an organized crime group or other antisocial forces, information on what the relevant party shall be notified of as a suspicious transaction, or information on malicious persons who obstruct business operations may have the information provider subject to unjustified resentment.	
(iii) Cases in which there is a need to cooperate in regard to 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; and	Specific examples of paragraph (4), item (iii) For example, a case in which a member acquires information on a suspect, etc. to cooperate in criminal investigations.	
(iv) Cases in which it can be recognized, judging from the circumstances of acquisition, that a utilization purpose is clear.	Specific examples of paragraph (4), item (iv) The following are the examples that fall under the definition: a. A case in which a person requests reference materials by phone, etc., and the information provided by the person regarding his/her address and name is used only for the purpose of sending the requested materials; b. A case in which business cards are exchanged to keep in touch in the future; c. A case in which a member receives a phone call with a non-anonymous number and makes a return call on the same subject to the non-anonymous caller.	
(Assurance etc. about the Accuracy of Data Contents) Article 9 A member must strive to maintain personal data accurate and up-to-date to the extent necessary to achieve utilization purposes by, for example: establishing procedures for reconciling and checking personal information when entering such information into personal information database, etc.; establishing procedures for making amendments when a mistake, etc. is found; updating recorded items; and specifying a retention period. In this case, it is not necessary to uniformly or constantly update personal data held, and it is sufficient with ensuring the accuracy and up-to-date state within the scope of necessity depending on the respective utilization purposes. Furthermore, when there is no need to use personal data held any more for such reasons as; its utilization purposes have been achieved and no reasonable grounds for holding the personal data exist anymore in relation to the purposes; or its utilization purposes were not achieved but the project that served as the premise for the purposes has been canceled, etc., a member must strive to delete the personal data without delay; provided, however, that this does not apply if a retention period is prescribed under laws and regulations.	(1) Methods to “keep personal data accurate and up to date” The following are the examples of possible methods: a. Encouraging customers to provide accurate and up-to-date data; and b. Reflecting notifications from customers in a database, etc. in a quickly and accurate manner. (2) Retention period Personal data may be retained permanently if reasonable grounds exist.	Article 19 of the Protection Act 3-3-1 of the General Rules Guidelines Article 7 of the Financial Sector Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(Security Control Measures) Article 10 (1) A member must establish basic policies and handling rules for security control of personal data, develop a system for security control measures, and take other necessary and appropriate measures in order to prevent the leak, loss or damage of personal data it handles or otherwise ensure security control of personal data, based on the "Operational Instructions on the Security Control Measures Based on the Guidelines for Protection of Personal Information in the Finance Sector." Necessary and appropriate measures 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 measures are to be those corresponding to risks arising from the nature of the business, the handling status of personal data (including the nature and volume of the personal data the member handles), the nature of the medium wherein personal data is recorded and other factors, in consideration of the significance of infringement of rights and interests that may be suffered by the person in question in the event of a leakage, loss or damage of personal data. For example, in the case of a name list that can be purchased by unspecified and large number of persons at any time at book stores and for which an operator makes no alterations, as such data is unlikely to cause any infringement of individuals' rights and interests, even if the operator has disposed of it without shredding it with a shredder or otherwise treating it or has handed it over to a recycling service provider, this does not constitute a violation to its obligation to take security control measures. The terms as used in this Article shall be defined as follows: (i) Institutional security control measures The term "institutional security control measures" means measures for system development and actions to be taken by a personal information handling business operator for security control of personal data, such as to clearly determine the responsibility and authority of officers and employees (persons engaging in the business of a member within its organization under direct or indirect control and supervision of the 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 member (directors, executive officers, board members, company auditors, inspectors and temporary staff, etc.); the same shall apply hereunder), establish and implement rules on security control, and inspect and audit the implementation status. (ii) Human security control measures The term "human security control measures" means to conclude a non-disclosure contract with officers and employees and provide them with education, training, etc., thereby supervising officers and employees so as to ensure security control of personal data. (iii) Technological security control measures The term "technological security control measures" 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. (2) A member must take institutional security control measures as follows for establishing basic policies and handling rules for security control of personal data: (i) 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		Article 20 of the Protection Act 3-3-2 of the General Rules Guidelines Article 8 of the Financial Sector Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(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 security control at each stage; (a) Handling rules at the stage of acquisition and input of data (b) Handling rules at the stage of use and processing of data (c) Handling rules at the stage of reservation 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 time of responding to information leakage or other incidents (3) A member must take institutional security control measures, human security control measures and technological security control measures as follows for developing a system for security control of personal data. (i) Institutional security control measures (a) Appointment of employees responsible for the management of personal data (the supervising personal data safety administrator, who is ultimately responsible for executing duties relating to the safety control of personal data, and the personal data administrators at each department handling personal data) (b) Development of security control measures 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 (ii) Human security control measures (a) Conclusion of a non-disclosure contract concerning personal data with officers and employees (b) Clarification of roles and responsibilities of officers and employees (c) Thorough dissemination of safety control measures to officers and employees, and their education and training (d) Checking of officers' and employees' compliance with predetermined personal data management procedures (iii) 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 leakage, damage, etc. of personal data (e) Recording and analysis of access to personal data (f) Recording and analysis of operation of the information system handling personal data (g) Monitoring and audit of information systems handling personal data		
(Supervision over Officers and Employees) Article 11 (1) A personal information handling business operator must, in having its officers and employees handle personal data, develop an appropriate internal control system and exercise necessary and appropriate supervision over its officers and employees so as to seek the security control of the personal data. The supervision is to 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 person in question in the event of a leakage, loss or damage of personal data. (2) A member must exercise necessary and appropriate supervision over its officers and employees as described in the	(Note) See Article 10 for the definition of officers and employees.	Article 21 of the Protection Act 3-3-3 of the General Rules Guidelines Article 9 of the Financial Sector Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
preceding paragraph through, for example, developing the following systems: (i) To conclude a contract upon recruiting an officer or employee to ensure that the person will not disclose to a third party any personal data that he/she has come to know in the course of performing duties in the investment management business or investment advisory and agency business carried out by the member, or use such data for unintended purposes while being employed and after resigning from the job; (ii) To clarify the roles and responsibilities of its 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; and (iii) To develop a system for checking its officers' and employees' compliance 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.		
(Supervision over Outsourcees) Article 12 (1) When a member outsources (including the entirety of outsourcing contracts, irrespective of the form or type thereof, under which the member has another entity carry out the whole or part of the handling of personal data) the handling of personal data partially or in its entirety, the member must exercise necessary and appropriate supervision over the relevant outsourcee so as to ensure the security control over the outsourced personal data. The supervision is to 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 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 operator must also supervise whether the outsourcee sufficiently supervises the sub-outsourcees.) Specifically, a member is required to take, for example, the measures mentioned below. (i) The member shall 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 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 employee responsible for the management of personal data make an evaluation of the candidate appropriately. (ii) The member shall 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. At the same time, the operator must 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 member has the supervising personal data administrator 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 member	(Note) Outsourcees include foreign ones.	Article 22 of the Protection Act 3-3-4 of the General Rules Guidelines Article 10 of the Financial Sector Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
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 be 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 applies to cases of further sub-outsourcing.		
(Restriction on Provision to a Third Party) Article 13 (1) A member must not provide personal data to a third party (any person other than the member who intends to provide the personal data and the principal associated with the personal data, regardless of natural person, juridical person or other body; the same shall apply hereinafter except for Articles 13-2 through 13-5) without obtaining prior consent of the principal. When the consent is obtained, depending on the size and nature of business, handling status of personal data (including the nature and volume of personal data handled), etc., the content within the reasonable and appropriate scope that is deemed necessary for the principal's judgment about the consent must be expressly showed. Where it is assumed in advance to provide personal information to a third party, the fact must be manifested in the utilization purposes; provided, however, that in the following cases, the principal's consent is not required when providing personal data to a third party:	Points to note when providing personal data to a third party When providing the acquired personal data to a third party, a member needs to confirm which of the following categories the case falls under: a. Methods where the principal's consent (including assumed consent) is obtained; b. Cases that are subject to an exemption from application as specified under laws and regulations, etc. (paragraph (1), items (i) to (iv)); c. Cases where an opt-out (suspension of provision at the principal's request) is exercised (paragraph (2)); d. Cases where the handling of personal data is outsourced (paragraph (4), item(i)); e. Cases where a merger or other types of business succession is carried out (paragraph (4), item(ii)); f. Cases where personal data is jointly utilized (paragraph (4), item (iii)); g. Cases where the handling is sub-outsourced (paragraph (4), Item (iv)).	Article 23, paragraph (1) of the Protection Act Article 11, paragraph (1) of the Financial Sector Guidelines
(i) Cases based on laws and regulations;	The following are the examples that fall under the definition: a. Article 56-2 (Collection of Reports and Inspections) of the Financial Instruments and Exchange Act b. Articles 210, 211, etc. (Investigation of Criminal Cases by Officials of Securities and Exchange Surveillance Commission) of the Financial Instruments and Exchange Act c. Article 8, paragraph (1) (Reporting of Suspicious Transactions) of the Act on Prevention of Transfer of Criminal Proceeds d. Articles 74-2 to 74-6 ("Right of Inquiries and Inspection of Tax Authority Officials") of the Act on General Rules for National Taxes e. Article 1, etc. (Inspection of Criminal Cases by Tax Collectors or Voluntary Investigations of Criminal Cases by Tax Collectors or Local Tax Officials) of the National Tax Violations Control Act f. Article 72-63 (Right of Inquiries and Inspection Concerning Enterprise Tax of Personnel of the Ministry of Internal Affairs and Communications) of the Local Tax Act g. Article 141 (Inquiries and Inspections) of the National Tax Collection Act	

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
	h. Article 197 (Report on Particulars Relating to Investigations) of the Code of Criminal Procedure i. Article 218, paragraph (1) (“Seizure, Search, and Inspection upon Warrant”) of the Code of Criminal Procedure j. Article 223 (Order to Submit Documents) of the Code of Civil Procedure k. Article 23-2, paragraph (2) (Request for Information) of the Attorney Act	
(ii) Cases in which there is a need to protect a human life, body or fortune (including fortune of a juridical person), and when it is difficult to obtain a principal’s consent;	The following are the examples that fall under the definition: a. When providing information concerning illegal activities by antisocial groups including so-called corporate racketeers or organized crime groups, or their members, etc.; b. When providing family members’ contact information, etc. to a medical institution to deal with sudden illnesses of a customer, etc.; c. Provision of the details of a contract, etc. to relatives of a principal in the event that the principal continues to be missing due to an earthquake, disaster, etc.; and d. When enterprises share information on antisocial forces such as organized crime groups and malicious persons who obstruct business operations.	
(iii) 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; and		
(iv) Cases in which there is a need to cooperate in regard to 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.	The following are the examples that fall under the definition: a. When responding to a voluntary investigation by tax authorities; b. When responding to a voluntary investigation by the police; and c. When responding to a general statistical survey. (Note) A member shall determine, on a case-by-case basis, whether or not it needs to cooperate.	
(2) Notwithstanding the provisions of the preceding paragraph, a member may provide personal data (excluding sensitive information; hereinafter the same shall apply in this paragraph) to a third party in cases where it is set to discontinue, 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 when it keeps them in a state in which a principal can readily gain knowledge of them and has notified them to the Personal Information Protection Commission; Furthermore, a member shall make a public announcement on the details of the notification by employing appropriate methods such as using its website, etc. Sensitive information may not be provided to a third party due to the opt-out consent.	State in which a principal can readily gain knowledge The “state in which a principal can readily gain knowledge” means a condition in which a principal can readily access the information the matter can be easily known, in terms of both time and means, by the principal if he/she wants to know. Accordingly, a member may take such measures as regularly making public announcements using, for example, the approaches listed below, depending on the way in which it performs solicitation activities, or notifying its customers in advance of how to be informed of the matter. a. Regular posting on the website; b. Regular posting and keeping at the counter of sales offices, etc.; or c. Continuous display in pamphlets and leaflets. (Note) Using multiple approaches is desirable.	Article 23, paragraph (2) of the Protection Act 3-4-2 of the General Rules Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(i) To set a third-party provision as a utilization purpose; (ii) The categories of personal data provided to a third party; (iii) A method of a third-party provision.	Specific examples of a "method of a third-party provision" The following are the examples that fall under the definition: a. Issuance of publications; b. Provision of information online, etc.;	
(iv) To cease, in response to a principal's request, a third-party provision of personal data that can identify the principal; and (v) A method of receiving a principal's request.	Specific example of a "method of receiving a principal's request" a. By mail; b. Send e-mails; c. Filling in a designated form on the website; d. Receiving at the counter of sales offices; e. Telephone:	
(3) A member shall, in case of altering those matters set forth in item (ii), item (iii) or item (v) of the preceding paragraph, in advance inform a principal of the contents to be altered or put them into a state in which a principal can easily gain knowledge and notify them to the Personal Information Protection Commission pursuant to rules of the Personal Information Protection Commission. When a member notifies the Personal Information Protection Commission of necessary matters in accordance with this paragraph, it shall make the details of the notification public on its own.		Article 23, paragraph (3) of the Protection Act 3-4-2 of the General Rules Guidelines
(4) In those cases set forth in the following, a person receiving the provision of the said personal data shall not fall under a third party in regard to applying the provisions of each preceding paragraph: (i) Cases in which personal data is provided accompanied by a member entrusting a whole or part of the handling of the personal data within the necessary scope to achieve a utilization purpose;	Specific examples of "cases in which personal data is provided accompanied by a member entrusting a whole or part of the handling of the personal data within the necessary scope to achieve a utilization purpose" The following are the examples that fall under the definition: a. Cases where customer data is provided and the data input function is outsourced; b. Cases where customer data is provided and the document sending function is outsourced; c. Cases where customer data storage and disposal are outsourced; and d. Cases where other administrative processes are outsourced. (Note) It should be noted that a member must exercise necessary and appropriate supervision over its outsourcees according to Article 12.	Article 23, paragraph (5) of the Protection Act 3-4-3 of the General Rules Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(ii) Cases in which personal data is provided accompanied with business succession caused by a merger or other reason (limited to cases in which personal data is used within the scope of the utilization purposes prior to the data is provided through the business succession even thereafter);	Specific examples of the "cases in which personal data is provided accompanied with business succession caused by a merger or other reason" The following are the examples that fall under the definition: a. Merger; b. Company split; and c. Business transfer.	
(iii) 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 of the categories of the jointly utilized personal data, the scope of a jointly utilizing person, the utilization purpose for the utilizing person and the name or appellation of a person responsible for controlling the said personal data (within the organization of the person who jointly utilizes the personal data, any individual who is primarily responsible for accepting and processing complaints, making decisions on amendments, etc. and discontinuation of use, etc. and performing security control; the individual is referred to as "supervising administrator" under paragraph (6)), or when such data is kept in a state in which a principal can easily gain knowledge of it;	Specific example of cases where personal data is "jointly utilized" Cases where a member utilizes customer data provide asset management services to its customers jointly with its group companies, etc. In principle, a "notification" is to be given in writing.	Article 11, paragraph (4) of the Financial Sector Guidelines
(5) When a member gives the notification as specified under item (3) of preceding paragraph, the notification shall be made, in principal, in a written form. With regard to a notification, etc. concerning "the scope of a jointly utilizing person," it is desirable to list the persons who jointly utilize the personal data respectively.	The "scope of a jointly utilizing person" a. It is desirable to list the jointly utilizing person individually. b. In the case of a. above, a member is suggested to show the scope of jointly utilizing persons in an easy-to-understand way by, for example, providing the names of such persons on its website.	3-4-3 of the General Rules Guidelines
(6) A member shall, in the case of altering a utilization purpose for a utilizing person or the name or appellation of the supervising administrator prescribed in paragraph (4), item (iii), inform in advance the principal of the contents to be altered or put them into a state in which the principal can easily gain knowledge of them.		Article 23, paragraph (6) of the Protection Act 3-4-3 of the General Rules Guidelines
(Restriction on Provision to a Third Party in a Foreign Country) Article 13-2 A member must, except in those cases set forth in each item of the preceding Article, paragraph (1), 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 in this Article) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same), obtain in advance a principal's consent to the effect that he/she approves the provision to a third party in a foreign country. In this case, the provisions of the preceding Article shall not apply.		Article 24 of the Protection Act Article 11 of the Enforcement Rules 3-4-4 of the General Rules Guidelines Guidelines on the Act on the Protection of Personal Information (Volume on

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
		Provision to a Third Party in a Foreign Country)
(Keeping etc. of a Record on a Third-Party Provision) Article 13-3 A member must, when having provided personal data to a third party (excluding a person set forth in each item of Article 2, paragraph (5); hereinafter the same in this Article up to paragraph (5)), keep a record on the date of the personal data provision, the name or appellation of the third party, and other matters prescribed by the Enforcement Rules; provided, however, in the case of provision to a third party in Japan, it is not necessary to keep a record if items (i) to (vii) below apply: Furthermore, in the case of provision to a third party in a foreign country, it is not necessary to keep a record if items (i) to (iv) below apply, or if the third party satisfies criteria provided for in the Enforcement Rules and the cases listed under items of Article 23 of the Protection Act apply. (i) Cases based on laws and regulations; (ii) Cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent; (iii) 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; and (iv) Cases in which there is a need to cooperate in regard to 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. (v) Cases in which personal data is provided as a consequence of a member entrusting a whole or part of the handling of the personal data within the scope necessary to achieve a utilization purpose; (vi) Cases in which personal data is provided as a consequence of business succession caused by a merger or other reason; and (vii) 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 of such effect, items of the jointly utilized personal data, the scope of jointly utilizing persons, the utilization purpose for the utilizing persons and the name or appellation of the person responsible for controlling the said personal data, or when these particulars are kept in a state in which a principal can readily gain knowledge of them.		Article 25 of the Protection Act Articles 12 and 13 of the Enforcement Rules 3-4-5 of the General Rules Guidelines Guidelines on the Act on the Protection of Personal Information (Volume on Confirmation and Record-Keeping Obligations upon Third-Party Provision)
(Confirmation etc. when Receiving a Third Party Provision) Article 13-4 Except for the cases listed below, a member must, 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 corporation, the name of its representative		Article 26 of the Protection Act

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(for an organization without legal personality having appointed a representative or administrator, the representative or administrator), circumstances under which the personal data was acquired by the third party, and create a record on the matters prescribed under Article 26, paragraph (3) of the Protection Act; provided, however, that the confirmation and record-keeping obligations do not apply to cases where the provision is not made in actuality by the "provider." (i) Cases based on laws and regulations; (ii) Cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent; (iii) 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; and (iv) Cases in which there is a need to cooperate in regard to 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. (v) Cases in which personal data is provided as a consequence of a member entrusting a whole or part of the handling of the personal data within the scope necessary to achieve a utilization purpose; (vi) Cases in which personal data is provided as a consequence of business succession caused by a merger or other reason; and (vii) 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 of such effect, items of the jointly utilized personal data, the scope of jointly utilizing persons, the utilization purpose for the utilizing persons and the name or appellation of the person responsible for controlling the said personal data, or when these particulars are kept in a state in which a principal can readily gain knowledge of them. (Retention Period pertaining to the Records on Third-party Provision) Article 13-5 A member must maintain records prepared as prescribed under Articles 13-3 and 13-4 for a period of time set forth in the Enforcement Rules from the date when the records are created.		Articles 15 through 17 of the Enforcement Rules 3-4-6 of the General Rules Guidelines Guidelines on the Act on the Protection of Personal Information (Volume on Confirmation and Record-Keeping Obligations upon Third-Party Provision)

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
		Articles 25 and 26 of the Protection Act Articles 14 and 18 of the Enforcement Rules 3-4-5 and 3-4-6 of the General Rules Guidelines Guidelines on the Act on the Protection of Personal Information 4-3 (Volume on Confirmation and Record-Keeping Obligations upon Third-Party Provision)
(Public Disclosure etc. on Matters relating to Personal Data Held) Article 14 (1) A member must, concerning its personal data held, keep the matters set forth in the following in a state in which a principal can readily gain knowledge of them (including those cases in which it, at the request of a principal, responds without delay). If its utilization purposes include the third party provision, it must describe that effect as the content of item (ii). (i) Member's name; (ii) Utilization purposes of all personal data held (excluding those cases falling under items (i) through item (iii) of Article 8, paragraph (4)); (iii) The procedures for responding to a request pursuant to the provisions of the succeeding paragraph, or to a demand pursuant to the provisions of paragraph (1) of the succeeding Article, paragraph (1) of Article 16 or paragraph (1) or (2) of Article 17 (including, when the amount of a fee has been decided pursuant to the provisions of Article 20, the amount of the fee); (iv) Contact address to make a complaint or inquiry about the handling of personal data held; and (v) Names of accredited personal information protection organizations and their contact address to lodge a complaint	Specific examples of the "state in which a principal can readily gain knowledge (including those cases in which it, at the request of the principal, responds without delay)" It refers to a state in which the principal can access if he/she so wishes. A member needs to take appropriate measures using, for example, the following methods depending on the way in which it performs solicitation activities, etc.; a. Regular posting on the website (or, posting in conjunction with the "Declaration on the Protection of Personal Information" under Article 23); b. Regular posting and keeping at the counter of sales offices, etc.; or c. Continuous display in pamphlets and leaflets. d. Issuance of documents or sending of the same via mail or facsimile according to the principal's request; and e. Oral, telephone, or e-mail responses to a principle according to his/her request.	Article 27, paragraph (1) of the Protection Act Enforcement Ordinance Article 8 3-5-1 of the General Rules Guidelines Article 12 of the Financial Sector Guidelines
(2) A member must, when requested by a principal to get informed of a utilization purpose of personal data held that can identify the principal, inform the said principal thereof without delay; provided, however, that this shall not apply in those cases falling under any of each following item: (i) Cases in which the utilization purpose of personal data held that can identify the said principal is clear pursuant to the provisions of the preceding paragraph; or (ii) Cases falling under items (i) through item (iii) of Article 8, paragraph (4).		Article 27, paragraph (2) of the Protection Act 3-5-1 of the General Rules Guidelines
(3) A member must, when having been requested based on the provisions of the preceding paragraph but decided not to inform a principal of the utilization purpose of personal data held, inform the principal to that effect without delay.		Article 27, paragraph (3) of the Protection Act

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
		3-5-1 of the General Rules Guidelines
(Disclosure) Article 15 (1) A member must, when it received a demand from a principal to disclose its personal data held that can identify the principal, disclose that personal data held by a member (including, if the data does not exist, a notification to that effect) without delay, by delivering a document (or in a method agreed with the person who demanded the disclosure, if any); provided, however, in cases where disclosing such data falls under any of each following item, a whole or part thereof may not be disclosed;	(i) The term "disclosure" refers to providing the details of the personal information whose disclosure is demanded, including the existence or nonexistence thereof. (ii) Specific examples of a "method agreed with the person who made a demand for disclosure" The following are the examples of possible methods: a. Using an e-mail; or b. Making a phone call.	Article 28, paragraph (2) of the Protection Act Article 9 of the Cabinet Order 3-5-2 of the General Rules Guidelines Article 13 of the Financial Sector Guidelines
(i) Cases in which there is a possibility of harming a principal or third party's life, body, fortune or other rights and interests; (ii) Cases in which there is a possibility of interfering seriously with the member implementing its business properly; or	(i) Examples of cases in which "there is a possibility of interfering seriously with the member implementing its business properly" The following are the examples that fall under the definition: a. Cases in which a member received a demand for disclosure of information added by the member, such as assessment information, or the disclosure of its personal data held by a member may hinder proper response to customers, etc.; b. Cases in which the disclosure is likely to seriously impede the execution of the member's business, including such cases where a principal repeatedly makes demands for the disclosure of the same information that requires complex disclosure procedures, and the demands practically occupy the inquiry response function and prevent the function from responding to other inquiries; c. Cases in which disclosure of the personal data held by a member may hinder proper assessment, testing, etc.; and d. Cases in which the disclosure may pose the risk of revealing business secrets. (ii) Examples of cases that do not fall under the definition of "cases in which "there is a possibility of interfering seriously with the member implementing its business properly"	

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
	For example, a member may not reject the disclosure only for the reason that there is a large volume of personal data held by a member to be disclosed.	
(iii) Cases of violating other laws or regulations.	Example “cases of violating other laws and regulations" For example, cases to which Article 8, paragraph 2 of the Act on Prevention of Transfer of Criminal Proceeds (Leakage of the Fact of Filing to Customers).	
(2) A member must, when having decided not to disclose a whole or part of personal data held by a member in connection with a demand pursuant to the provisions of preceding paragraph or when the personal data held by a member does not exist, inform a principal thereof without delay. It shall also provide explanation about the reason for the decision without delay, by showing the provisions of laws that were used as legal basis, as well as the facts based on which the decision was made.	Specific examples of the method of “explanation” The following are the examples of possible methods: a. Written explanation; b. Verbal explanation; c. Explanation using an e-mail; and d. Explanation by telephone (including automatic voice).	Article 28, paragraph (3) of the Protection Act 3-5-2 of the General Rules Guidelines Article 13 of the Financial Sector Guidelines
(Correction, etc.) Article 16 (1) If a member receives a demand from a principal for a correction, addition, or deletion (hereinafter referred to as a “correction, etc.”) of its personal data held by a member that identifies the principal on the grounds that the personal data held by a member is incorrect and not true, the member must undertake, without delay, necessary investigations including fact check, etc., within the scope necessary to achieve the utilization purposes, and must, in principle, make corrections, etc. to the personal data held based on the investigation results.	a. A correction, etc. shall be made within the scope necessary to achieve the utilization purposes. Accordingly, a member is not required to make a correction, etc. beyond necessary. b. If a request for a correction, etc. is made in relation to assessment information rather than a fact, it is not necessary to make the correction, etc.	Article 29, paragraph (2) of the Protection Act 3-5-3 of the General Rules Guidelines
(2) A member shall, when having made a correction etc. to a whole or part of the contents of the personal data held by a member in connection with a demand pursuant to the preceding paragraph or when having made a decision not to make a correction etc., inform the principal thereof (including, when having made a correction etc., the details thereof) without delay. If the member does not make corrections, etc., it shall provide an explanation thereof by showing the grounds for not making corrections, etc. and the facts that support the grounds.		Article 29, paragraph (3) of the Protection Act 3-5-3 of the General Rules Guidelines
(Discontinuance of Use, etc.) Article 17 (1) In case where a member receives, from a principal, a demand for the discontinuance of use or erasure (hereinafter referred to as “discontinuance of use, etc.”) of such personal data held as may lead to the identification of the principal on the ground that the personal data held by a member is being handled in violation of Article 4 or was acquired in violation of the provisions of Article 7, and where it is found that the request has a reason, the member must implement the discontinuance of use, etc. of the personal data held by a member without delay to the extent necessary for redressing the violation; provided, however, this provision shall not apply to cases in which it costs large amount or otherwise difficult to implement the discontinuance of use, etc. and in which the member takes necessary alternative measures to protect the rights and interests of the principal.		Article 30, paragraph (2) of the Protection Act 3-5-4 of the General Rules Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(2) Where a member received a demand from a principal to discontinue providing to a third party such personal data held by a member that may identify the principal on the ground that the personal data held by a member is being provided to a third party in violation of paragraph (1) of Article 13, and where it is found that the demand has a reason, the member must discontinue providing the personal data held by a member to a third party without delay; provided, however, this provision shall not apply to cases in which it costs large amount to discontinue providing the personal data held by a member to a third party or otherwise difficult to discontinue providing the personal data held by a member to a third party and in which the member takes necessary alternative measures to protect the rights and interests of the principal.		Article 30, paragraph (4) of the Protection Act 3-5-4 of the General Rules Guidelines
(3) When a member has discontinued using or has erased all or part of the personal data held by a member for which a demand was made under paragraph (1), or has decided not to discontinue using or not to erase the personal data held by a member, or when a member has discontinued providing to a third party all or part of the personal data held by a member for which a demand was made under the provision of the preceding paragraph or has decided not to discontinue providing the personal data held by a member to a third party, the member shall inform the person thereof (including, when the member takes measures different from those requested by the principal, the details of the measures) without delay.		Article 30, paragraph (5) of the Protection Act 3-5-4 of the General Rules Guidelines
(Explanation of Reason) Article 18 When a member informs a principal that it would not take all or some of the measures requested or demanded by the principal or would take measures different therefrom pursuant to the provisions of Article 14, paragraph (3), Article 15, paragraph (2), Article 16, paragraph (2), or Article 17, paragraph (3) hereof and provides explanations about the reasons therefor to the principal, the member shall present to the principal the grounds for deciding not to take those measures or to take different measures, as well as the facts that support those grounds.		Article 31 of the Protection Act 3-5-5 of the General Rules Guidelines Article 14 of the Financial Sector Guidelines
(Procedures for Responding to Demands for Disclosure) Article 19 (1) With regard to requests pursuant to the provisions of Article 14, paragraph (2) or demands pursuant to the provisions of Article 15, paragraph (1), Article 16, paragraph (1), or Article 17, paragraphs (1) or (2) hereof (hereinafter referred to as "demands, etc. for disclosure, etc."), a member may prescribe, within a reasonable scope, the following matters listed under the items below as the methods of accepting those requests or demands: In this case, the member shall regularly post them on its website or take such measures as posting and keeping of them at the counter of sales offices, etc., in conjunction with the "Declaration on the Protection of Personal Information" stipulated in Article 23.		Article 32 of the Protection Act Articles 10 and 11 of the Cabinet Order 3-5-6 of the General Rules Guidelines Article 15 of the Financial Sector Guidelines
(i) Contacts to file a demand for disclosure;	Specific examples of the contacts to file a demand for disclosure For example, name of contact persons or team, mailing address, reception telephone number, reception fax number, e-mail address, etc.	

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(ii) Format of the documents to be submitted when filing a demand, etc. for disclosure, etc. and other methods of accepting a demand, etc. for disclosure, etc.; and	(1) Format of documents to be submitted when filing a demand, etc. for disclosure, etc. For example, when setting the format of documents to file demands to, for example, disclose, change, or discontinue the use of personal data held personal data held by a member, a member may include, in the documents, columns to fill in matters that are necessary to identify the personal data held by a member subject to the demand, etc. for disclosure, etc., including columns for name, address, customer number, contract date, etc., in order to facilitate the procedure of the demand, etc. for disclosure, etc. from a principal. (2) Specific examples of other methods of accepting a demand, etc. for disclosure, etc. For example, a member may accept a demand via mail, fax, e-mail, etc. It is desirable for a member to provide multiple methods so that a principal can easily make a demand, etc. for disclosure, etc.	
(iii) A method to confirm that the person who makes a demand, etc. for disclosure, etc. is the principle or his/her agent;	(1) The “agent” is a statutory agent of a minor or an adult ward, or an agent discretionally appointed by the principal. (2) Specific example of the methods to confirm that the person is the principal or his/her agent It is considered necessary to perform a confirmation procedure based on the provisions of the Identity Confirmation Act or equivalent procedures.	
(iv) The amount of fee set out in Article 20 and the method to collect the fee (including cases where the fee is free);		
(v) A method, etc. to respond to demands, etc. for disclosure, etc.; and	Specific examples of methods to respond to demands, etc. for disclosure, etc. The following are the examples of possible methods: a. Postal mail, telephone, and e-mail; b. Depending on the type of information to be disclosed, the response will be made at a later time rather than immediately.	
(vi) A method to confirm the power of representation when the person who makes a demand, etc. for disclosure etc. is an agent.	Specific examples of methods to confirm an agent’s power of representation The following are the examples of possible methods: a. Only the power of attorney prescribed by the member shall be accepted; b. When a power of attorney, etc. is submitted but there are some exceptional circumstances that make the existence of power of representation suspicious, no disclosure shall be made until the principal’s intent to grant the power is confirmed by phone, etc.; and c. If it is unable to confirm the power of representation using a method prescribed by the member, no disclosure shall be made.	

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(2) A member is not precluded from disclosing the relevant personal data directly only to the principal in response to a demand, etc. for disclosure, etc. by an agent.		Article 15, paragraph (2) of the Financial Sector Guidelines
(3) A member must, in establishing a procedure for responding to a 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.	Examples of cases where “excessive burden is imposed on a principal” a. Cases where a principal has no means than visiting a member to file a demand; b. Cases where a principal is required to submit documents that are needlessly complex; and c. Cases where unreasonable restrictions are placed on the demand receiving function.	Article 32, paragraph (4) of the Protection Act
(Fee) Article 20 (1) A member may, when having been requested to inform of a utilization purpose of personal data held pursuant to the provisions of Article 14, paragraph (2) hereof, or when having received a demand for the disclosure of personal data held pursuant to the provisions of Article 15, paragraph (1) hereof, collect a fee in relation to taking that measure. Furthermore, once the amount of fee is decided, a member shall keep the information in a state in which a principal can gain knowledge of it.		Article 33, paragraph (1) of the Protection Act 3-5-7 of the General Rules Guidelines
(2) A member shall, 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.	A reasonable method to “consider actual expenses" is to estimate and calculate an average of actual expenses required for disclosure process, etc. These actual expenses would include the cost of paper, photocopies, mailing, etc.	Article 33, paragraph (2) of the Protection Act 3-5-7 of the General Rules Guidelines
(Dealing with Complaints by a Member) Article 21 (1) A member must, when a complaint about the handling of personal information is lodged, investigate the details and strive to process it appropriately and promptly within a reasonable period of time.		Article 35, paragraph (1) of the Protection Act 3-6 of the General Rules Guidelines
(2) A member must strive to establish a system necessary to handle complaints appropriately and promptly, such as formulating complaint processing procedures, establishing a complaint receiving desk, and providing sufficient education and training to officers and employees who handle complaints.		Article 35, paragraph (2) of the Protection Act 3-6 of the General Rules Guidelines Article 16 of the Financial Sector Guidelines
()		

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(Response to Personal Information Leakage Cases) Article 22 (1) In the event of the leakage of any personal information or the leakage of information concerning descriptions, etc. and individual 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 Act (hereinafter referred to as a "personal information leakage or other incident"), a member shall immediately report it to the relevant supervisory authority.	(1) Leakage cases, etc. shall include losses of, and damages to, personal information. (2) It shall be noted that depending on the case, reporting to the police and other investigative authorities may be necessary. (3) The notification to the Association shall be made after excluding the information which will enable identification of a specific individual from the report. (4) Depending on the administrative category to which a member belongs, a report shall be made to a supervisory authority, i.e. the Commissioner of the Financial Services Agency, the Director-General of Local Finance Bureau, or the Director of Local Branch Finance Bureau.	Basic Policy Article 17, paragraph (1) of the Financial Sector Guidelines Question IV-7 in the Q&A about personal information at financial institutions
(2) In the event of the leakage of personal information or any other related incident, a member shall disclose the facts concerning the incident and measures to prevent a recurrence to the public without delay from the perspective of preventing secondary damage or the occurrence of any similar incidents.	(1) Even if an incident was caused by a wrong delivery or transmission of a mail, e-mail, facsimile message, or the like, and the leakage is minor in terms of volume, content, etc., it needs to be disclosed if there is a possibility that secondary damage or similar cases may occur. (2) "Prevention of recurrence" A member may take such measures as investigating actually occurred leakage incidents, etc. to find deficiencies in the security control system and remedying and correcting those deficiencies as soon as possible.	Article 17, paragraph (2) of the Financial Sector Guidelines
(3) In the event of the leakage of personal information or other related incident, a member shall promptly inform the principal involved in the relevant incident of the facts concerning the incident.		Article 17, paragraph (3) of the Financial Sector Guidelines
(Formulation of the Declaration on the Protection of Personal Information) Article 23 (1) In consideration of the significance of explaining policies related to personal information in advance in an easy-to-understand manner, a member shall formulate and publicly announce 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 "Declaration on the Protection of Personal Information").	Specific examples of methods to "announce" The following are the examples of possible methods: a. Regular posting on the website; b. Posting and keeping at the counter of sales offices; and c. Describing in, and delivery of, pamphlets.	Articles 18 and 27 of the Protection Act Basic Policy Article 18 of the Financial Sector Guidelines
(2) In the Declaration on the Protection of Personal Information, a member shall, for example, describe the following matters: (i) Pronouncement of policies concerning protection of personal information, such as the compliance with relevant laws,		

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
regulations, and association rules, prohibition of utilization of personal information for unintended purposes and proper processing of complaints; (ii) Easy-to-understand explanation about procedures for notification and announcement of its personal information utilization purposes; (iii) Easy-to-understand explanation about procedures for disclosure, etc. or other various procedures for handling of personal information; and (iv) Contact information on offices processing inquiries and complaints concerning handling of personal information. (3) A member shall ensure that the Declaration on the Protection of Personal Information incorporates 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 person in question, including general consumers: (i) When a principal makes a request, a member shall suspend sending direct mail or otherwise voluntarily suspend the utilization of the personal data held by a member; (ii) A member shall strive to increase transparency regarding outsourcing, such as clarifying whether it outsources any business or the content of outsourced business if any; (iii) A member shall devise means to clarify utilization purposes for respective principals, 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 the principal's choice; and (iv) A member shall indicate sources and methods of acquiring personal information (types of information sources, etc.) as concretely as possible.	If a member outsources numerous types of business, it is acceptable to show only representative ones. However, comprehensive descriptions, such as "businesses involving information about transactions with the company," may not necessarily show the details of the outsourced businesses clearly, and therefore are not appropriate. The phrase "by customer type" refers to, when a member operates a multiple number of businesses, the type of customers relevant to respective businesses operated by the member. If there are a number of acquisition sources and methods, it is acceptable to show only representative ones.	
(Report to the Association) Article 24 (1) The Association may request a member to submit a report from time to time to confirm its compliance herewith. (2) The Association will take measures necessary to have its members comply herewith, such as providing members with guidance and making recommendations.		Article 53, paragraph (4) of the Protection Act Basic Policy Article 1, paragraph (4) of the Financial Sector Guidelines

Procedural Guidelines on the Protection of Personal Information	Reference	Provisions Referred
(3) Members must comply herewith and abide by necessary guidance, recommendations, and other measures taken by the association.		
Supplementary Provisions These Procedural Guidelines come into effect as of on April 1, 2005. Supplementary Provisions (October 24, 2007) This amendment comes into effect as of the date on which the Articles of Incorporation (as of September 30, 2007) is approved by the competent minister. (Note) Amended provisions are as follows: (1) Articles 1, 6, 11, and 13 are amended; (2) Interpretation on the Procedural Guidelines in Articles 1, 2, 3, 4 and 13 are amended. Supplementary Provisions (February 24, 2010) This amendment comes into effect as of February 24, 2010. (Note) Amended provisions are as follows: (1) Articles 1, 2, 3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 16, 18, 21, and 23 are amended; (2) Interpretation on the Procedural Guidelines in Articles 2, 3, 4, 8, 13, 15, and 23 are amended; (3) Provisions referred to in Articles 2 and 3 are amended. Supplementary Provisions (September 16, 2015) This amendment comes into effect as of September 16, 2015. (Note) Amended provisions are as follows: (1) Articles 7 and 12 are amended; (2) Interpretation on the Procedural Guidelines in Articles 4, 7, and 13 are amended. Supplementary Provisions (December 16, 2015) This amendment comes into effect as of January 1, 2016. (Note) Amended provisions are as follows: Articles 10 and 11 are amended. Supplementary Provisions (May 24, 2017) This amendment comes into effect as of May 30, 2017. (Note) Amended provisions are as follows: (1) Articles 1, 2, 3, 4, 5, 6, 8, 9, 10, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, and 24 are amended. (2) Articles 13-2, 13-3, 13-4, and 13-5 are newly established.		