Explanation on the Guidelines for Protection of Personal Information

Established on April 20, 2017
Revised on July 15, 2021

Guidelines for Protection of Personal Information	Explanations
Article 1. Purpose 1. In accordance with the Act on the Protection of Personal Information (Act No. 57 of 2003; hereinafter referred to as the "Protection Act"), the Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003; hereinafter referred to as the "Enforcement Order"), the Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3 of 2016; hereinafter referred to as the "Enforcement Rules"), the Basic Policy on the Protection of Personal Information (Cabinet Decision on April 2, 2004), the Guidelines on the Act on the Protection of Personal Information (Volume on General Rules) (Notification of the Personal Information Protection Commission No. 6 of 2016), (Volume on Provision to a Third Party in a Foreign Country) of the said guidelines (Notification of the Personal Information Protection Commission No. 7 of 2016), (Volume on Confirmation and Record-Keeping Obligations upon Third-Party Provision) of the said guidelines (Notification of the Personal Information Protection Commission No. 8 of 2016), (Volume on Anonymously Processed Information) of the said guidelines (Notification of the Personal Information Protection Commission No. 9 of 2016), the Guidelines for the Protection of Personal Information in the Finance Sector (Notification of the Personal Information Protection Commission, Financial Services Agency No. 1 of 2017) and the Practical Guideline on the Security Control Actions under the Guidelines for Protection of Personal Information in the Finance Sector (Notification of the Personal Information Protection Commission, Financial Services Agency No. 2 of 2017), and others (hereinafter referred to as the "Laws and Regulations on Protection of Personal Information"), these guidelines provide for specification of utilization purposes, security control actions and other matters related to personal information as well as specific actions to be taken by Full Members (meaning Full Members specified in Article 7, Paragraph 1, Item 1 of the Articles of Incorporation; the same shall apply hereinafter) of the Investment Trusts Association, Japan (hereinafter referred to as the "Association") in order to ensure the proper handling of personal information in business operations related to the investment management business operated by Full Members (meaning operations set forth in Article 2, Paragraph 8, Item 12 (a) and Item 14 of the same paragraph of the Financial Instruments and Exchange	(1) The Guidelines have been developed based on the provisions of Article 53 of the Protection Act, and provide for matters to be observed by Full Members and necessary actions, etc. to ensure proper handling of Personal Information in operation and direct public offering services conducted by Full Members in line with the current circumstances of Full Members' services. (2) The Guidelines shall apply to all Full Members. (3) "Explanations" presents specific examples and reference examples of ideas and practices for implementing the Guidelines. Specific examples shown in the explanations are not intended to be limited to these examples, and attention is required, as there may be elements to be considered separately depending on individual cases. (4) The individual number (Article 2, Paragraph 5 of the Act on the Uses of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 27 of 2013; hereinafter referred to as the "Numbers Act")) is also regarded as Personal Information; however, it should be noted that handling of the individual number and specific personal information (Article 2, Paragraph 8 of the Numbers Act) may be separately provided for in the Numbers Act, relevant government ordinances, and related guidelines. (5) A Full Member shall comply with the Personal Information Protection Guidelines established by each accredited personal information protection organization with regard to handling of Personal Information in services other than the operation and direct public offering services of Full Members, and shall endeavor to appropriately handle Personal Information in accordance with the purport of the Guidelines if the relevant accredited personal information protection organization has no guidelines, etc. (6) With regard to the Finance Sector GL and the Finance Sector Practical Guidelines, based on the General Rules GL, a Full Member has stipulated matters for which strict actions are required particularly of Personal Information Handling Business Operators in the finance sector in connection with handling of Personal Information, and other matters in light of the nature and use of Personal Information in the finance sector, and it should be noted that any matters not provided for in the Finance Sector GL and the Finance Sector Practical Guidelines are governed by the General

Guidelines for Protection of Personal Information	Explanations
Act (Act No 25 of 1948; hereinafter referred as the "FIEA") including business operations incidental thereto) and business operations related to investment trust managed without instructions from the settlor, and business operations set forth in Article 2, Paragraph 8, Item 7 of the FIEA in association with beneficiary certificates, etc. (meaning beneficiary certificates (including book-entry transfer beneficial interest in an investment trust), investment corporation bond certificates (including book-entry transfer investment equity), or investment corporation bond certificates (including book-entry transfer investment corporation bonds)). 2. In order to prevent divulgation, unauthorized leakage, or any other similar incident involving personal information, it is necessary for Full Members to develop systems for appropriate control of personal information in accordance with Laws and Regulations on Protection of Personal Information as well as related laws and regulations and guidelines, etc.	Rules GL, etc. In addition, it should also be noted that the Finance Sector GL states as follows. (i) Failure to follow any of the provisions that are described with the phrase "must (do)" may be judged to constitute violation of the provision of the Act. (ii) Failure to follow any of the provisions that are described with the phrases "is to (do)," "it is appropriate to (do)," or "it is desirable to (do)" is not judged immediately to constitute violation of the provision of law. Nevertheless, a Full Member is required to take strict measures in light of the nature and use of personal information in the finance sector. (7) In this explanation, the abbreviated name of guidelines, etc. relating to Personal Information shall be as follows. (i) General Rules GL Guidelines on the Act on the Protection of Personal Information (Volume on General Rules) (Notification of the Personal Information Protection Commission No. 6 of 2016) (ii) Foreign GL Guidelines on the Act on the Protection of Personal Information (Volume on Provision to a Third Party in a Foreign Country) (Notification of the Personal Information Protection Commission No. 7 of 2016) (iii) Confirmation and Record-Keeping GL Guidelines on the Act on the Protection of Personal Information (Volume on Confirmation and Record-Keeping Obligations upon Third-Party Provision) (Notification of the Personal Information Protection Commission No. 8 of 2016) (iv) Anonymous Processing GL Guidelines on the Act on the Protection of Personal Information (Volume on Anonymously Processed Information) (Notification of the Personal Information Protection Commission No. 9 of 2016) (v) Finance Sector GL Guidelines for the Protection of Personal Information in the Finance Sector (Notification of the Personal Information Protection Commission, Financial Services Agency No. 1 of 2017) (vi) Finance Sector Practical Guidelines Practical Guideline on the Security Control Actions under the Guidelines for Protection of Personal Information in the Finance Sector (Notification of the Personal Information Protection Commission, Financial Services Agency No. 2 of 2017) (vii) Numbers Act, Finance GL (Supplementary volume) Guidelines for Proper Handling of Specific Personal Information in Financial Services of the Guidelines for Proper Handling of Specific Personal Information (for Business Operators) (Notification of the Specific

Guidelines for Protection of Personal Information	Explanations
	Personal Information Protection Commission No. 5 of 2014) (viii) Basic Policy the Basic Policy on the Protection of Personal Information (Cabinet Decision on April 2, 2004) [Reference provisions, etc.] Article 1 and Article 60 of the Protection Act, Article 1 of the Finance Sector GL, Article 4 of the Numbers Act
Article 2. Definition In the Guidelines, the terms set forth in the following items are as defined in the respective items.	The definitions of the terms used in the Guidelines are based on each paragraph of Article 2 of the Protection Act, 2 of the General Rules GL, and Article 5, Paragraph 1 of the Finance Sector GL
(1) Personal Information This term refers to any information relating to a living person that is capable of identifying a specific person (including any information that can be readily collated with other information and thereby can identify a specific individual) or which contains a personal identification code. "Information Relating to an Individual" is not limited to information identifying an individual such as name, address, gender, date of birth and face image, and is all information representing facts, judgment, and evaluation with respect to attributes such as body, property, occupation and title of an individual, which also includes evaluation information, information made public by publications, etc., and information in the form of image or voice, whether or not such information is concealed by encryption, etc. If the above-mentioned "Information Relating to an Individual," combined with names, etc., "can identify a specific individual," it becomes "Personal Information." If Information Relating to a non-living Individual is simultaneously Information Relating to a living Individual such as bereaved family members, the information shall be regarded as Information Relating to the living Individual. In addition, information relating to corporations and other organizations, such as company name, does not basically fall under the category of "Personal Information"; however, when Information Relating to an Individual, such as names of officers, is included in the information, such part of the information falls under the category of "Personal Information." Furthermore, "individuals" naturally include foreign nationals.	1. Personal Information (No. 1) (1) Specific examples of "Personal Information" In addition to information relating to beneficiaries, etc. and information relating to customers for direct public offering (hereinafter referred to as "customers"), information relating to individuals of prospective customers, client companies, securities issuing companies, etc. and information relating to individuals acquired by a Full Member in its operation and direct public offering services, etc. broadly meet the definition. Personal Information in management of employment of a Full Member's officers and employees (refer to Article 10, Paragraph 2 of the Guidelines), etc. (such as information on recruitment, wages, personal evaluation, and medical checkups) and Personal Information on shareholders of a Full Member itself are not subject to the Guidelines. (i) Information on Beneficiaries, etc. For example, the following may fall under this category. (a) Description in documents proving opinions of beneficiaries on change of contracts stipulated in Article 17 of the Act on Investment Trusts and Investment Corporations (Act No. 198 of 1951; hereinafter referred to as the "Investment Trust Act") (b) Matters stated in beneficial interest registers provided in Article 26, Paragraph 1, Item 8 of the Ordinance for Enforcement of the Act on Investment Trusts and Investment Corporations (Ordinance of the Prime Minister's Office No. 129 of 2000) (c) Information pertaining to Investors of an investment corporation in the event that administrative work has been entrusted by the investment corporation under Article 117 of the Investment Trust Act (ii) Information on customers (including information on original customers whose account was closed by cancellation of contract, etc.) For example, the following may fall under this category. (a) Matters stated in the Customer Card

Guidelines for Protection of Personal Information	Explanations
	(b) Matters stated in identification records (c) Matters stated in transaction account application forms (d) Information pertaining to a customer's transactions (including matters stated in a transaction balance report, as well as cash flows of customer accounts and acceptance and delivery of beneficiary certificates, etc.) (e) Matters stated in an application form for brokerage to a custodian (f) Correspondence with customers (iii) Information on individuals of prospective customers, client companies, securities issuing companies, etc. For example, the following may fall under this category. (a) Information such as name, company name, title, and telephone number (b) Information obtained from questionnaires and list brokers, etc. (c) Information that is in the public domain through official gazettes, large taxpayer lists, personnel records, etc. * Since the acquisition of Individual Number is limited to the purpose of performing clerical work specified in the Number Act, the provision of Individual Number must not be requested from any prospective customer. [Reference provisions, etc.] Article 15 of the Numbers Act (2) Examples falling under the category of information that "can identify a specific individual" For example, the following may fall under this category. (i) Information including name (ii) Information that does not include names but can identify a specific individual by numbers, symbols, images, sounds, or other information attached to each individual contained in the information (iii) Information that cannot solely identify a specific individual but can identify a specific individual by comparing numbers, symbols, or other information contained in the information with other information held by a Full Member or information disclosed to the public through processing by a computer, etc. (3) Cases falling under the category of "information that can be readily collated with other information and thereby can identify a specific individual" For example, in the case where Personal Information independently acquired by each handling department of a Full Member is separately stored in a database installed in each handling department, when both handling departments can check information on both databases in a general manner in the ordinary course of business, the information is considered in a state where it "can be readily collated."

Guidelines for Protection of Personal Information	Explanations
	On the other hand, in the case where it is necessary to make inquiries of other business operators and other cases, when it is difficult to collate information, or when it is not possible for a Full Member to collate information on both databases in a general manner in the ordinary course of business without taking time and effort because both handling departments of the Full Member or the person in the position of supervising the departments, etc. are strictly prohibited from handling both databases in the regulations or operation, the information is considered in a state where it "cannot be readily collated." [Reference provisions, etc.] Article 2 of Protection Act, 2-1 of General Rules GL
1-2 Personal Identification Codes This term refers to letters, numbers, symbols, and other codes specified in Article 1 of the Enforcement Order as those that can identify a specific individual from the information alone.	1-2. Personal Identification Codes (Item 1-2) A "Personal Identification Code" refers to any character/letter, number, symbol, or other codes prescribed by cabinet order as those that can identify a specific individual from the information alone. Any information containing those falling under this category is regarded as Personal Information. Specific examples of Personal Identification Codes are as follows. (1) A character/letter, symbol, or other codes into which any bodily feature has been converted for use by computers that is enough to identify a specific individual, as shown in the following examples (i) Linear pattern formed by undulations on the surface of the iris (ii) Vocal quality determined by vibration of vocal cords, opening and closing of glottis, and shape and change of vocal tract when vocalizing (iii) Posture while walking and movement of both arms, stride length, and other aspects of walking (iv) Shape of veins defined by their branches and endpoints in a palm or in the back of a hand or under the skin of fingers (v) Fingerprint or palm print (2) Passport number (3) Basic pension number (4) License number (5) Resident register code (6) Individual number * Information on the deceased is not included in Personal Information, but it should be noted that individual numbers are subject to security control action even if they are related to the deceased. [Reference provisions, etc.]Article 12 of the Numbers Act (7) Number, etc. stated in an insurance card for health insurance that can identify a Principal * Numbers attached by private sector, etc. shall not be Personal Identification Codes. * It should be noted that there is some Personal Information that is not a Personal Identification Code but is regarded as Personal Information.

Guidelines for Protection of Personal Information	Explanations
	[Reference provisions, etc.] Article 2 of the Protection Act, Article 1 of Enforcement Order, Article 2 through Article 4 of the Enforcement Rules, 2-2 of the General Rules GL
(2) Personal Information Database, etc. This term refers to a collection of information including Personal Information listed below; provided, however, that this shall exclude those that are unlikely to damage rights and interests of individuals in light of the method of use. (a) Database, etc. systematically arranged so that specific Personal Information can be searched by using a computer (b) In addition to those described in (a) above, database, etc. systematically arranged so that specific Personal Information can be easily searched by organizing personal information in accordance with certain rules, which are placed in such a state that it can be easily searched with a table of contents, index, codes, etc.	2. Personal Information Database, etc. (No. 2) (1) Examples falling under the category of "Personal Information Database, etc." For example, the following may fall under this category. (i) Cases where officers and employees enter and organize information in business cards using spreadsheet software, etc. on business computers (irrespective of the owner), and use or provide it for "the company's businesses" such as solicitation of transactions to customers (Item 2 (a)) (ii) Even if a computer is not used, customer cards, etc. that are arranged in Japanese alphabetical order with an index (Item 2 (b)) (2) Examples not falling under the category of "Personal Information Database, etc." Telephone directories, housing maps, personnel records, car navigation systems, questionnaire results, etc. on the market that have not been edited, processed, classified, or organized (3) Under the Numbers Act, a Personal Information Database, etc. is stipulated as a "personal information file." In addition, a personal information file containing an individual number is a "specific personal information file." It should be noted that the Numbers Act prohibits financial institutions from using individual numbers as customer numbers for the purpose of customer management. The same shall apply in cases where the number is replaced by alphabet, etc. by a certain rule of replacement, etc. *1 The Numbers Act stipulates that the person in charge of processes using individual numbers, etc. and the person engaged in processes using individual numbers, etc. must not create a specific personal information file beyond the extent necessary for handling processes using individual numbers, etc. Therefore, when an individual number is stated in an inquiry document, etc. received through tax investigation, the individual number must be deleted or disposed of immediately after the utilization purpose is achieved, regardless of whether the individual number is for an existing customer or not. *2 Since April 2020, an account management institution has been required under the General Act of National Taxes to manage subscriber information in a state of being searchable by an individual number. However, under the Numbers Act, it is prohibited to use an individual number as customer number for customer management. [Reference provisions, etc.] Article 2 of the Number Act, 1-(1) of the Numbers Act, Finance GL, 2-4 of the General Rules, Article 74-13-3 of the General Rules for National Taxes

Guidelines for Protection of Personal Information	Explanations
(3) Personal Data This term refers to Personal Information constituting a Personal Information Database, etc.	3. Personal Data (Item 3) (1) Examples falling under the category of "Personal Data" For example, the following may fall under this category. (i) Personal Information downloaded from a Personal Information Database, etc. to a recording medium (ii) Information output from a Personal Information Database, etc. on paper (including copies thereof) (iii) In the case where a paper-based application form for opening a transaction account or a customer card, etc. prior to data entry is searchable in Japanese alphabetical order or account number order (falling under the category of "Personal Information Database, etc."), Personal Information constituting the Personal Information Database, etc. (iv) In the case where even if the data has been processed by deleting "names" or any other means so that a third party cannot identify a specific individual from the data, specific Personal Information can be identified by comparing with other information and specific Personal Information can be easily retrieved from a Full Member's perspective (falling under the category of "Personal Information Database, etc."), Personal Information constituting the Personal Information Database, etc. (2) Examples not falling under the category of "Personal Data" For example, in the case where a paper-based application form for opening a transaction account or a customer card, etc. prior to data entry is not in a state of being searchable in Japanese alphabetical order or account number order, etc., Personal Information contained therein does not fall under the category. [Reference provisions, etc.] Article 2 of the Protection Act, 2-6 of the General Rules
(4) Personal Information Handling Business Operators This term refers to a person providing a Personal Information Database, etc. for use in business; however, excluding central government organizations, local governments, incorporated administrative agencies, etc. set forth by the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003), and local incorporated administrative agencies set forth by the Local Incorporate Administrative Agencies Act (Act No. 118 of 2003). The term "business" used herein in reference to "for use in business" means similar acts that are repeatedly and continuously carried out for a certain purpose and deemed to be business under normal social conventions, whether for profit or non-profit. In addition, any person providing a Personal	[Reference provisions, etc.]Article 2 of the Protection Act, 2-5 of the General Rules GL

Guidelines for Protection of Personal Information	Explanations
Information Database, etc. for use in business is deemed to be a Personal Information Handling Business Operator, regardless of the number of specific individuals identified by Personal Information constituting the Personal Information Database, etc. Even a non-juridical association (voluntary organization) or an individual with no capacity of right shall be deemed to be a Personal Information Handling Business Operator if the association or individual provides a Personal Information Database, etc. for use in business.	
(5) Principal The term refers to a specific person identified by Personal Information.	[Reference provisions, etc.] Article 2 of the Protection Act
(6) Retained Personal Data This term refers to any Personal Data for which a Full Member has all authority to disclose, correct, add to or delete from the contents, to discontinue use, to erase, or to discontinue provision to any third party at the request of a Principal or his/her representative, other than the following Personal Data.	4. Retained Personal Data (Item 6) (1) Examples of "Retained Personal Data" For example, the following may fall under this category. (i) Personal information constituting Personal Information Database, etc. internally prepared and processed (database on the company's customers, etc., or documents and books thereof) (ii) When a Full Member itself has authority to respond to all requests for disclosure, correction, addition or deletion, cessation, elimination, and cessation of provision to a third party (referred to as "authority for disclosure, etc." in (2)) for a database created and possessed by combining external data such as corporate data with data within the Full Member, the data falls under the category of "Retained Personal Data." (2) Examples not falling under the category of "Retained Personal Data" For example, a database, etc. obtained by a Full Member from an outsourcer in the case of handling Personal Data as outsourced service, and for which a Full Member itself has no authority for disclosure, etc. does not fall under the category. [Reference provisions, etc.] Article 2 of the Protection Act, 2-7 of the General Rules
(a) Personal Data that are likely to harm the life, body, or property of a Principal or a third party if their presence or absence is made known (b) Personal Data that are likely to promote or induce illegal or unjust acts if their presence or absence is made known	(3) Specific Examples of "Personal Data that are likely to promote or induce illegal or unjust acts if their presence or absence is made known" (Item 6 (b)) (i) Cases where a Full Member holds Personal Data of an organized crime group, so-called "sokaiya" (corporate racketeer), an antisocial organization or its members, etc. for the purpose of preventing acts of unreasonable demand or otherwise examining the commencement of transactions (ii) Cases where a Full Member holds Personal Data of a person who repeats such acts of unreasonable demands in order to prevent such acts from so-called suspicious persons, malicious claimants, etc. [Reference provisions, etc.] Article 2 of the Protection Act, 2-7 of the General Rules

Guidelines for Protection of Personal Information	Explanations
(c) Personal Data that are likely to impair the safety of Japan, impair trust relationship with other countries or international organizations, or suffer disadvantages in negotiations with other countries or international organizations if their presence or absence is made known	(4) Specific examples of "Personal Data that are likely to impair the safety of Japan, impair trust relationship with other countries or international organizations, or suffer disadvantages in negotiations with other countries or international organizations if their presence or absence is made known" (Item 6 (c)) For example, information on schedule of VIPs' activities [Reference provisions, etc.] Article 2 of the Protection Act, 2-7 of the General Rules
(d) Personal Data that are likely to interfere with the prevention, suppression, or investigation of crimes or the maintenance of public safety and order if their presence or absence is made known	(5) Specific examples of "Personal Data that are likely to interfere with the prevention, suppression, or investigation of crimes or the maintenance of public safety and order if their presence or absence is made known" (Item 6 (d)) (i) Cases where a Full Member holds Personal Data of suspect, etc. in the course of receiving and replying to inquiries from the police regarding matters related to investigations (ii) Information subject to notification of transactions that are suspected to relate to criminal proceeds (suspicious transactions) (iii) Information on an account used for a bank transfer fraud [Reference provisions, etc.] Article 2 of the Protection Act, Article 4 and Article 5 of the Enforcement Order, 2-7 of the General Rules
(e) Personal data to be deleted (except for renewal) within six (6) months	[Reference provisions, etc.] Article 2 of the Protection Act, 2-7 of the General Rules
(7) Special Care-required Personal Information The term refers to Personal Information comprising certain descriptions, etc. as those whose handling requires special care so as not to cause unfair discrimination, prejudice, or other disadvantages.	5. Special Care-required Personal Information (Item 7) Specific examples of information falling under the category of Special Care-required Personal Information (1) Race (2) Creed (3) Social status (4) Medical history (5) Criminal background (6) Fact that a person has been damaged by crime (7) Fact that a person has a physical disability, an intellectual disability, a mental disability (including a developmental disability), or any other physical or mental disability stipulated by the Enforcement Rules (8) Results of medical checkups or other inspections for prevention and early detection of diseases conducted by physicians or other persons engaged in healthcare-related duties for a Principal (9) Fact that based on results of medical checkups, etc., or on the grounds of sickness, injury, or other mental or physical change, guidance or medical treatment or prescription for improving the mental or physical condition of a Principal has been provided by a physician, etc. (10) Fact that arrest, search, seizure, detention, institution of prosecution, or any other proceeding in connection with a criminal case has been taken

Guidelines for Protection of Personal Information	Explanations
	with a Principal as the suspect or defendant (11) Fact that investigation, protective measures, adjudication, protective measures, or any other proceedings relating to a case for the protection of a juvenile have been taken for a Principal as a juvenile prescribed in Article 3, Paragraph 1 of the Juvenile Act or a person suspected of being such a juvenile [Reference provisions, etc.] Article 2 of the Protection Act, 2-3 of the General Rules
(8) Sensitive Information In the finance sector, this term refers to Special Care-required Personal Information and information relating to individuals' membership in a labor union, family origin, registered domicile, healthcare, and sex life (among these, excluding the matters falling under the category of the Special Care-required Personal Information) (excluding any information made public by the Principal or by a national government organ, local public entity, or any of those set forth in the items of Article 76, Paragraph 1 of the Protection Act, or the items of Article 6 of the Enforcement Rules, or seemingly clear information acquired by visual observation, filming, or photographing of the Principal).	6. Sensitive Information (Item 8) It should be noted that any information made public by the Principal or by a national government organ, local public entity, or any of those set forth in the items of Article 76, Paragraph 1 of the Protection Act, or the items of Article 6 of the Enforcement Rules, or seemingly clear information acquired by visual observation, filming, or photographing of the Principal shall not be included in Sensitive Information even if such information falls under the category of Special Care-required Personal Information under laws and regulations. [Reference provisions, etc.] Article 5 of the Finance Sector GL
(9) Anonymously Processed Information This term refers to Information Relating to an Individual that can be produced from processing Personal Information so as to neither be able to identify a specific individual by taking action prescribed in accordance with the divisions of Personal Information nor be able to restore the Personal Information.	7. Anonymously Processed Information (Item 9) (1) The following information is considered to fall under the category of Anonymously Processed Information. (i) In the case of Personal Information that is "those containing a name, date of birth, or other descriptions, etc. whereby a specific individual can be identified (including those that can be readily collated with other information and thereby identify a specific individual)," information generated by deleting a name, date of birth, or other descriptions, etc. contained from the Personal Information so that a specific individual cannot be identified (ii) In the case of Personal Information that "contains a Personal Identification Code," information from which all Personal Identification Codes included in the Personal Information are deleted so that a specific individual cannot be identified * "Can identify a specific individual" refers to a state that can be judged so under social conventions from the information alone or those stored by combining multiple pieces of information, and depends on whether it can be concluded that identity between a specific living person and information is recognized with a common person's judgment or understanding. (2) When Anonymously Processed Information is created, it is necessary to take actions in accordance with the Protection Act and the Anonymous Processing GL. "Anonymously Processed Information is created" refers to

Guidelines for Protection of Personal Information	Explanations
	creating such information to be handled as Anonymously Processed Information. For example, cases where information continues to be handled as Personal Information after some Personal Information such as name is deleted (or replaced by other descriptions, etc.) as part of security control action (including cases where original Personal Information is restored) or where Personal Information is processed to create statistical information, or other cases do not fall under the category of "Anonymously Processed Information is created." [Reference provisions, etc.] Article 2 of Protection Act, 2-8 of the General Rules, 2-1 of the Anonymous Processing GL
Article 3. Specification of Purpose of Use 1. A Full Member must, in handling Personal Information, specify in what kind of business the Personal Information is provided for use and for what purpose it is used as explicitly as possible so that the Principal can reasonably anticipate them. 2. When a utilization purpose in the preceding paragraph is specified, abstract expressions such as "to be used for a purpose required by the company" are not considered to satisfy the requirement of "as explicitly as possible." Therefore, a Full Member must make efforts to specify the utilization purpose by indicating the financial instruments or services to be provided. 3. When utilization purposes of specific Personal Information are limited by laws and regulations, etc., a Full Member is to clearly indicate that fact. 4. A Full Member must, in case of altering utilization purpose, not do so beyond "the scope recognized reasonably relevant to the pre-altered utilization purpose" stipulated in Article 15, Paragraph 2 of the Protection Act.	1. If provision of Personal Information to a third party is assumed in advance when identifying the utilization purpose, a Full Member needs to specify the purpose so that the fact is clearly understood. 2. Examples of specifying a utilization purpose Each Full Member shall specify a purpose of utilizing Personal Information by reference to the following examples. (1) Business details (optional matter) The description of business details shall be at the discretion of each company, and in the case where they are described, the following examples shall be referred to. (i) Business operations set forth in Article 2, Paragraph 8, Item 12, (a) of the FIEA or business operations set forth in Item 14 of the said paragraph and business operations incidental thereto (in the case of a trust company, etc. which is the trustee company of an investment trust managed without instructions from the settlor, trust business, and business operations incidental thereto) (ii) Business operations stipulated in Article 2, Paragraph 8, Item 7 of the FIEA (iii) Business operations that a Full Member may engage in under Article 35, Paragraph 2 of the FIEA and business operations incidental thereto (iv) Any other business operations that a Full Member may engage in and business operations incidental thereto (including any business operations that may be permitted in the future) (2) Utilization purpose (required matter) For example, a utilization purpose shall be concretely specified as follows. It is also possible to describe the purpose of utilizing individual numbers. In this case, make sure that customers can clearly understand that the utilization purpose is independent of the purpose of utilizing other Personal Information. (i) To solicit, sell, or offer services for securities issued by the company (ii) To judge the appropriateness of provision of goods and services in light of the principle of

Guidelines for Protection of Personal Information	Explanations
	suitability, etc. (iii) To receive applications for securities or services such as opening transaction accounts, etc. (iv) To confirm that the person is a customer, the Principal, or a representative of the Principal (v) To report the transaction results, balance, etc. to customers (vi) To perform clerical work for transactions with customers (vii) To exercise rights and perform obligations under contracts with customers or laws, etc. (viii) To conduct market research, and research and development of financial products and services through data analysis, questionnaires, etc. (ix) To appropriately perform entrusted work in the case where a whole or part of administration work for Personal Information is entrusted by an investment corporation to the company as a trustee for general administration work, and other cases (x) Otherwise to perform transactions with customers properly and smoothly ● Purpose of utilizing individual number Regardless of the purpose of utilizing Personal Information in any of the preceding items, an individual number shall be used solely for "clerical work for application and notification for opening an account for financial Instruments transaction" and "clerical work for preparation and submission of legal documents related to financial instruments transactions." * In the case of notifying, publicizing, or clearly showing the purpose of utilizing individual numbers separately from the purpose of utilizing Personal Information, it is necessary to clearly indicate to the customer that the purpose of utilizing Personal Information has been notified, publicized, or clearly shown separately and then take care not to make any omission in notifying, publicizing, or clearly showing the respective utilization purposes. For example, it is possible to describe the purpose of utilizing individual number as follows. ● Purpose of utilizing individual number (i) Clerical work for application and notification for account opening for financial instruments transactions (ii) Clerical work for preparation and submission of legal documents relating to financial instruments transactions * Please check the purpose of utilizing Personal Information other than personal number, which has been made public on our website, etc. 3. Scope of change of a utilization purpose (Examples of acceptable cases) "Send product information, etc. by mail" → "Send product information, etc. via e-mail" (Examples of unacceptable cases) "Used for tabulation of questionnaire" → "Used

Guidelines for Protection of Personal Information	Explanations
	for mailing of product information, etc." [Reference provisions, etc.] Article 15 of the Protection Act, Article 2 of the Finance Sector GL, 1 - (1) of the Numbers Act, Finance GL, 3-1-1 and 3-1-2 of the General Rules GL
Article 4. Format of Consent When obtaining the consent of a Principal specified in the next article, Article 13 and Article 13-2, a Full Member is to do so in writing (including an electromagnetic record; the same shall apply hereinafter) in principle. In the case where the Principal is a minor, adult ward, person under curatorship, or person under assistance and does not have the ability to judge results of the consent to the handling of Personal Information, and other cases, consent must be obtained from a person with parental authority or legal representative, etc.	(1) Specific examples of methods to obtain "consent" (i) Method to obtain consent by stating a utilization purpose and consent wording on a written document with which Personal Information is obtained directly from the Principal or on another written document and requiring a Principal's signature (and seal) (ii) In the case of the Internet, etc., method through reception of intercommunication using electric communication lines such as e-mail, SMS, etc. from a Principal with indication of intention to give consent on the screen (such as clicking of an approval button by a Principal, touching a touch panel to indicate consent, and input using a button, switch, etc.) or consent wording stated on it (hereinafter referred to as "e-mail, etc."), voice entry by a Principal, and other means (iii) In the case of non-face-to-face communication, such as telephone calls, other than (i) and (ii) above, when consent is obtained orally, it is necessary to establish a system in which indication of a customer's intention to consent can be verified subsequently by making internal records (listening sheets, etc.) or recording voice, etc. (2) Matters to be noted in the case of using a written consent that is prepared in advance It is desirable that a Principal understand provisions regarding handling of Personal Information that are clearly separated from others by changing the size of letters and expression of sentences, etc. Alternatively, it is desirable to check consent in such a way that the intention of a Principal can be clearly reflected, for example, by providing a confirmation field in a written consent document that is prepared in advance and allowing the Principal to check the consent. (3) In the case where a Principal is a minor, it is considered that consent of a person with parental authority is necessary when the minor does not have the ability to judge the result of his or her consent regarding handling of Personal Information. [Reference provisions, etc.] 2-12 of the General Rules GL, Article 3 of the Finance Sector GL
Article 5. Restriction due to a Utilization Purpose 1. A Full Member must not handle Personal Information without obtaining in advance a Principal's consent beyond the necessary scope to achieve a utilization purpose specified in Article 3. However, use of Personal Information (such as	(1) When a Full Member uses Personal Information that has already been obtained in connection with business operations to be newly handled, the Personal Information is considered to be within the scope necessary to achieve a utilization

Guidelines for Protection of Personal Information	Explanations
sending an e-mail or making a telephone call) to obtain a Principal's consent in advance shall not be deemed as a utilization for unintended purposes even if it is not included the utilization purposes as originally specified.	purpose specified in Article 3, unless these business operations are deviated from "any other business operations that a Full Member may engage in and business operations incidental thereto (including any business operations that may be permitted in the future)" specified in the utilization purpose. [Reference provisions, etc.] Article 16 of the Protection Act, 3-1-3 of the General Rules GL
2. A Full Member must, in case of having acquired Personal Information as a result of succession of a business from another Personal Information Handling Business Operator because of a merger or other reason, not handle the Personal Information without obtaining in advance a Principal's consent beyond the necessary scope to achieve the pre-succession utilization purpose of the said Personal Information. In addition, when personal information is handled within the necessary scope to achieve the pre-succession utilization purpose, it shall not be deemed as a utilization for unintended purposes, and a Principal's consent does not need to be obtained.	(2) Under the category of "merger or other reason" (Paragraph 2), in addition to a merger, generally business succession in which Personal Data, such as customer information, related to the business are generally also taken over as a whole, including business transfer, contribution in kind of business, and company split, etc., fall. After the business succession, when handling Personal Information beyond the scope necessary to achieve the utilization purpose before the business succession, it is necessary to obtain consent of a Principal in advance. However, even if the use of Personal Information to obtain the consent (such as sending e-mails and making telephone calls) is not stated as the utilization purpose before the succession of business, such use of Personal Information shall not be regarded as use for any purpose other than the original intent. (3) It should be noted that, in principle, individual number may not be used for any purpose other than the original intent even if consent of the Principal is obtained. [Reference provisions, etc.] Article 16 of the Protection Act, 3-1-4 of the General Rules GL, Article 9, and Article 30, Paragraph 3 of the Numbers Act and 1 - (1) of the Numbers Act, Finance GL
3. The preceding two paragraphs shall not apply to any of the following cases.	(4) Notwithstanding any of the items set forth in Paragraph 3, individual numbers may be handled exceptionally only in the following cases. (i) Cases in which a financial institution pays money at the time of serious disaster, etc. (ii) Cases in which there is a need to protect a human life, body, or property, and when the Principal has given consent or it is difficult to obtain a Principal's consent [Reference provisions, etc.] Article 16 of the Protection Act, Article 9 of the Numbers Act, 1 - (1) of the Numbers Act, Finance GL
(1) Cases based on laws and regulations	(5) Specific examples of "cases based on laws and regulations" (Paragraph 3, Item 1) For example, the following may fall under this category. (i) Article 74-2 through Article 74-6 of the Act on General Rules for National Taxes (Questioning and Inspection by Tax Authorities) (ii) Article 1 of the National Tax Violations Control Act (Voluntary Investigation of Criminal Cases by

Guidelines for Protection of Personal Information	Explanations
	Collecting Officials or Tax Collectors) (iii) Article 197 of the Code of Criminal Procedure (Inquiry for Matters Related to Investigation) (iv) Article 8, Paragraph 1 of the Act on Prevention of Transfer of Proceeds from Crime (hereinafter referred to as the "Crime Proceeds Transfer Prevention Act") (Notification of Suspicious Transactions, etc.) (v) Article 223 of the Code of Civil Procedure (Order to Submit Documents) (vi) Article 218, Paragraph 1 of the Code of Criminal Procedure (Seizure, Search and Inspection by Warrant) (vii) Article 225 of the Income Tax Act (Payment Record and Notice of Payment) (viii) Article 72-63 of the Local Tax Act (Right of Employees of the Ministry of Internal Affairs and Communications to Ask Questions and Make Inspection Pertaining to Individual Business Tax); (ix) Article 141 of the National Tax Collection Act (Questioning and Inspection) (x) Article 10-6 of the Act on Special Provisions, etc. of the Income Tax Act, the Corporation Tax Act, and the Local Tax Act Incidental to Enforcement of Tax Treaties, etc. (Report of Account Information Pertaining to Automatic Information Exchange System based on the Common Reporting Standards (CRS)) (xi) Article 56-2, Article 210, and Article 211 of the FIEA (Collection and Inspection of Report, Questioning, Inspection, Retention, etc., Visit, Search, Seizure, etc.) (xii) Article 78, Paragraph 2, Article 78, Paragraph 6, and Article 78, Paragraph 7 of the FIEA * Provision of information to self-regulating organizations under the FIEA, etc. Cases where a Full Member provides Personal Information to the Association in order to carry out the Association's self-regulation related services, such as reporting and notification to the Association, investigation by the Association or complaint consultation and mediation business by the Association, etc. under the provisions of the Articles of Incorporation and other rules of the Association, which have been established in accordance with the FIEA, etc. (xiii) Article 23-2, Paragraph 2 of the Attorney Act (Inquiries from Bar Associations) For example, cases where it becomes necessary as evidential material to be submitted to a court, etc. It should be noted that although the relevant laws and regulations have a provision stating that a third party may request provision of Personal Information, when a Full Member is allowed not to respond to the request for a justifiable reason, the Full Member shall respond within the scope of the necessity and

Guidelines for Protection of Personal Information	Explanations
	reasonableness of use for any purpose other than the original intention in light of the purport of the relevant laws and regulations. In this case, for example, as a response when an inquiry of a bar association is received, if it is difficult to judge whether the response is within the scope of the necessity and reasonableness of providing Personal Data, it is desirable to obtain the Principal's consent. [Reference provisions, etc.] Article 16 of the Protection Act, 3-1-5 of the General Rules GL
(2) Cases in which there is a need to protect a human life, body, or property, and when it is difficult to obtain a Principal's consent	(6) Specific examples of "cases in which there is a need to protect a human life, body, or property, and when it is difficult to obtain a Principal's consent" (Paragraph 3, Item 2) For example, "person" includes "corporation," and the following may fall under this category. (i) Cases of collecting information on illegal activities of an organized crime group, so-called "sokaiya" (corporate racketeer), an antisocial organization or its members, etc., information on an account used for a bank transfer fraud, and other information (ii) Cases of making inquiries of the police about customers who are suspected to be antisocial forces (iii) Cases of providing information to medical institutions in order to deal with sudden illness of customers, etc. (iv) Cases of providing information to the police about a person who persistently and intentionally interferes with business (v) Assets disclosure to a family member of a Principal in a situation in which the Principal is missing due to an earthquake, disaster, etc. continues [Reference provisions, etc.] Article 16 of the Protection Act, 3-1-5 of the General Rules GL
(3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a Principal's consent	[Reference provisions, etc.] Article 16 of the Protection Act, 3-1-5 of the General Rules GL
(4) Cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a Principal's consent would interfere with the performance of the said affairs	(7) Specific examples of "cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a Principal's consent would interfere with the performance of the said affairs" (Paragraph 3, Item 4) For example, the following may fall under this category. (i) Cases of responding to voluntary investigation conducted by tax authorities from the perspective of achieving appropriate taxation without exercising individual rights to ask questions and investigate.

Guidelines for Protection of Personal Information	Explanations
	(Note) A Full Member individually judges whether or not "there is a need to cooperate." However, it is desirable that a Full Member accepts an "inquiry form for transactions of securities, etc." and other documents from tax authorities, identifies Personal Information subject to the inquiry, and then provides the relevant information. (ii) Cases of responding to voluntary investigation by police (iii) Cases of providing police with information on an account used for a bank transfer fraud (iv) Cases of replying to a general statistical survey It should be noted that a Full Member shall respond within the scope of the necessity and reasonableness of use for any purpose other than the original intention in light of the purport of the voluntary request. [Reference provisions] Article 16 of the Protection Act, Article 4 of the Finance Sector GL, 3-1-5 of the General Rules GL
Article 6. Handling of Sensitive Information 1. A Full Member shall not acquire, use, or provide to a third party any Sensitive Information, except for the following cases.	(1) Examples of information not falling under the category of Sensitive Information For example, the following does not fall under the category. (i) Publicly known information stated in newspapers, television programs, official gazettes, etc. (ii) Information on "nationality (including the existence of permanent residence)" in the case of using the "nationality" in order to confirm the governing law in the performance of inheritance and tax obligations (2) Matters to be noted regarding Sensitive Information (i) The timing for acquiring Sensitive Information is the stage at which a Full Member stores the information as information used for business purposes by binding it to a file or other means. (ii) When a copy of a driver's license stating registered address, conditions of the license, etc. (limited to those where the content of the conditions, etc. falls under the category of Sensitive Information) is received as an identification document from a customer in order to identify the customer under the Crime Proceeds Transfer Prevention Act, etc. on and after April 1, 2005, if the registered address, conditions of the license, etc. are blacked out swiftly before filing (storing), this is not regarded as "acquisition" of Sensitive Information. In addition, it should be noted that information regarding intention to donate organs, etc. (including special columns), which is not necessary for identification confirmation, shall not be acquired from the back of a driver's license, the face of an individual number card, a health insurance card, and others, regardless of whether it is Sensitive Information, because such

Guidelines for Protection of Personal Information	Explanations
	information is not necessary for operation and direct public offering services, etc. It should be noted that Sensitive Information acquired prior to April 1, 2005 may not be used or provided to any third party on and after the said date, except in the cases set forth in each item of Paragraph 1 of this article. It should also be noted that any Special Care-required Personal Information acquired prior to May 30, 2017 (excluding Sensitive Information prior to May 30, 2017) may not be used or provided to any third party after May 30, 2017 except in the cases set forth in the items of Paragraph 1 of this Article.
(1) Cases based on laws and regulations, etc.	(3) Specific examples of "cases based on laws and regulations, etc." (Paragraph 1, Item 1) In addition to laws, government ordinances, ordinances, and treaties, with regard to guidance documents issued by cabinet decision or a public office, for example, the following may fall under this category. (i) Cases of receiving a physical disability certificate (copy) from a customer in order to check his or her qualification to use the "tax-free small-sum savings system for people with disabilities." (ii) Cases of acquiring information on the antisocial activities of an organized crime group, an antisocial organization or its members described in documents and others at a meeting, etc. of the Organized Crime Group Expulsion Campaign Promotion Center under the Act on the Prevention of Unjust Acts by Organized Crime Group Members (iii) Cases of providing Personal Information through notification of suspicious transactions under Article 8, Paragraph 1 of the Crime Proceeds Transfer Prevention Act
(2) Cases in which there is a need to protect a human life, body, or property	(4) Specific examples of "cases in which there is a need to protect a human life, body, or property" (Paragraph 1, Item 2) (i) Cases of acquiring criminal information for the purpose of identifying an organized crime group, so-called "sokaiya" (corporate racketeer), an antisocial organization or its members, etc. (ii) Cases where a Full Member obtains information on sickness such as dementia from a family member or the like of a customer whose decision-making ability has deteriorated on behalf of the customer, when the Full Member confirms conformity of the customer [Reference provisions, etc.] Article 17, Paragraph 2, Item 2 of the Protection Act
(3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children	

Guidelines for Protection of Personal Information	Explanations
(4) Cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations	
(5) Cases in which there is a need to acquire, use, or provide to a third party any Sensitive Information of its employees, etc. concerning their affiliation to or membership in a political or religious group or labor union within the scope necessary for the performance of affairs relating to withholding taxes, etc.	
(6) Cases in which any Sensitive Information is acquired, used, or provided to a third party to the extent necessary for performing the transfer of rights and obligations arising from inheritance procedures	(5) Specific examples of cases in which any Sensitive Information is acquired, used, or provided to a third party to the extent necessary for performing the transfer of rights and obligations arising from inheritance procedures (Paragraph 1, Item 6) For example, cases of obtaining a copy of a family register for inheritance proceedings [Reference provisions, etc.] Article 5 of the Finance Sector GL
(7) Cases in which a Full Member acquires, uses, or provides to a third party any Sensitive Information based on the consent of a Principal to the extent necessary for performing its services from the necessity to ensure appropriate operation of its businesses run by the Full Member	
(8) Cases in which biometric information, which falls under the category of Sensitive Information, is used based on a Principal's consent for the purpose of identity verification	(6) "Biometric information" refers to an example of a Personal Identification Code (1) in Explanation 1-2 of Article 2.
2. When a Full Member acquires, uses, or provides to a third party any Sensitive Information in the case set forth in the preceding paragraph, the Full Member shall handle the information with extreme caution so as to avoid acquisition, use, or provision to a third party of the information beyond the grounds set forth in the same paragraph.	
3. When a Full Member acquires, uses, or provides to a third party any Sensitive Information in the cases set forth in Paragraph 1 of this article, the Full Member must make a response appropriately in accordance with Laws and Regulations on Protection of Personal Information.	(7) It should be noted that, for example, in acquiring Special Care-required Personal Information, consent of the Principal shall be obtained in advance in accordance with Article 17, Paragraph 2 of the Protection Act.
4. Article 23, Paragraph 2 of the Protection Act (opt-out provision) is not to apply to the case where a Full Member provides Sensitive Information to a third party.	(8) Since provision of Special Care-required Personal Information to third parties through opt-out is prohibited by the Protection Act, any Sensitive Information that does not fall under the category of special care-required Personal Information also is not to be provided to a third party through opt-out.
Article 7. Proper Acquisition of Personal Information 1. A Full Member must not acquire Personal Information by deceit or other improper means. In addition, a Full Member must not unjustifiably infringe interests of a Principal in acquiring Personal Information from a third party.	(1) Cases where Personal Information has been obtained by "improper means" For example, the following may fall under this category. (i) Cases of acquiring Personal Information of a family member, such as income situation of family, which is not relevant in consideration of the acquisition circumstance from a child or a

Guidelines for Protection of Personal Information	Explanations
	person with a disability who does not have adequate judgment ability, without consent of the family member. (ii) Cases of acquiring Personal Information by forcing someone into the violation of the restriction of provision to a third party stipulated in Article 23, Paragraph 1 of the Protection Act (iii) Cases of acquiring Personal Information from a Principal by intentionally showing false information as to the entity acquiring personal Information, utilization purpose, etc. (iv) Cases of acquiring Personal Information from other business operators by instructing the other business operators to obtain the Personal Information through improper means (v) Cases of acquiring Personal Information despite knowing or being able to know easily that violation of the restriction of provision to a third party prescribed in Article 23, Paragraph 1 of the Protection Act is being committed (vi) Cases of acquiring Personal Information despite knowing or being able to know easily that the Personal Information has been acquired by improper means (2) Acquisition of individual number and basic pension number It should be noted that individual number and basic pension number must not be obtained other than in cases specified by laws and regulations (* 1). From May 25, 2020, the notification card for confirming individual number has been abolished, but a transitional measure has been taken, and the card may be used for identification under the Numbers Act only when the following conditions are satisfied (pursuant to the partial enforcement of the "Act for Partial Revision of the Act on Use of Information and Communications Technology in Administrative Procedures, etc. for Improving the Convenience for Persons Concerned in Administrative Procedures, etc. through Use of Information and Communications Technology and Simplifying and Streamlining Administrative Operations"). (i) There is no change to matters described on the notification card. However, in the case where there is any change to matters described on the notification card before the date of abolishment, if measures to change matters to be described on the notification card have not been taken by the mayor of the municipality (including the mayor of a special ward), the transitional measures concerning the guidance for protection of Personal Information shall not apply. (ii) Confirmation is to be made that matters described on a notification card are present information, by the method specified by the Numbers Act such as receiving identification

Guidelines for Protection of Personal Information	Explanations
	documents separately. * 1. It should be also noted that in addition to individual number, any request to disclose basic pension number, symbol, number, etc. for insured persons (meaning insurer number and number, symbol, number, etc. for insured persons; the same shall apply hereinafter) is prohibited in principle, even for the purpose of identity confirmation (the restriction on request for disclosure is imposed on symbol, number, etc. for insured persons on and after October 1, 2020 when the revised Health Insurance Act, etc. comes into effect). For example, in the case of requesting a copy of a health insurance card, etc. as an identification document on the website or leaflets, etc. for customers, if "Please confirm that the symbol or number is clearly shown." or other descriptions are presented on the website or leaflets, etc., this might be deemed as request for disclosure of number, symbol, number, etc. for insured persons. Therefore, a Full Member should refrain from providing such notification. [Reference provisions, etc.] Article 17 of the Protection Act, 3-2-1 of the General Rules GL, Articles 15, 16, 19 and 20 of the Numbers Act, 3-(2) and 3-(3) of the General Rules GL, Article 108-4 of the National Pension Act, Article 194-2 of the Health Insurance Act, Article 161-2 of the Act on Assurance of Medical Care for Elderly People, Article 111-2 of the National Health Insurance Act, Article 143-2 of the Mariners Insurance Act, Article 45 of the Private School Personnel Mutual Aid Act, Article 112-2 of the National Public Officers Mutual Aid Association Act, Article 144-24-2 of the Act on Mutual Aid Association for Local Public Officers, Article 74-13-4 of the Act on General Rules for National Taxes, Article 8 of the Act on Improvement in Method of Number Use (Act No. 28 of 2013)
2. When acquiring Personal Information through provision from a third party, a Full Member shall confirm the status of compliance with laws and regulations of the provider and also confirm that the Personal Information has been lawfully acquired.	(3) Specific method to confirm the status of compliance of a provider For example, confirmation for opt-out, the utilization purpose, and disclosure procedures, and that contact information for receiving inquiries and complaints, and other matters are possible. (4) For example, the fact that "Personal Information to be provided has been obtained legally" is confirmed by any of the following methods. (i) Inspection of documents such as contracts showing the process of acquisition, etc. (ii) Acceptance of confirmation stating that the information has been obtained legally (iii) Oral confirmation of legality and proper preservation of internal records If it cannot be confirmed that Personal Information to be provided has been legally obtained, it is desirable to consider a prudent response, including voluntary restraint of the acquisition. [Reference provisions, etc.]3-2-1 of the General Rule

Guidelines for Protection of Personal Information	Explanations
	GL (*) With regard to Personal Data transferred from the European Economic Area (EEA) based on an adequacy decision under Article 45 of the Regulation of the European Parliament and of the Council on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95-46-EC (General Data Protection Regulation: hereinafter referred to as the "GDPR") (meaning "Personal Data" set forth in Article 4, Item 1 of the GDRP), it should be noted such Personal Data are subject to application of the complementary rules. [Reference provisions, etc.] Complementary Rules
Article 8. Notification, Public Disclosure, Clear Indication, etc. of a Utilization Purpose When Acquiring Personal Information 1. A Full Member must, in case of having acquired Personal Information except in cases where a utilization purpose has been disclosed in advance to the public, promptly inform a Principal of, or disclose to the public, the utilization purpose. In this case, the method to "inform" is to be in writing, in principle, and as for the method to "disclose to the public," a Full Member must employ appropriate methods, such as making the relevant matters public on its website, etc. or posting or keeping the document at a counter of the head office or any other business office, etc., depending on the sales method of its financial instruments or other mode of business.	(1) Specific examples of the method to "Inform" For example, there are the following methods. (i) Notification by directly delivering documents such as leaflets (in principle) (ii) Notification given orally or through automatic answering machine, etc. (iii) Notification sent by e-mail,facsimile, etc. or notification by sending a document by mail, etc. (2) Specific examples of a method to "disclose to the public" For example, there are the following methods. (i) Posting at a place that can be accessed from the top page of the company's own website with one operation or so. (ii) Posting of posters, etc. and keeping and distribution of pamphlets, etc. at a place that customers are expected to visit, such as the company's business office (Note) With regard to Personal Information held prior to the date of enforcement of the Protection Act on April 1, 2005, there was no act of acquiring relevant Personal Information at the time of the enforcement of the Protection Act, and the provisions of Article 18 of the Protection Act shall not apply. [Reference provisions, etc.] 2-10, 2-11 of the General Rules GL
2. A Full Member must, notwithstanding the provisions of the preceding paragraph, in cases where it acquires the Principal's Personal Information stated in a written contract or other document as a result of conclusion of a contract with a Principal, state the utilization purpose explicitly to the said Principal in advance. This, however, shall not apply in cases where there is an urgent need to protect a human life, body, or property.	(3) Examples of "cases where it acquires Personal Information stated in a written contract or other document" from a Principal (Paragraph 2) For example, there are the following cases. (i) Cases of receiving an application form for transaction account setup or an application form for brokerage to a custodian company, etc. from a Principal (ii) Cases of receiving identification documents or copies thereof from a Principal (iii) Cases of directly obtaining Personal Information stated in a reply card or questionnaire from a Principal (iv) Cases of obtaining Personal Information that a person wishing to participate in a campaign

Guidelines for Protection of Personal Information	Explanations
	sponsored by the company entered on the input screen of the company's website to apply for the participation (4) Specific examples of "clear indication" method For example, there are the following methods. (i) Method of clearly indicating the matter on a document stating a utilization purpose (ii) Method of clearly indicating the matter by posting posters, etc. (iii) Method of clearly indicating the matter by distributing pamphlets or leaflets, etc. (iv) In the case of Internet transactions, method of clearly indicating the matter on the input screen for customers or by e-mail to customers (5) Content of "clear indication," etc. (i) The content to be "clearly indicated" is the purpose of utilizing Personal Information obtained. "Clear indication" shall be made either by indicating only the purpose of utilizing Personal Information stated in the contract or other documents, or by indicating all or part of the comprehensive utilization purpose specified in Article 3. (ii) In the case where the comprehensive utilization purpose is clearly indicated at the time of commencing a transaction, etc., when a purpose of utilizing Personal Information stated in the contract or any other documents is within the scope of the comprehensive utilization purpose that has been clearly indicated at the time of commencing a transaction, etc., it is not necessary to clearly indicate a utilization purpose again, each time the Personal Information in writing is obtained. (6) Specific examples of required notification or public disclosure to a Principal (excluding Cases where notification is to be given individually before acquisition) (i) Cases of obtaining Personal Information that has been voluntarily made public by a Principal on the Internet (excluding cases of merely browsing the Personal Information) (ii) Cases of obtaining Personal Information from the Internet, official gazettes, personnel records, etc. (excluding cases of merely browsing the Personal Information) (iii) Cases of receiving a third-party provision of Personal Information [Reference provisions, etc.]3-2-3 and 3-2-4 of the General Rules GL (7) Notification, public disclosure, and clear indication of the purpose of utilizing individual number (i) A Full Member must also make notification, public disclosure, and clear indication of the purpose of utilizing individual number. (ii) It is possible that notification, public disclosure, and clear indication of the purpose of utilizing individual number are made by adding the purpose to the purpose of utilizing Personal

Guidelines for Protection of Personal Information	Explanations
	Information. However, it is not precluded to make notification, public disclosure, and clear indication of the purpose of utilizing individual number separately from the purpose of utilizing Personal Information. (iii) When notification, public disclosure, and clear indication of the purpose of utilizing individual number is made by adding it to the purpose of utilizing Personal Information, make sure that customers can clearly understand that the purpose of utilizing individual number is independent from the purpose of utilizing other Personal Information. For example, the following descriptions are possible. ● Regardless of the above purpose of utilizing Personal Information, an individual number shall be used solely for "clerical work for application and notification for opening an account for financial Instruments transaction" and "clerical work for preparation and submission of legal documents related to financial instruments transactions." (iv) In the case of notifying, publicizing, or clearly showing the purpose of utilizing individual numbers separately from the purpose of utilizing Personal Information, it is necessary to clearly indicate to the customer that the purpose of utilizing Personal Information has been notified, publicized, or clearly shown separately and then take care not to make any omission in notifying, publicizing, or clearly showing the respective utilization purposes. For example, it is possible to describe the purpose of utilizing individual number as follows. ● Purpose of utilizing individual number 1) Clerical work for application and notification for account opening for financial instruments transactions 2) Clerical work for preparation and submission of legal documents relating to financial instruments transactions * Please check the purpose of utilizing Personal Information other than personal number, which has been made public on our website, etc. (v) When entrusting collection of individual numbers to a Financial Instruments Intermediary Service Provider, it should be noted that the utilization purpose to be clearly indicated by the Financial Instruments Intermediary Service Provider to customers is not the utilization purpose of the Financial Instruments Intermediary Service Provider itself but the utilization purpose stipulated by the entrusting Full Member.
3. A Full Member must, in case of altering a utilization purpose, inform a Principal of, or disclose to the public, the post-altered utilization purpose.	[Reference provisions, etc.] Article 18, Paragraph 3 of the Protection Act, 3-1-2 of the General Rules GL
4. The preceding three paragraphs shall not apply to any of the following cases. (1) Cases in which there is a possibility that informing a	(8) Specific examples of "cases in which there is a

Guidelines for Protection of Personal Information	Explanations
Principal of, or disclosing to the public, a utilization purpose would harm a Principal or third party's life, body, property, or other rights and interests	possibility that informing a Principal of, or disclosing to the public, the utilization purpose would harm a Principal or third party's life, body, property or other rights and interests" (Paragraph 4, Item 1) For example, cases where a provider of information on an organized crime group, so-called "sokaiya" (corporate racketeer), an antisocial organization or its members, etc., information subject to a report of suspicious transactions, information on an account used for bank transfer fraud, information on a malicious person who has interfered with business operations may cause a third party's unjustified resentment [Reference provisions, etc.] Article 18, Paragraph 4 of the Protection Act, 3-2-5 of the General Rules GL
(2) Cases in which there is a possibility that informing a Principal of, or disclosing to the public, a utilization purpose would harm the rights or legitimate interests of the Full Member	(9) Specific examples of "cases in which there is a possibility that informing a Principal of, or disclosing to the public, the utilization purpose would harm the rights or legitimate interests of the Full Member" (Paragraph 4, Item 2) For example, the following may fall under this category. (i) Cases where the revelation that a Full Member has acquired information on antisocial forces such as an organized crime group, information subject to a report of suspicious transactions, information on an account used for bank transfer fraud, information on a malicious person who has interfered with business operations causes harm to the Full Member that has received provision of information (ii) Cases where something related to company secrets such as the content of development of new products, etc. conducted by a Full Member and know-how on sales and marketing is revealed from notification or a utilization purpose made public, causing harm to healthy competition [Reference provisions, etc.] Article 18, Paragraph 4 of the Protection Act, 3-2-5 of the General Rules GL
(3) Cases in which there is a need to cooperate with a central government organization or a local government performing affairs prescribed by laws and regulations, and when there is a possibility that informing a Principal of, or disclosing to the public, a utilization purpose would interfere with the performance of the said affairs	(10) Specific examples of "cases in which there is a need to cooperate with a central government organization or a local government performing affairs prescribed by laws and regulations, and when there is a possibility that informing a Principal of, or disclosing to the public, the utilization purpose would interfere with the performance of the said affairs" (Paragraph 4, Item 3) For example, cases of receiving provided Personal Information on a suspect necessary for cooperation in an investigation from an investigation agency [Reference provisions, etc.] Article 18, Paragraph 4 of the Protection Act, 3-2-5 of the General Rules GL

Guidelines for Protection of Personal Information	Explanations
(4) Cases in which it can be recognized, judging from the acquisitional circumstances, that a utilization purpose is clear	(11) Specific examples of "cases in which it can be recognized, judging from the acquisitional circumstances, that a utilization purpose is clear" (Paragraph 4, Item 4) For example, the following may fall under this category. (i) Cases where information on the address and name provided by a requester in connection with a document request by phone, etc. is used solely for sending the requested document (ii) Cases of acquiring personal names, etc. of the representative person, officers, and employees in charge of a corporation through transactions with the corporation and using such Personal Information solely for these transactions (iii) Cases of acquiring Personal Information through exchange of business cards for future communications When sending direct mails or conducting solicitation activities, it is considered that the utilization purpose is clearly indicated by confirming the fact at the time of exchanging business cards or before sending direct mails. (iv) Cases of calling back at an incoming number that is not anonymous concerning the same matter [Reference provisions, etc.] Article 18, Paragraph 4 of the Protection Act, 3-2-5 of the General Rules GL, Article 6 of the Finance Sector GL
Article 9. Assurance, etc. about the Accuracy of Data Contents 1. A Full Member must endeavor to keep Personal Data accurate and up-to-date within the necessary scope to achieve the utilization purpose by establishing procedures for collation and confirmation at the time of inputting Personal Information into Personal Information Database, etc., establishing procedures for correction, etc. in the event of discovery of errors, etc., renewing record matters, setting a retention period, etc. It should be noted that it is not necessary to update the Personal Data held in a single uniform way or at all times, and it is sufficient to ensure accuracy and recency within the necessary scope in accordance with the respective utilization purposes. In addition, a Full Member must endeavor to delete Personal Data without delay when utilization of the data has become unnecessary, such as cases where the utilization purpose has been achieved and there is no longer reasonable reason to hold such Personal Data in relation to the purpose, and where the business constituting the premise for the purpose has been discontinued although the utilization purpose has not been achieved. However, this shall not apply to cases where the retention period, etc. is stipulated by laws and regulations.	(1) Specific examples of methods to "keep Personal Data accurate and up to date" Each Full Member shall endeavor to reflect the content of notification from customers promptly and accurately in a Personal Information Database, etc., and at the same time, make necessary responses, for example, by the following methods. (i) Disseminate procedures for notification of change of names, addresses, etc. of customers on documents delivered at the time of concluding contracts, transaction balance reports, etc., and websites. (ii) Inform the customer himself or herself of information on a customer card, etc. on a regular basis and request the customer to confirm the content thereof. * It should be noted that individual numbers shall not be described in any documents, etc. other than payment records, etc., because individual numbers may not be used beyond the scope of the utilization purpose. (2) "Retention period" The retention period also applies to permanent storage with reasonable reason. * It should be noted that individual numbers may be stored only if it is necessary to do clerical work specified in the Numbers Act, and must therefore be deleted and disposed of as soon as possible

Guidelines for Protection of Personal Information	Explanations
	when the retention period set forth in the applicable laws and regulations expires. [Reference provisions, etc.] Article 19 of the Protection Act, 3-3-1 of the General Rules GL, Article 7 of the Finance Sector GL, Article 20 of the Numbers Act, 3 - (3) of the Numbers Act, Finance GL
Article 10. Security Control Action 1. A Full Member must take necessary and appropriate action, such as establishment of basic policies and handling rules for security control and development of a system for security control measures, for the security control of Personal Data including preventing the leakage, loss, or damage of its handled Personal Data. In addition, necessary and appropriate action must include "Institutional Security Control Measures," "Human Security Control Measures," and "Technological Security Control Measures" in accordance with each stage of acquisition, utilization and preservation, etc. of Personal Data. These actions shall be those corresponding to risks arising from the scale and nature of the business, the handling status of Personal Data (including the size and volume of its handled Personal Data; the same shall apply hereinafter), the nature of the medium in which Personal Data is recorded and other factors, in consideration of the significance of infringement and rights and interests that may be suffered by the Principal in the event of a leakage, loss, or damage of Personal Data. 2. The definition of terms in this article is as follows. (1) Institutional Security Control Measures This term means measures for system development and actions to be taken by Full Member for security control of Personal Data, such as to clearly determine the responsibility and authority of each officer and employee (meaning persons engaging in the business of a Full Member within its organization under direct or indirect control and supervision of the Full Member, not limited to employees having an employment relationship (regular employees, contract employees, fixed-term employees, part-timers, and casual staff, etc.), but including those without an employment relationship with the Full Member (directors, accounting advisors (when an accounting advisor is a corporation, employees who are to perform the duties thereof), company auditors, executive officers, or temporary staff; the same shall apply hereinafter), establish and implement rules on security control, and inspect and audit the implementation status. (2) Human Security Control Measures This term means to conclude a non-disclosure contract with officers and employees and provide them with education and training, thereby supervising officers and employees so as to ensure security control of Personal Data. (3) Technological Security Control Measures	(1) A Full Member shall take appropriate measures in accordance with the size, content of businesses, etc. of the Full Member based on the Finance Sector GL and the Finance Sector Practical Guidelines, in order to prevent leakage, loss, or damage of Personal Data, and otherwise to ensure security control of Personal Data. (2) Specific examples of those corresponding to risks For example, a list that is available for purchase by many and unspecified people as needed at bookstores and has not been processed at all by a Full Member (line markers and sticky notes on the list does not constitute processing) is considered to be unlikely to infringe any right or interest of an individual. Therefore, even if such a list is disposed of without being processed by a document shredder or if such a list is collected, the list will not violate the Full Member's obligation to take security control measures. [Reference provisions, etc.] Article 20 of the Protection Act, Article 8 of the Finance Sector GL, Finance Sector Practical Guidelines, Article 12 of the Numbers Act)

Guidelines for Protection of Personal Information	Explanations
This term means technological measures concerning security control of Personal Data, such as to limit access to Personal Data and the information system handling such data, and to monitor that information system.	
3. A Full Member must take the following Institutional Security Control Measures for establishing basic policies and handling rules for security control of Personal Data. (1) Development of rules, etc. (a) Development of basic policies for security control of Personal Data (b) Development of handling rules for security control of Personal Data (c) Development of rules for inspection and audit of the handling status of Personal Data (d) Development of rules for outsourcing (2) Handling rules for safety control at each stage (a) Handling rules at the stage of acquisition and input of data (a) Handling rules at the stage of use and processing of data (a) Handling rules at the stage of preservation and retention of data (d) Handling rules at the stage of transfer and sending of data (e) Handling rules at the stage of deletion and disposal of data (f) Handling rules at the stage of responding to information leakage or other incidents 4. A Full Member must take the following Institutional Security Control Measures, Human Security Control Measures and Technological Security Control Measures for developing a system for security control of Personal Data. (1) Institutional Security Control Measures (a) Appointment of employees responsible for the management of Personal Data, etc. (a person responsible for Personal Data management who is the overall person in charge of execution of operations relating to security control of Personal Data, persons responsible for Personal Data management in each division handling Personal Data) (b) Development of security control actions in rules of employment, etc. (c) Operation in line with the handling rules for security control of Personal Data (d) Development of means to check the handling status of Personal Data (e) Development and implementation of a system for inspection and audit of the handling status of Personal Data (f) Development of a system for responding to information leakage or other incidents (2) Human Security Control Measures (a) Conclusion of a non-disclosure contract, etc. concerning Personal Data with officers and employees	(3) Specific examples of means to check the handling status of Personal Data (i) As for Personal Data, it is required to put in place a ledger containing the following matters. (a) Items to be obtained, (b) Utilization purpose, (c) Place of storage, method of storage, and storage life, (d) Department of administration, (e) Status of access authority (ii) On the other hand, as for specific Personal Information files, it is required to put in place a ledger (not to state any specific Personal Information) with the following matters serving as examples. (a) Type and name of the specific Personal Information file, (b) Responsible person, department in charge of handling, (c) Utilization purpose, (d) Status of deletion and disposal, (e) Person with access rights

Guidelines for Protection of Personal Information	Explanations
(b) Clarification of roles, responsibilities, etc. of officers and employees (c) Thorough dissemination of security control actions to officers and employees and their education and training (d) Checking of compliance with predetermined Personal Data management procedures by officers and employees (3) Technological Security Control Measures (a) Identification and authentication of Personal Data users (b) Setting of management categories of Personal Data and access control (c) Management of authority to access Personal Data (d) Measures to prevent the leakage, damage, etc. of Personal Data (e) Recording and analysis of access to Personal Data (f) Recording and analysis of operation of the information systems handling Personal Data (g) Monitoring and audit of the information system handling Personal Data	
	(4) It should be noted that some of Institutional Security Control Measures and Technological Security Control Measures are required to be put in place as "physical security control measures" under the Numbers Act, Finance GL. Specifically, the following measures may be taken. (i) Specific examples of control of areas where specific Personal Information, etc. is handled (a) In installation sites of a computer system, etc. storing a specific Personal Information file or an area where the specific Personal Information file can be taken out by writing it on an external storage medium, as controlled areas, entering and leaving management, restriction on devices brought, installation of surveillance cameras where needed, and other measures may be implemented. (b) Other than the above, in places where specific Personal Information, etc. is obtained and input to a computer system, or documents, etc. are temporarily stored, as handling areas, installation of walls or partitions, inventions on seating configuration, and other measures may be implemented. (ii) Specific examples of measures to prevent theft, etc. of equipment, electronic media, etc. In order to prevent theft or loss, etc. of equipment, electronic media, documents, etc. in areas where specific Personal Information files are handled, electronic media or documents, etc. shall be stored in lockable cabinets, folders, etc., and equipment shall be fixed using security wires, etc. (iii) Specific examples of measures to prevent leakage, etc. in the case of taking out electronic

Guidelines for Protection of Personal Information	Explanations
	media, etc. When electronic media or documents, etc. on which specific Personal Information, etc. are recorded are taken out, secure measures shall be taken, including encryption, protection using passwords, implementation of measures where individual numbers are not found out easily due to use of lockable transport containers, etc., and use of traceable transport means. (iv) Specific examples of deletion of individual numbers and disposal of equipment, electronic media, etc. When the retention period, etc. set forth in the applicable laws and regulations, etc. expires, individual numbers shall be deleted or disposed of by any means that cannot be restored as promptly as possible, and the record of such deletion or disposal shall be kept. In addition, when commissioning these works, a Full Member shall confirm with its contractor whether individual numbers have been surely deleted or disposed of by means of certificates, etc. (v) Specific examples of responses to tax inspections in and after April 2020 - In and after April 2020, while as part of a tax investigation using individual numbers, national tax authorities present reference documents, etc. containing individual numbers through research visit, the receipt of such reference documents, etc. (including copies thereof) shall be handled by the person managing handling clerical affairs relating to individual numbers, such as branch manager, or the person in charge of handling clerical affairs relating to individual numbers. In addition, the person managing handling clerical affairs relating to individual numbers, or the person in charge of handling clerical affairs relating to individual numbers shall forward the inquiry documents, etc. to a specific controlled area in each company, and shall check such inquiry documents, etc. with its own customer information and answer the inquiry, etc. to national tax authorities in the controlled area. - When an individual number is stated in an inquiry document, etc. received through forwarding from a branch office that received a research visit or by mail from national tax authorities, the individual number must be deleted or disposed of immediately after the utilization purpose is achieved, regardless of whether the individual number is for an existing customer or not. [Reference provisions, etc.] Article 20 of the Protection Act, 3-3-2 of the General Rules, Article 8 of the Finance Sector GL, Finance Sector Practical Guidelines

Guidelines for Protection of Personal Information	Explanations
Article 11. Supervision over Officers and Employees 1. A Full Member must, in having its officers and employees handle Personal Data, establish an appropriate internal management system and exercise necessary and appropriate supervision over the officers and employees so as to seek the security control of the Personal Data. The supervision shall correspond to risks arising from the nature of the business, the handling status of Personal Data and other factors, in consideration of the significance of infringement of rights and interests that may be suffered by the Principal in the event of a leakage, loss, or damage of Personal Data. 2. A Full Member is to exercise the "necessary and appropriate supervision" over the officers and employees in the preceding paragraph by establishing the following systems, etc. (1) To conclude a contract, etc. upon recruiting an officer or employee to ensure that the officer or employee will not disclose to a third party any Personal Data that the person has come to know in relation to businesses operated by the Full Member or use such data for unintended purposes while being employed and after resigning from the job (2) To clarify the roles and responsibilities of officers and employees through establishing handling rules to ensure proper handling of Personal Data, and thoroughly disseminate the obligation to ensure security control among its officers and employees and provide them with education and training (3) To develop a system for checking compliance of its officers and employees with the matters specified in internal security control rules and inspecting and auditing their attitudes toward the protection of Personal Data in order to prevent them from taking out any Personal Data.	(1) For the definition of officers and employees in this article, see Article 10, Paragraph 2, Item 1 of the Guidelines (2) Specific examples of cases where necessary and appropriate supervision has not been exercised over officers and employees (i) Cases where it is not confirmed that officers and employees are performing their duties in accordance with the rules for security control measures for Personal Data, and as a result, Personal Data are leaked (ii) Cases where any laptop computer or external recording medium containing Personal Data has been repeatedly taken out in violation of internal rules, etc. of the company, but the act has been neglected, and as a result, the personal computer or external recording medium is lost and Personal Data are leaked. [Reference provisions, etc.] Article 21 of the Protection Act, 3-3-3 of the General Rules GL, Article 9 of the Finance Sector GL, Finance Sector Practical Guidelines, Article 12 of the Numbers Act
Article 12. Supervision over Outsourcees 1. When a Full Member outsources the partial or entire handling of Personal Data (including the entirety of outsourcing contracts, irrespective of the form or type thereof, under which a Full Member has another entity carry out the whole or part of the handling of Personal Data), the Full Member must exercise necessary and appropriate supervision over the relevant outsourcee so as to ensure security control of the outsourced Personal Data. The supervision shall correspond to risks arising from the scale and nature of the outsourced business, the handling status of Personal Data and other factors, in consideration of the significance of infringement of rights and interests that may be suffered by the Principal in the event of a leakage, loss, or damage of Personal Data. 2. A Full Member must select an entity that is found to be properly handling Personal Data as an outsourcee and secure measures for security control of Personal Data also at that outsourcee so that security control measures are taken for the outsourced Personal Data (in the case where an outsourcee further outsources	(1) Outsourcees include foreign outsourcees. (2) It should be noted that when clerical affairs relating to individual numbers are outsourced, the same control as that of the outsourcer must be required. (3) In the case of sub-outsourcing and thereafter, it is necessary to require the equivalent control and to provide supervision appropriately. [Reference provisions, etc.] Article 22 of the Protection Act, Article 10 of the Finance Sector GL, Finance Sector Practical Guidelines, Article 11 of the Numbers Act, 2-(1) of the Numbers Act, Finance GL (4) It should be noted that, in the case of sub-outsourcing of clerical affairs relating to individual numbers, it is necessary to obtain permission from the original outsourcer. [Reference provisions, etc.] Article 10 of the Numbers Act, 2 - (1) of the Numbers Act, Finance GL (5) Specific examples of cases where necessary and appropriate supervision has not been exercised

Guidelines for Protection of Personal Information	Explanations
personal information-related duties, the Full Member shall also supervise whether the outsourcee sufficiently supervises the sub-outsourcees). Specifically, a Full Member must make the following responses, etc. for example. (1) Specify the requirements to develop an organizational system and establish basic policies and handling rules for security control as the criteria for selecting outsourcees and review those criteria regularly in order to ensure the security control of the Personal Data. When selecting an outsourcee, it is desirable that the Full Member checks the candidate's capabilities by visiting the place where Personal Data is handled, as necessary, or by other reasonable methods and has its person responsible for the management of Personal Data make an evaluation of the candidate appropriately. (2) Incorporate in an outsourcing contract specific security control actions that clarify the authority on the supervision and audit of and the collection of reports from the outsourcee, prohibition of the leakage of, stealing and alteration, and the utilization of Personal Data for unintended purposes by the outsourcee, conditions concerning sub-outsourcing and the responsibility of the outsourcee in the event of information leakage, etc., and at the same time, check the outsourcee's compliance with the security control actions incorporated in the outsourcing contract, regularly or as needed, and review those measures through conducting audits regularly or taking other actions. It is desirable that the person responsible for Personal Data management, etc. review the security control actions incorporated in the outsourcing contract and appropriately evaluate the outsourcee's compliance therewith. When an outsourcee intends to outsource the relevant duties to another entity, it is desirable that the Full Member sufficiently confirms that the outsourcee appropriately supervises the sub-outsourcee of this article and that the sub-outsourcee takes security control actions based on Article 20 of the Protection Act, as in the case with the outsourcee, by such means as requesting the outsourcee to make a report on the sub-outsourcee, the content of duties to the sub-outsourced, and sub-outsourcee's method of handling Personal Data in advance and go through prior approval process or implementing regular audits by themselves or making the outsourcee do so. The same shall apply to cases of further sub-outsourcing.	over those receiving outsourcing contracts (i) Cases where as a result of outsourcing to an external business operator without understanding the status of security control actions for Personal Data at the time of concluding the contract and thereafter, the outsourcee leaks Personal Data (ii) Cases where as a result of giving no instructions to an outsourcee on the content of necessary security control actions in relation to handling Personal Data, the outsourcee leaks Personal Data (iii) Cases where an outsourcer does not give any instructions to an outsourcee on terms and conditions of sub-outsourcing and failed to confirm the status of handling Personal Data of the outsourcee, and the outsourcee sub-outsources processing of Personal Data, and as a result, the sub-outsourcee leaks Personal Data. (iv) Cases where an outsourcer has not taken any necessary measures such as requesting an outsourcee to make a report on sub-outsourcing, despite the contract providing for understanding of the implementation status of sub-outsourcing by the outsourcee, and sub-outsourcing that the outsourcer does not know is implemented, and as a result, the sub-outsourcee leaks Personal Data. [Reference provisions, etc.] Article 22 of the Protection Act, 3-3-4 of the General Rules GL
Article 13. Restriction on Third-Party Provision 1. A Full Member must not provide Personal Data to a third party (meaning those who do not fall under any of the categories of a Full Member attempting to provide the Personal Data and a Principal relating to the Personal Data, regardless of whether the party is	(1) Matters to be noted in the case of providing Personal Data When a Full Member provides Personal Data to a third party, it is necessary to obtain consent from the Principal in advance. If a Full Member intends

Guidelines for Protection of Personal Information	Explanations
an individual, corporation or any other organization; the same shall apply except for Article 13-2 through Article 13-5) without obtaining in advance a Principal's consent. In obtaining consent, the Full Member must clearly indicate the content within a reasonable and appropriate scope that is considered necessary for the Principal to make a judgment on the consent in accordance with the scale and nature of the business, the handling status of Personal Data and other factors. If provision of Personal Information to a third party is assumed in advance, a Full Member must specify the fact in the utilization purpose. However, in any of the following cases, a Principal's consent is unnecessary in the provision of Personal Data to a third party.	to provide Personal Data without obtaining consent from the Principal, the Full Member shall confirm whether or not the provision of Personal Data falls under any of the following and take necessary actions. (i) Exclusion from application under laws and regulations, etc. (Paragraph 1, Item 1 through Item 4) (ii) By opt-out (Paragraph 2) * It should be noted that any opt-out is not allowed for Sensitive Information (as defined in Article 2, Paragraph 1, Item 8 of the Guidelines). (iii) Outsourcing (Paragraph 4, Item 1) (iv) Business succession such as merger (Paragraph 4, Item 2) (v) Joint use (Paragraph 4, Item 3) When obtaining consent for provision of Personal Data to a third party, consent shall be acquired in writing in principle, and the consent shall be obtained after having the Principal recognize the third party to which the Personal Data is provided, the utilization purpose of the third party receiving the provided data, and the content of information to be provided to the third party through descriptions in the written document. (2) Third-party provision of specific Personal Information Specific Personal Information may be provided to a third party only in the cases stipulated under the Numbers Act. Notwithstanding Items 1 through 4 in the left column, a Full Member may provide specific Personal Information only when a payment record with individual number stated on it is submitted to the district director of the tax office. Also, it should be noted that individual numbers are not intended for joint use, and such use is regarded as third-party provision. [Reference provisions, etc.] Article 15, Article 19, Article 30, Paragraph 3 of the Numbers Act, 3 - (2) of the Numbers Act, Finance GL
(1) Cases based on laws and regulations	(3) Specific Examples of "cases based on laws and regulations" (Paragraph 1, Item 1) For example, the following may fall under this category. (i) Article 74-2 through Article 74-6 of the Act on General Rules for National Taxes (Questioning and Inspection by Tax Authorities) (ii) Article 1 of the National Tax Violations Control Act (Voluntary Investigation of Criminal Cases by Collecting Officials or Tax Collectors) (iii) Article 197 of the Code of Criminal Procedure (Inquiry for Matters Related to Investigation) (iv) Article 8, Paragraph 1 of the Crime Proceeds Transfer Prevention Act (Notification of Suspicious Transactions) (v) Article 223 of the Code of Civil Procedure (Order to Submit Documents)

Guidelines for Protection of Personal Information	Explanations
	(vi) Article 218, Paragraph 1 of the Code of Criminal Procedure (Seizure, Search, and Inspection by Warrant) (vii) Article 225 of the Income Tax Act (Payment Record and Notice of Payment) (viii) Article 72-63 of the Local Tax Act (Right of Employees of the Ministry of Internal Affairs and Communications to Ask Questions and Make Inspection Pertaining to Individual Business Tax); (ix) Article 141 of the National Tax Collection Act (Questioning and Inspection) (x) Article 10-6 of the Act on Special Provisions, etc. of the Income Tax Act, the Corporation Tax Act, and the Local Tax Act Incidental to Enforcement of Tax Treaties, etc. (Report of Account Information Pertaining to Automatic Information Exchange System based on the Common Reporting Standards (CRS)) (xi) Article 56-2, Article 210 and Article 211 of the FIEA (Collection and Inspection of Report, Questioning, Inspection, Retention, etc., Visit, Search, Seizure, etc.) (xii) Article 78, Paragraph 2, Article 78, Paragraph 6, and Article 78, Paragraph 7 of the FIEA * Provision of information to self-regulating organizations under the FIEA Cases where a Full Member provides Personal Information to the Association in order to carry out the Association's self-regulation related services, such as reporting and notification to the Association, investigation by the Association or complaint consultation and mediation business by the Association, etc. under the provisions of the Articles of Incorporation and other rules of the Association, which have been established in accordance with the FIEA, etc. (xiii) Article 23-2, Paragraph 2 of the Attorney Act (Inquiries from Bar Associations) For example, cases where it becomes necessary as evidential material to be submitted to a court, etc. It should be noted that although the relevant laws and regulations have a provision stating that a third party may request provision of Personal Information, when a Full Member is allowed not to respond to the request for a justifiable reason, the Full Member shall respond within the scope of the necessity and reasonableness of use for any purpose other than the original intention in light of the purport of the relevant laws and regulations. In this case, for example, as a response when an inquiry of a bar association is received, if it is difficult to judge whether the response is within the scope of the necessity and reasonableness of providing Personal Data, it is desirable to obtain the Principal's consent. [Reference provisions, etc.] Article 23 of the Protection Act, 3-4-1 of the General Rules GL

Guidelines for Protection of Personal Information	Explanations
(2) Cases in which there is a need to protect a human life, body, or property, and when it is difficult to obtain a Principal's consent	(4) Specific examples of "cases in which there is a need to protect a human life, body, or property, and when it is difficult to obtain a Principal's consent" (Paragraph 1, Item 2) For example, "person" includes "corporation," and the following may fall under this category. (i) Cases of providing information on illegal activities of an organized crime group, so-called "sokaiya" (corporate racketeer), an antisocial organization or its members, etc., information on an account used for a bank transfer fraud, and other information (ii) Cases of making inquiries of the police about customers who are suspected to be antisocial forces (iii) Cases of providing information to medical institutions in order to deal with sudden illness of customers, etc. (iv) Cases of providing information to the police about a person who persistently and intentionally interferes with business (v) Cases of assets disclosure to a family member of a Principal in the case where the situation in which the Principal is missing due to an earthquake, disaster, etc. continues [Reference provisions, etc.] Article 23 of the Protection Act, 3-4-1 of the General Rules GL
(3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a Principal's consent	[Reference provisions, etc.] Article 23 of the Protection Act, 3-4-1 of the General Rules GL
(4) Cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a Principal's consent would interfere with the performance of the said affairs	(5) Specific examples of "cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a Principal's consent would interfere with the performance of the said affairs" (Paragraph 1, Item 4) For example, the following may fall under this category. (i) Cases of responding to voluntary investigation conducted by tax authorities from the perspective of achieving appropriate taxation without exercising individual rights to ask questions and investigate. (Note) A Full Member individually judges whether or not "there is a need to cooperate." However, it is desirable that a Full Member accepts an "inquiry form for transactions of securities, etc." and other documents from tax authorities, identifies Personal Information subject to the inquiry, and then provides the relevant information. (ii) Cases of responding to voluntary investigation by police (iii) Cases of replying to a general statistical survey It should be noted that a Full Member shall respond

Guidelines for Protection of Personal Information	Explanations
	within the scope of the necessity and reasonableness of use for any purpose other than the original intention in light of the purport of the voluntary request. [Reference provisions, etc.] Article 23 of the Protection Act, 3-4-1 of the General Rules GL
2. A Full Member, with regard to Personal Data provided to a third party (excluding Sensitive Information; the same shall apply in this paragraph) may, in cases where it is set to cease in response to a Principal's request a third-party provision of Personal Data that can identify the Principal and when it has in advance informed a Principal of those matters set forth in the following or put them into a state where a Principal can easily know, and notified them to the Personal Information Protection Commission, provide the said Personal Data to a third party notwithstanding the provisions of the preceding paragraph. In addition, a Full Member itself shall also disclose the content of the notification by using the Internet or other appropriate methods. Sensitive Information may not be provided to a third party due to an opt-out policy.	(6) Specific examples of methods to "inform" (Paragraph 2) For example, there are the following methods. (i) Notification by directly delivering documents (in principle) (ii) Notification given orally or through automatic answering machine, etc. (iii) Notification sent by e-mail, facsimile, etc. or notification by sending a document by mail, etc. (7) "State where a Principal can easily know" (Paragraph 2) A "state where a Principal can easily know" means a condition in which a Principal can easily know some information in terms of time and means if he or she tries to know. Therefore, it is necessary for a Full Member to make continuous public announcements in the following manner, for example, in accordance with the manner of its business. (i) Posting or keeping posters, etc. at store counters, etc. all the time (ii) Continuous distribution of pamphlets and leaflets (iii) Posting on the website all the time (Note) It is desirable to have multiple means. (8) Third-party provision of specific Personal Information Specific Personal Information may be provided to a third party only in the cases stipulated under the Numbers Act. Notwithstanding the provisions of Paragraph 2 in the left column, a Full Member may provide specific Personal Information only when a payment record with individual number stated on it is submitted to the district director of the tax office. [Reference provisions, etc.] Article 23 of the Protection Act, 2-10, 3-4-2 of the General Rules GL
(1) To set a third-party provision as a utilization purpose	[Reference provisions, etc.] Article 23 of the Protection Act, 3-4-2 of the General Rules GL
(2) The categories of Personal Data provided to a third party	[Reference provisions, etc.] Article 23 of the Protection Act, 3-4-2 of the General Rules GL
(3) Means or method of a third-party provision	(9) Specific Examples of "means or method of a third-party provision" (Paragraph 2, Item 3) For example, the following may fall under this category. (i) Published as a book (including e-book) (ii) Posted on the Internet (iii) Printed out and delivered (iv) Distributed by various communication means (v) Delivered in the form of other external recording

Guidelines for Protection of Personal Information	Explanations
	media [Reference provisions, etc.] Article 23 of the Protection Act, 3-4-2 of the General Rules GL
(4) To cease, in response to a Principal's request, a third-party provision of Personal Data that can identify the Principal	[Reference provisions, etc.] Article 23 of the Protection Act, 3-4-2 of the General Rules GL
(5) Method of receiving a Principal's request	(10) Specific examples of "method of receiving a Principal's request" (Paragraph 2, Item 5) (i) By mail (ii) By sending e-mails (iii) Input to a designation form on the webpage (iv) Reception at the counter of business offices (v) Telephone [Reference provisions, etc.] Article 23 of the Protection Act, 3-4-2 of the General Rules GL
3. A Full Member must, in case of altering those matters set forth in item (2), item (3), or item (5) of the preceding paragraph, in advance inform a Principal of the contents to be altered or put them into a state where a Principal can easily know and notify them to the Personal Information Protection Commission. In addition, when notifying the contents to be altered to the Personal Information Protection Commission pursuant to this paragraph, a Full Member itself shall also disclose the content.	(11) Specific examples of methods to "inform" and for "a state where a Principal can easily know" (Paragraph 3) Same as (6) and (7) above [Reference provisions, etc.] Article 23 of the Protection Act, 2-10, 3-4-2 of the General Rules GL
4. In any of the following cases, a person receiving the provision of the Personal Data does not fall under a third party.	[Reference provisions, etc.] Article 23 of the Protection Act, 3-4-3 of the General Rules GL
(1) Cases in which Personal Data is provided as a result of a Full Member's outsourcing of the whole or part of the handling of the Personal Data within the necessary scope to achieve a utilization purpose.	(12) Specific examples of "cases in which Personal Data are provided as a result of a Full Member's outsourcing of a whole or part of the handling of the Personal Data within the necessary scope to achieve a utilization purpose" (Paragraph 4, Item 1) For example, the following cases may fall under this category. (i) Cases of providing customer data and commissioning entry work (ii) Cases of providing customer data and commissioning sending of documents (iii) Outsourcing of clerical work (iv) Outsourcing of storage and disposal of customer data (Note) Because reasonableness lies in an outsourcee being treated as being coupled with the Personal Information Handling Business Operator who is the providing entity in relation with the Principal only within the scope of outsourced work, the outsourcee cannot handle the Personal Data in anything other than the outsourced work. (Note) It should be noted that a Full Member must provide necessary and appropriate supervision over its outsourcees pursuant to Article 12. [Reference provisions, etc.] Article 23 of the Protection Act, 3-4-3 of the General

Guidelines for Protection of Personal Information	Explanations
	Rules GL
	(12-1) Financial Instruments Intermediary Services The giving and receiving of Personal Data obtained in connection with the financial instruments intermediary service between a Full Member and a Financial Instruments Intermediary Service Provider can be organized as “method of obtaining consent of a Principal,” “case of outsourcing,” or “case of joint use,” and it is necessary to take necessary measures according to each case. It should be noted that individual numbers cannot be organized as “method of obtaining consent of a Principal,” and “case of joint use,” and organized as “case of outsourcing” (financial instruments intermediary service is also considered to be a form of outsourcing), and such cases are regarded as third-party provision. It should be noted that, even if a Financial Instruments Intermediary Service Provider does not use an individual number, when the Financial Instruments Intermediary Service Provider performs the business of receiving a document containing an individual number (including an envelope or the like that clearly indicates that the document contains an individual number with a sight of “individual number related documents are enclosed,” etc. even if the document is sealed) from customers and transferring the document to an outsourcing Association member, this case shall be deemed as outsourcing under the Numbers Act.
(2) Cases in which Personal Data is provided as a result of business succession caused by a merger or other reason (limited to cases where Personal Data is used even after the succession of the business within the scope of the utilization purpose before the Personal Data is provided due to the business succession)	(13) Specific examples of “cases in which Personal Data are provided as a result of business succession caused by a merger or other reason” (Paragraph 4, Item 2) In addition to a merger, generally business succession in which Personal Data, such as customer information, related to the business is generally also taken over as a whole, including business transfer, contribution in kind of business and company split, etc., fall. In cases where at the negotiation stage before entering into a contract for the business succession, a Full Member undergoes investigation by the other party and provides the other party with its own Personal Data, the Full Member may provide the Personal Data without obtaining consent of the Principal in advance or without going through opt-out procedures in the third-party provision. However, the Full Member must conclude a contract to have the other party comply with the security control actions such as the utilization purpose and handling method for the Personal Data, measures when a leakage, etc. occurs, and measures when the negotiation for the business succession breaks down. [Reference provisions, etc.] Article 23 of the Protection Act, 3-4-3 of the General Rules GL

Guidelines for Protection of Personal Information	Explanations
(3) Cases in which Personal Data to be jointly utilized by a specified person is provided to the specified person, and when a Principal has in advance been informed or a state has been in place where a Principal can easily know to that effect as well as of the categories of the jointly utilized Personal Data, the scope of a jointly utilizing person, the utilization purpose of the utilizing person, and the name or appellation of the person responsible for controlling the said Personal Data (meaning a person who primarily accepts and processes complaints, makes decisions on disclosure, correction, etc. and utilization cease, etc., and has responsibilities for security control in the jointly utilizing person; hereinafter referred to as the "Control Manager" in Paragraph 6)	(14) Specific examples of "joint use" (Paragraph 4, Item 3) (i) Cases where information is jointly used within the scope of the utilization purpose at the time of acquisition in order to provide comprehensive services with group companies (i) Cases where Personal Data is jointly used among the parent company and fellow subsidiaries within the scope of the utilization purpose at the time of acquisition It should be noted that it is not always necessary for all the joint users to mutually provide Personal Data subject to the joint use. However, with regard to joint use, it is necessary to pay attention to the restriction on provision of non-disclosure information prescribed in Article 153, Paragraph 1, Item 7 and Article 154, Paragraph 1, Item 4 of the Cabinet Office Order on Financial Instruments Business, etc. The same shall apply hereinafter. In addition, when Personal Data that has been already obtained by a specific business operator is used jointly with other business operators, the Personal Data must be jointly used within the scope of the utilization purpose specified by the business operator that has already obtained the data in accordance with the provisions of Article 15, Paragraph 1 of the Protection Act. [Reference provisions, etc.] Article 23 of the Protection Act, 3-4-3 of the General Rules GL (15) Specific examples of methods to "inform" and for "a state has been in place where a Principal can easily know" (Paragraph 4, Item 3) Same as (6) and (7) above [Reference provisions, etc.] Article 23 of the Protection Act,2-10, 3-4-2 of the General Rules GL (16) It should be noted that individual numbers are not intended for joint use, and such use is limited to cases allowed by laws and regulations. [Reference provisions, etc.] Article 30, Paragraph 3 of the Numbers Act, 3-(2) of the Numbers Act, Finance GL
5. Any notification given by a Full Member pursuant to the provisions of item (3) of the preceding paragraph is to be in writing in principle. With regard to a notification, etc. concerning "the scope of a jointly utilizing person," a Full Member must make efforts to list jointly utilizing persons individually.	(17) Scope of joint users (Paragraph 5) (i) It is desirable to list joint users individually. In the case where they are not listed individually, in order to clarify the extent to which the scope of jointly using persons from a perspective of a Principal, such joint users shall be stated as, for example, "The Company and consolidated companies and companies accounted for by the equity method described in the securities report, etc." (ii) In the case of (i) above, it is possible to indicate the scope of joint users in an easy-to-understand manner by, for example, stating names of the joint users on the website. (18) When a Full Member implements joint use, from

Guidelines for Protection of Personal Information	Explanations
	the viewpoint of clarifying and smoothly implementing responsibilities, etc. of joint users, it is desirable to determine in advance the following matters, for example, in addition to information in the preceding paragraph. (i) Requirements for joint users (certain frameworks in implementation of business operations through joint use such as being a group company and participating in a specific campaign business) (ii) Person responsible for handling Personal Information, person in charge of inquiries, and contact information of each joint user (iii) Matters related to handling of Personal Data to be jointly used (a) Matters related to prevention of leakage, etc. of Personal Data (b) Prohibition of processing, use, copying, reproduction, etc. for a purpose other than the original purpose (c) Matters related to return, deletion, and disposal of data after termination of joint use (iv) Measures to be taken when arrangements for handling Personal Data to be jointly used have not been observed (v) Matters related to reports and communications in the event of an incident or accident involving Personal Data to be jointly used (vi) Procedures for terminating the joint use [Reference provisions, etc.] Article 23 of the Protection Act, 3-4-3 of the General Rules GL
6. A Full Member must, in case of altering a utilization purpose for a utilizing person or the name or appellation of the Control Manager set forth in Paragraph 4, item (3), in advance inform a Principal of the contents to be altered or put them into a state where a Principal can easily know.	(19) Specific examples of methods to “inform” and for “a state where a Principal can easily know” (Paragraph 6) Same as (6) and (7) above [Reference provisions, etc.]Article 23 of the Protection Act, 2-10 and 3-4-2 of the General Rules GL, Article 11, and Article 4 of the Finance Sector GL (20) It is not permitted in principle to change the “categories of the jointly utilized Personal Data” and the “scope of jointly using persons”; however, in the following cases, for example, these items may be jointly used after being changed. (i) Cases where consent of a Principal is obtained in advance for any category of Personal Data to be jointly used or change of the business operator (ii) Cases where there is a change in the name of a jointly using business operator, but there is no change in the categories of Personal Data to be jointly used (iii) Cases where business of a jointly using business operator was succeeded However, it should be noted that this is based on the premise that there is no change in the categories of Personal Data to be jointly used. [Reference provisions, etc.] Article 23 of the Protection Act, 3-4-3 of the General Rules GL

Guidelines for Protection of Personal Information	Explanations
Article 13-2. Restriction on Provision to a Third Party in a Foreign Country 1. A Full Member, except in those cases set forth in each item of Paragraph 1 of the preceding article, must, in case of providing Personal Data to a third party (excluding a person establishing a system conforming to standards prescribed by the Enforcement Rules as necessary for continuously taking action equivalent to the one that a Personal Information Handling Business Operator shall take concerning the handling of Personal Data; hereinafter the same shall apply in this article) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same shall apply) (excluding those prescribed in the Enforcement Rules as a country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests; hereinafter the same shall apply in this article and the next article), in advance obtain a Principal's consent to the effect that he or she approves for the provision to a third party in a foreign country. In this case, the provisions of the same article shall not apply.	With regard to provision of Personal Data to a third party, when the party is excluded from "foreign countries" under Article 24 of the Protection Act or when the party does not fall under "third parties" under (2) or (3), it is not necessary to obtain "a Principal's consent to the effect that he or she approves of the provision to a third party in a foreign country," or otherwise, such consent is required. When the case is regarded as provision of data to a third party in a foreign country, it is necessary to obtain a Principal's consent to the provision to a third party in a foreign country, unless each item of Article 23, Paragraph 1 of the Protection Act applies. In other words, even in the case of outsourcing, business succession, or joint use (in the cases set forth in the respective items of Article 23, Paragraph 5 of the Protection Act), consent of a Principal is required, unlike provision to a third party in Japan. (1) "Countries" to be excluded from "foreign countries" Under the category of foreign countries that have a personal information protection related system which is considered to be at the level equivalent to that of Japan in protection of rights and interests of individuals stipulated in the provisions of Article 24 of the act, countries set forth in the Notification of the Specific Personal Information Protection Commission No. 1 of 2019 pursuant to Article 11 of the Enforcement Rules (*) falls. * Countries stipulated in the Agreement on the European Economic Area Agreement as of February 14, 2020 listed below * If the following countries stipulated in the Agreement on the European Economic Area Agreement are changed on or after February 14, 2020, prompt response is required. Iceland, Ireland, Italy, Great Britain, Estonia, Austria, the Netherlands, Cyprus, Greece, Croatia, Sweden, Spain, Slovakia, Slovenia, the Czech Republic, Denmark, Germany, Norway, Hungary, Finland, France, Bulgaria, Belgium, Poland, Portugal, Malta, Latvia, Lithuania, Liechtenstein, Romania, and Luxembourg (2) Views of "third party" In general, a "third party" means any person other than a Personal Information Handling Business Operator providing Personal Data and a Principal specified by the Personal Data. [Specific examples] (i)When the person providing Personal Data and the recipient are both corporations, they do not constitute a "third party" if their corporate status is the same. - When a Japanese company provides Personal Data to a local subsidiary of the company, the subsidiary falls under "third party in a foreign country." - When a Japanese corporation of a

Guidelines for Protection of Personal Information	Explanations
	foreign-affiliated company provides Personal Data to the parent company located abroad, the parent company falls under "third party in a foreign country." - When a Japanese company provides Personal Data within the same legal personality such as its local business offices or branch offices, such offices do not fall under "third party in a foreign country." (ii) Even if the recipient of Personal Data is a foreign juridical person, it shall not be deemed to be a "third party in a foreign country" when it is recognized that "Personal Information Database, etc." is used for the purpose of its business in Japan, for example, the case where the foreign juridical person has established a business office in Japan. - When a Japanese company's head office in Tokyo provides Personal Data to a Tokyo branch of a foreign company, the branch shall not be regarded as a "third party in a foreign country." (3) Those who are excluded from "third parties" as "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" With regard to 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, consent of a Principal set forth in this article is not required for handling of Personal Data. In cases that fall under (i) or (ii) below, the person shall be deemed to have established such a system. (i) Between a Full Member and the recipient of Personal Data, the implementation of measures in line with the purport of the provisions of Chapter 4, Section 1 of the Protection Act is ensured by appropriate and reasonable means with regard to handling of the Personal Data by the recipient of the provision [Contents to be put in place for "measures in line with the purport of the provisions of Chapter 4, Section 1 of the Protection Act"] Article 15 through Article 35 of the Protection Act (excluding Article 17, Paragraph 2, Article 25, Article 26, and Article 34 of the Protection Act) [Specific examples of the "international framework" having the above contents in place (reference)] - OECD Privacy Guidelines - APEC Privacy Framework ["appropriate and reasonable means] "Appropriate and reasonable means" should be judged on a case-by-case basis, but it is necessary to be a means whereby a third party in a foreign

Guidelines for Protection of Personal Information	Explanations
	country to whom Personal Data is provided can assure that the third party continues to take measures equivalent to measures to be taken by a Japanese Personal Information Handling Business Operator. For example, the following cases fall under this category. - In the case of outsourcing handling of Personal Data to a business operator located in a foreign country, contracts, confirmations, memoranda, etc. between the provider and the recipient - In the case of transferring Personal Data within the same corporate group, internal rules, privacy policies, etc. applicable to the provider and the recipient (ii) The recipient of Personal Data shall have obtained a certification based on an international framework for handling personal information. [Specific examples of certification system based on an international framework] - APEC Cross-Border Privacy Rule (CBPR) System In the case where a providing Full Member has obtained the CBPR certification and the recipient "third party in a foreign country" is a person handling personal information on behalf of the Full Member, the Full Member's meeting requirements for obtaining the CBPR certification is also construed as one of "appropriate and reasonable means." [Reference provisions, etc.] Article 24 of the Protection Act, Article 11, and Article 11-2 of the Enforcement Rules, 3-4-4 of the General Rules, Foreign GL
Article 13-3. Keeping, etc. of a Record on a Third-Party Provision 1. A Full Member must, when having provided personal data to a third party (excluding a person set forth in each item of Article 2, Paragraph 5 of the Protection Act; the same shall apply in this article through Article 13-5), keep a record of the date of the Personal Data provision, the name or appellation of the third party, and other matters prescribed in the Enforcement Rules. However, when providing Personal Data to a third party in Japan, keeping of records shall be unnecessary if the case falls under any of items (1) through (7) below. In addition, in the provision to a third party in a foreign country, keeping of records shall be unnecessary if the case falls under any of items (1) through (4), or if the third party meets standards stipulated in the Enforcement Rules and the case falls under each item of Article 23, Paragraph 5 of the Protection Act. (1) Cases based on laws and regulations (2) Cases in which there is a need to protect a human life, body, or property, and when it is difficult to obtain a Principal's consent (3) Cases in which there is a special need to enhance	(1) In this Article, those who fall under the following categories are excluded from "third party." (i) National governmental institutions (ii) Local governments (iii) Independent administrative agencies, etc. (iv) Local incorporated administrative agencies (2) Pursuant to the provisions of Article 23, Paragraph 2 of the Protection Act, when providing Personal Data to a third party through opt-out, records of the following items shall be made. (i) Date of provision of the Personal Data (ii) Name or appellation of the third party or any other matters sufficient to specify the third party (if data is provided to many and unspecified persons, to that effect); (iii) Name of Principals to be identified by the Personal Data or other matters sufficient to identify the Principals (iv) Categories of the Personal Data (3) Pursuant to the provisions of Article 23, Paragraph 1 or Article 24 of the Protection Act, when providing Personal Data to a third party, records of the following items shall be made (in the case of obtaining consent of a Principal each time; * The same shall apply regardless of whether the third

Guidelines for Protection of Personal Information	Explanations
public hygiene or promote fostering healthy children, and when it is difficult to obtain a Principal's consent (4) Cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a Principal's consent would interfere with the performance of the said affairs (5) Cases in which Personal Data is provided as a result of a Full Member's outsourcing of the whole or part of the handling of the Personal Data within the necessary scope to achieve a utilization purpose. (6) Cases in which Personal Data is provided as a result of business succession caused by a merger or other reason. (7) Cases in which Personal Data to be jointly utilized by a specified person is provided to the specified person, and when a Principal has in advance been informed or a state has been in place where a Principal can easily know to that effect as well as of the categories of the jointly utilized Personal Data, the scope of a jointly utilizing person, the utilization purpose of the utilizing person, and the name or appellation of the person responsible for controlling the said Personal Data	party is in Japan or abroad). (i) Fact that consent of the Principal set forth in Article 23, Paragraph 1 or Article 24 of the Protection Act has been obtained (ii) Name or appellation of the third party or any other matters sufficient to specify the third party (if data is provided to many and unspecified persons, to that effect); (iii) Name of Principals to be identified by the Personal Data or other matters sufficient to identify the Principals (iv) Categories of the Personal Data (4) In the case where Personal Data was provided to a third party, records shall be made in writing, electromagnetic records, or microfilm. (5) The record-keeping obligation shall not apply to any case that is not the provision by a "provider" substantially. The following cases fall under this category. (i) Provision by the Principal Content entered by the poster himself or herself through SNS, etc. (ii) Provided on behalf of the Principal (a) Cases where the name, contact information, etc. of a person in charge are provided in response to a customer's inquiry about the content of transactions by telephone (b) Cases of introducing a customer in a joint venture among a parent company and its subsidiaries and where an application for opening an account, placement of orders has been made by the customer and the customer has recognized the content of information to be received or provided among the parent company and its subsidiaries, the recipient of the data, etc. at the time of the application, and the provision is considered to be specifically identified. (c) Cases of receiving Personal Data provided from a customer as introduction by his or her acquaintance (6) The record-keeping obligation shall not apply to any case that is not the provision to a "recipient" substantially. The following cases fall under this category. (i) Cases of providing information to those who are in a relationship that can be assessed to be an integral part of the Principal, such as the Principal's representative, family member, etc. For example, this means the case where a salesperson of a financial institution explains the profit and loss situation of financial instruments held to a customer who comes with his or her family. (ii) Cases where with the provider's intention to eventually provide information to the Principal, the information is provided to a third party through the intervention of the recipient, and the Principal can recognize this clearly

Guidelines for Protection of Personal Information	Explanations
	(7) Views on the act of "provision" Published information that can be obtained by many and unspecified persons is originally information that the recipient can obtain by itself, and the act of the providers' intentionally providing the information to the recipient means that the provider takes care of the obtaining act on behalf of the recipient. Therefore, this act substantially does not fall under the category of third-party provision for which the confirmation and record-keeping obligations should be imposed, and the obligations shall not apply. For example, information disclosed on a website, etc., information reported by the media, and others fall under this category. However, information that can be accessed only by specific persons, non-public information that can be obtained in business operations of the provider, etc. are excluded. In addition, the act of making Personal Data available for public must be recorded as the provider. * It should be noted that as even so-called public information falls under the category of "personal information," provisions other than the confirmation and record-keeping obligations shall apply. [Reference provisions, etc.] Article 23 and Article 25 of the Protection Act, 2 and 3 of the Confirmation and Record-Keeping GL
Article 13-4. Confirmation, etc. when Receiving a Third-Party Provision 1. A Full Member, when receiving the provision of Personal Data from a third party, confirm the name or appellation and address of the third party and, for a corporate body, the name of its representative (for non-corporate body having appointed a representative or administrator, the said representative or administrator), and process of acquisition of the personal information by the third party, and keep a record of matters stipulated in Article 26, Paragraph 3 of the Protection Act, except in the following cases. However, the confirmation and record-keeping obligations shall not apply to any case that is not a provision by a "provider" substantially. (1) Cases based on laws and regulations (2) Cases in which there is a need to protect a human life, body, or property, and when it is difficult to obtain a Principal's consent (3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a Principal's consent (4) Cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that	(1) The concept of "third party" in this article is the same as the concept in Article 13-3. (2) Concept of "process of acquisition of the Personal Data by the third party" When it is suspected that Personal Data to be provided has not been legally obtained, confirmation of the process of acquisition of the Personal Data by the third party is required in order to prevent the use and distribution of the Personal Data. For example, this means confirmation of the content of the following items. (i) Type of the obtainer (Principal as a customer, Principal as an employee, other Personal Information Handling Business Operator, private person such as a family member, friend, etc., so-called public information, etc.) (iii) Manner of the obtaining act (Whether it is obtained directly from the Principal, whether it is obtained with charge, whether it is obtained from so-called public information, whether it is obtained by introduction, whether it is obtained as a private person, etc.) A "letter of consent on information sharing" accepted from a customer among a parent company and its subsidiaries can be used

Guidelines for Protection of Personal Information	Explanations
obtaining a Principal's consent would interfere with the performance of the said affairs (5) Cases in which Personal Data is provided as a result of a Full Member's outsourcing of the whole or part of the handling of the Personal Data within the necessary scope to achieve a utilization purpose. (6) Cases in which Personal Data is provided as a result of business succession caused by a merger or other reason. (7) Cases in which Personal Data to be jointly utilized by a specified person is provided to the specified person, and when a Principal has in advance been informed or a state has been in place where a Principal can easily know to that effect as well as of the categories of the jointly utilized Personal Data, the scope of a jointly utilizing person, the utilization purpose of the utilizing person, and the name or appellation of the person responsible for controlling the said Personal Data	because it generally shows the process of acquisition. (3) When receiving Personal Data provided from a third party, records on the following items shall be made. (i) Cases of receiving third-party provision from a Personal Information Handling Business Operator through opt-out (a) Date of receiving provision of the Personal Data (b) Name or appellation and address of the third party and, for a corporate body, the name of its representative (for non-corporate body having appointed a representative or administrator, the said representative or administrator) (c) Process of acquisition of the Personal Data by the third party (d) Name of Principals to be identified by the Personal Data or other matters sufficient to identify the Principals (e) Categories of the Personal Data (f) Fact that the information has been published by the Personal Information Protection Commission (ii) Cases of receiving third-party provision from a Personal Information Handling Business Operator each time by consent of the Principal (a) Fact that consent of the Principal set forth in Article 23, Paragraph 1 or Article 24 of the Protection Act has been obtained (b) Name or appellation and address of the third party and, for a corporate body, the name of its representative (for non-corporate body having appointed a representative or administrator, the said representative or administrator) (c) Process of acquisition of the Personal Data by the third party (d) Name of Principals to be identified by the Personal Data or other matters sufficient to identify the Principals (e) Categories of the Personal Data (iii) Cases of receiving third-party provision from a private person, etc. (a) Name or appellation and address of the third party and, for a corporate body, the name of its representative (for non-corporate body having appointed a representative or administrator, the said representative or administrator) (b) Process of acquisition of the Personal Data by the third party (c) Name of Principals to be identified by the Personal Data or other matters sufficient to identify the Principals (d) Categories of the Personal Data * When the personal data provider is a Personal Information Handling Business Operator, confirmation of the process of individual acquisition is not required if it can be confirmed that the business operator's internal rules or basic

Guidelines for Protection of Personal Information	Explanations
	terms and conditions for customers, etc. stipulate that Personal Information shall be acquired appropriately. (4) With regard to the content in (3) above confirmed upon receiving Personal Data provided from a third party, records shall be made in writing, electromagnetic records, or microfilm. (5) The confirmation and record-keeping obligations shall not apply to any case that is not the provision by a "provider" substantially. The following cases fall under this category. (i) Provision by the Principal Content entered by the poster himself or herself through SNS, etc. (ii) Provided on behalf of the Principal (a) Cases where the name, contact information, etc. of a person in charge are provided in response to a customer's inquiry about the content of transactions by telephone (b) Cases of introducing a customer in a joint venture among a parent company and its subsidiaries and where an application for opening an account, placement of orders has been made by the customer and the customer has recognized the content of information to be received or provided among the parent company and its subsidiaries, the recipient of the data, etc. at the time of the application, and the provision is considered to be specifically identified. (c) Cases of receiving Personal Data provided from a customer as introduction by his or her acquaintance (6) A case that is not the provision to a "recipient" substantially means the following cases. (i) Cases of providing information to those who are in a relationship that can be assessed to be an integral part of the Principal, such as the Principal's representative, family member, etc. For example, this means the case where a salesperson of a financial institution explains the profit and loss situation of financial instruments held to a customer who comes with his or her family. (ii) Cases where with the provider's intention to eventually provide information to the Principal, the information is provided to a third party through the intervention of the recipient, and the Principal can recognize this clearly (7) Concept of the action of "receiving provision" Because the confirmation and record-keeping obligations apply in cases where there is the action of "receiving Personal Data provided from a third party," you cannot say that there is the action of receiving provision in the action of merely browsing Personal Data, so the confirmation and record-keeping obligations shall not apply. The action of a Personal Information Handling

Guidelines for Protection of Personal Information	Explanations
	Business Operator making Personal Data available for use by a third party falls under the category of the providing action. In addition, in the case where Personal Data is provided orally, by facsimile, by e-mail, by telephone, etc., unilaterally without regard to the recipient's intention, if the recipient has not taken any action of "receiving provision," the confirmation and record-keeping obligations shall not apply. (8) Concept in the case where the confirmation and record-keeping obligations shall not apply to the recipient Even if information falls under the category of Personal Data to the provider, in the case where information not falling under the category of "Personal Data," or even "Personal Information," to the recipient is received, the confirmation and record-keeping obligations shall not apply. For example, the following cases fall under this category. (i) Cases of receiving provided data from which it is impossible to identify an individual by deleting his or her name etc. by the provider (ii) Cases of receiving data with only ID number controlled by the provider attached [Reference provisions, etc.] Article 25 and Article 26 of the Protection Act, 2 and 4 of the Record-Keeping GL
Article 13-5. Retention Period for Keeping Records upon Third-Party Provision Records made in accordance with Article 13-3 and Article 13-4 must be kept for the period specified in the Enforcement Rules from the date of creating these records.	(1) When Personal Data is provided to a third party, created records shall be maintained according to the following cases. (i) In the case where records are made by means set forth in Article 12, Paragraph 3 of the Enforcement Rules, until the day on which one year has passed since the last provision of Personal Data pertaining to the records (ii) In the case where records are made by means set forth in Article 12, Paragraph 2 or Article 16, Paragraph 2 of the Enforcement Rules, until the day on which three years have passed since the last provision of Personal Data pertaining to the records *When Personal Data of multiple persons are provided, records of the Personal Data may be made collectively instead of individually. In this case, the retention period shall be calculated for each individual. (iii) Three years in cases other than (i) and (ii) (2) In providing Personal Data, it is possible to use logs of the date and time of transmission, the destination of transmission, etc. as part of records in this section. [Reference provisions, etc.] Article 25 and Article 26 of the Protection Act

Guidelines for Protection of Personal Information	Explanations
Article 14. Public Disclosure, etc. on Matters Relating to Retained Personal Data 1. A Full Member must, concerning its Retained Personal Data, put the following matters into a state where a Principal can know (including those cases in which it, at the request of a Principal, responds without delay). When the utilization purpose includes provision of information to a third party, the fact must be clearly stated as the content in Item (2).	(1) Specific examples of cases where matters related to Retained Personal Data are put into a "state where a Principal can know (including those cases in which it, at the request of a Principal, responds without delay)" (Paragraph 1) The state means a condition in which a Principal can know the information if he or she tries to know. A Full Member needs to take appropriate measures, for example, by the following methods, in accordance with the manner of its business. (i) Continuous posting of posters or keeping of documents the front of the store at stores (Alternatively, there is a means of posting information together with the Pronouncement Concerning Protection of Personal Information set forth in Article 23; the same shall apply hereinafter). (ii) Continuous distribution of pamphlets and leaflets (iii) Continuous posting on the website (iv) Delivery of a documents, sending of documents by mail, facsimile, etc. at the request of the Principal. (v) Replying orally or by telephone, e-mail, etc. in response to the Principal's request It is sufficient to inform the subject Principal of necessary matters, and it is not necessary to make a change on all the used media at the same time. [Reference provisions, etc.] Article 27 of the Protection Act, 3-5-1 of the General Rules GL
(1) Appellation of the Full Member	[Reference provisions, etc.] Article 27 of the Protection Act, 3-5-1 of the General Rules GL
(2) Utilization purpose of all Retained Personal Data (excluding those cases falling under Article 8, Paragraph 4, Item (1) through Item (3))	- When the utilization purpose includes third-party provision, the fact shall also be clearly presented. [Reference provisions, etc.] Article 27 of the Protection Act, 3-5-1 of the General Rules GL
(3) Procedures for responding to a request pursuant to the provisions of Paragraph 1 of the succeeding paragraph or a demand pursuant to the provisions of Article 15, Paragraph 1, Article 16, Paragraph 1, or Article 17, Paragraph 1 or Paragraph 2 (including the amount of a fee when it is prescribed pursuant to the provisions of Article 20)	[Reference provisions, etc.] Article 27 of the Protection Act, 3-5-1 of the General Rules GL
(4) In-house contact point to which a complaint is to be filed in regard to handling of Retained Personal Data	[Reference provisions, etc.] Article 27 of the Protection Act, 3-5-1 of the General Rules GL
(5) Appellation of the accredited personal information protection organization and contact point to which resolution of its complaint is to be filed	[Reference provisions, etc.] Article 27 of the Protection Act, 3-5-1 of the General Rules GL
2. A Full Member must, when requested by a Principal to get informed of a utilization purpose of Retained Personal Data that can identify the Principal, inform the said Principal thereof without delay. This, however, shall not apply in those cases falling under any of the following items. (1) Cases in which the utilization purpose of Retained	(2) Specific examples of methods to "inform" (Paragraph 2 and Paragraph 3) For example, there are the following methods. (i) Notification by directly delivering documents (ii) Notification given orally or through automatic answering machine, etc. (iii) Notification sent by e-mail, facsimile, etc. or

Guidelines for Protection of Personal Information	Explanations
Personal Data that can identify the said Principal is clear pursuant to the provisions of the preceding paragraph (2) Cases falling under Article 8, Paragraph 4, Items (1) through Item (3)	notification by sending a document by mail, etc. [Reference provisions, etc.] Article 27 of the Protection Act, Article 8 of the Enforcement Order, 2-10 and 3-5-1 of the General Rules GL, Article 12 of the Finance Sector GL
3. A Full Member must, when having been requested based on the provisions of the preceding paragraph but deciding not to inform a Principal of the utilization purpose of Retained Personal Data, inform the Principal to that effect without delay.	[Reference provisions, etc.] Article 27 of the Protection Act, 3-5-1 of the General Rules GL
Article 15. Disclosure 1. A Full Member must, when having received a demand of disclosing Retained Personal Data that can identify a Principal (when such data does not exist, including informing a Principal thereof) from the Principal, disclose the Retained Personal Data to the Principal without delay by means of issuing a document (when there is a method agreed by the person demanding the disclosure, that method). However, in cases where disclosing such data falls under any of the following cases, the whole or part thereof may not be disclosed. (1) Cases in which there is a possibility of harming a Principal or third party's life, body, property, or other rights and interests	(1) Specific examples of a "method agreed by the person demanding the disclosure" (Paragraph 1) For example, there are the following methods. (i) By e-mail, etc. (ii) By telephone (2) When a demand for disclosing "whether or not there is any individual number" is made by a Principal, it is sufficient to disclose the fact of "obtaining individual numbers." [Reference provisions, etc.] Article 28 of the Protection Act, 3-5-2 of the General Rules GL
(2) Cases in which there is a possibility of interfering security with the said Full Member implementing its business properly	(3) Examples falling under cases in which there is a possibility of interfering with the said Full Member implementing its business properly (Paragraph 1, Item 2) For example, the following cases may fall under this category. (i) Cases where a demand for disclosure of information added by a Full Member, such as assessment information, is received, or where disclosure of Retained Personal Data prevents proper implementation of transactions with customers (ii) Cases where the same Principal repeatedly demands disclosure of the same content that requires a complicated response, and the contact point for inquiries is practically occupied, which is likely to cause substantial hindrance to business operations such as interruption of other inquiry handling operations (iii) Cases where corporate secrets are likely to be revealed (4) Examples not falling under "cases in which there is a possibility of interfering with the said Full Member implementing its business properly" (Paragraph 1, Item 2) For example, only the large amount of Retained Personal Data to be disclosed cannot constitute a reason for non-disclosure. [Reference provisions, etc.] Article 28 of the Protection Act, 3-5-2 of the General Rules GL
(3) Cases of violating other laws or regulations	(5) "Cases of violating other laws or regulations" means, for example, violation of Article 134 of the Penal Code (unlawful disclosure of confidential

Guidelines for Protection of Personal Information	Explanations
	information) or Article 4 of the Telecommunications Business Act (protection of secrecy of communications) (Paragraph 1, Item 3). In addition, if, pursuant to the provisions of other laws and regulations, Retained Personal Data that specifies the person is to be disclosed by a method equivalent to the methods set forth in Article 28, Paragraph 2 of the Protection Act and Article 9 of the Cabinet Order (when there is a method agreed by the person demanding the disclosure, that method), the provisions of Article 28, Paragraph 1 and Paragraph 2 shall not apply, and the provisions of the other laws and regulations shall apply. [Reference provisions, etc.] Article 28 of the Protection Act, 3-5-2 of the General Rules GL
2. A Full Member must, when having decided not to disclose the whole or part of Retained Personal Data in connection with a demand pursuant to the provisions of the preceding paragraph or when the Retained Personal Data does not exist, inform a Principal thereof without delay. The reasons for the decision shall be explained by showing the provisions of the law supporting the decision and facts that are the basis of the decision.	(6) Specific examples of methods to "inform" and "explain" (Paragraph 2) For example, there are the following methods. (i) Notification by directly delivering documents (ii) Notification given orally or through automatic answering machine, etc. (iii) Notification sent by e-mail,facsimile, etc. or notification by sending a document by mail, etc. [Reference provisions, etc.] Article 28 of the Protection Act, Article 9 of the Enforcement Order, 2-10 and 3-5-2 of the General Rules GL, Article 13 of the Finance Sector GL
Article 16. Correction, etc. 1. In case of having received a demand made by a Principal for making a correction, addition, or deletion (hereinafter referred to as a "Correction, etc.") of the contents of Retained Personal Data that can identify the Principal by reason that the data are neither correct nor factual, a Full Member must conduct a necessary investigation, such as confirmation of facts, without delay to the extent necessary to achieve the utilization purpose and, based on the result thereof, make a Correction, etc. of the contents of the Retained Personal Data in principle.	(1) Correction, etc. (i) Correction, etc. is to be made within the scope necessary for achieving the utilization purpose, and any Correction, etc. beyond the necessity shall not be required. (ii) Correction, etc. is based on the Protection Act, and shall not apply to notification of change of name, address, etc. from customers, etc. (2) When Correction, etc. is not necessary for the utilization purpose or when it is not correct to indicate that the Retained Personal Data is erroneous, Correction, etc. is not necessary. In this case, however, it should be noted that it is necessary to notify the Principal without delay that any Correction, etc. will not be made. [Reference provisions, etc.] Article 29 of the Protection Act, 3-5-3 of the General Rules GL
2. A Full Member must, when having made a Correction, etc. on the whole or part of the contents of the Retained Personal Data in connection with a demand specified in the preceding paragraph or when having made a decision not to make a Correction, etc., inform a Principal without delay to that effect (including, when having made a Correction, etc., the contents thereof). If a Full Member does not make a Correction, etc., the Full Member is to explain the reasons by presenting grounds for the decision not to	(3) Specific examples of methods to "inform" and "explain" (Paragraph 2) For example, there are the following methods. (i) Notification by directly delivering documents (ii) Notification given orally or through automatic answering machine, etc. (iii) Notification sent by e-mail,facsimile, etc. or notification by sending a document by mail, etc. [Reference provisions, etc.] Article 29 of the Protection Act, 2-10 of the General

Guidelines for Protection of Personal Information	Explanations
make a Correction, etc. and facts supporting the decision.	Rules GL, Article 14 of the Finance Section GL
Article 17. Utilization Cease, etc. 1. In case of having received a demand made by a Principal for a utilization use or deletion (hereinafter referred to as a "Utilization Cease, etc.") of Retained Personal Data that can identify the Principal by reason that the Retained Personal Data has been handled in violation of the provisions of Article 5 or has been acquired in violation of the provisions of Article 7 and when it has become clear that there is a reason for the demand, a Full Member must fulfill a Utilization Cease, etc. of the said Retained Personal Data to the extent necessary to redress a violation without delay. This, however, shall not apply in case where a Utilization Cease, etc. of the said Retained Personal Data requires a large expense or other cases where it is difficult to fulfill a Utilization Cease, etc. and when necessary alternative action is taken to protect a Principal's rights and interests.	(1) Even if all of Retained Personal Data are requested to be deleted, when the violation of the procedures can be corrected by suspension of use, taking such measures has fulfilled the obligation to do so, and it is not always necessary to implement the required measures as they are. When it is not correct to indicate that the violation of the procedures is erroneous, utilization suspension, etc. is not necessary. (2) When it is not correct to indicate that the violation of the procedures is erroneous, it is not necessary to suspend the third-party provision. [Reference provisions, etc.] Article 30 of the Protection Act, 3-5-4 of the General Rules GL
2. In case of having received a demand made by a Principal for ceasing a third-party provision of Retained Personal Data that can identify the Principal by reason that the Retained Personal Data are being provided to a third party in violation of the provisions of Article 13, Paragraph 1 and when it has become clear that there is a reason in the demand, a Full Member must cease the third-party provision of the Retained Personal Data without delay in principle. This, however, shall not apply in cases where ceasing the third-party provision of the said Retained Personal Data requires a large expense or other cases where it is difficult to cease the third-party provision and when necessary alternative action is taken to protect a Principal's rights and interests.	[Reference provisions, etc.] Article 30 of the Protection Act, 3-5-4 of the General Rules GL
3. A Full Member must, when having fulfilled a utilization cease etc. or decided not to fulfill a Utilization Cease, etc. of the whole or part of Retained Personal Data in connection with a demand pursuant to the provisions of Paragraph 1, or when having ceased a third-party provision or decided not to cease a third party provision of the whole of Retained Personal Data in connection with a demand pursuant to the provisions of the preceding paragraph, inform a Principal to that effect (including, when taking a measure that is different from the action requested by the Principal, the contents of the measure) without delay.	(3) Specific examples of methods to "inform" (Paragraph 3) For example, there are the following methods. (i) Notification by directly delivering documents (ii) Notification given orally or through automatic answering machine, etc. (iii) Notification sent by e-mail,facsimile, etc. or notification by sending a document by mail, etc. [Reference provisions, etc.] Article 30 of the Protection Act, 2-10, 3-5-4 of the General Rules GL
Article 18. Explanation of Reason In case of informing a Principal to the effect that, as regards the whole or part of action requested or demanded by the Principal pursuant to the provisions of Article 14, Paragraph 3, Article 15, Paragraph 2, Article 16, Paragraph 2, and Paragraph 3 of the preceding article, the action will not be taken, or to the effect that different action from the said action will be taken, when explaining a reason therefor to the said Principal, a Full Member is to present grounds for the decision not to take the action or to	○ Specific examples of methods to "inform" and "explain" For example, there are the following methods. (i) Notification by directly delivering documents (ii) Notification given orally or through automatic answering machine, etc. (iii) Notification sent by e-mail,facsimile, etc. or notification by sending a document by mail, etc. [Reference provisions, etc.] Article 31 of the Protection Act, 2-10 of the General

Guidelines for Protection of Personal Information	Explanations
take a different action and facts supporting the decision.	Rules GL, 3-5-5, Article 14 of the Finance Sector GL
Article 19. Procedures for Responding to Demand, etc. for Disclosure, etc. 1. A Full Member may, as regards a request pursuant to the provisions of Article 14, Paragraph 2 or a demand pursuant to the provisions of Article 15, Paragraph 1, Article 16, Paragraph 1, Article 17, Paragraph 1 or Paragraph 2 (hereinafter referred to as a "Demand, etc. for Disclosure, etc."), decided on a method of receiving a request or demand. In this case, a Full Member is to regularly post that method on its website together with the Pronouncement Concerning Protection of Personal Information as specified in Article 23, or regularly posting or keeping it at a business office counter, etc.	1. When a Full Member has stipulated a method for receiving a Demand, etc. for Disclosure, etc., the Full Member shall keep such information available to a Principal (including cases where the Full Member answers such a request from a Principal without delay). 2. A Full Member may request a Principal to present matters necessary to specify Retained Personal Data (e.g.: address, ID, password, member number, etc.) for identification of the Principal subject to a Demand, etc. for Disclosure, etc. in order to facilitate procedures for disclosure, etc. [Reference provisions, etc.] Article 32 of the Protection Act, 3-5-6 of the General Rules GL, Article 15 of the Finance Sector GL
(1) Contact point to which a Demand, etc. for Disclosure, etc. is to be made	(1) Specific example of "Contact point to which a Demand, etc. for Disclosure, etc. is to be made" (Paragraph 1, Item 1) For example, department names, addresses, telephone numbers, e-mail addresses, etc. of head offices, branch offices, business offices, business centers, and others. [Reference provisions, etc.] Article 32 of the Protection Act, 3-5-6 of the General Rules GL, Article 15 of the Finance Sector GL
(2) Form of documents to be submitted at the time of a Demand, etc. for Disclosure, etc. and other methods of receiving Demand, etc. for Disclosure, etc.	(2) "Documents to be submitted at the time of a Demand, etc. for Disclosure, etc." (Paragraph 1, Item 2) It is desirable for a Full Member to determine documents to be submitted by a Principal at the time of a Demand, etc. for Disclosure, etc. (i) For a Principal For example, an application for disclosure of "Retained Personal Data," an application for change, etc., an application for utilization suspension, etc., and an identification document (ii) For a representative For example, in addition to documents in (i) above, a letter of attorney specified by a Full Member, and an identification document of a representative (3) Specific example of "other methods of receiving a Demand, etc. for Disclosure, etc." (Paragraph 1, Item 2) For example, multiple means are possible, such as visit, mails, and electronic means. (Note) Because restricting a method of a Demand, etc. for Disclosure, etc. to visit may "impose excessive burden on a Principal," it is desirable to provide an alternative method. [Reference provisions, etc.] Article 32 of the Protection Act, 3-5-6 of the General Rules GL, Article 15 of the Finance Sector GL

Guidelines for Protection of Personal Information	Explanations
(3) Method of confirming that a person who makes a Demand, etc. for Disclosure, etc. is the Principal or a representative (meaning a legal representative for a minor or adult ward, or a representative entrusted by the Principal; the same shall apply in this article)	(4) Specific Examples of "Method for identity verification" (Paragraph 1, Item 3) Adequate and appropriate identification procedures shall be established, including identification procedures based on the provisions of the Crime Proceeds Transfer Prevention Act or identification procedures at the same level. It should be noted that the term "representative" used herein shall be limited to a representative set forth in Article 11 of the Enforcement Order, not a transaction representative stipulated in the internal rules, etc. by each Full Member. [Reference provisions, etc.] Article 32 of the Protection Act, 3-5-6 of the General Rules GL, Article 15 of the Finance Sector GL
(4) Amount of the fee in Article 33, Paragraph 1 of the Protection Act and method for collection thereof (including the case where such a demand, etc. is free of charge)	[Reference provisions, etc.] Article 32 of the Protection Act, 3-5-6 of the General Rules GL, Article 15 of the Finance Sector GL
(5) Matters necessary to identify Retained Personal Data that are subject to a Demand, etc. for Disclosure, etc.	(5) Specific examples of "matters necessary to identify Retained Personal Data" (Paragraph 1, Item 5) For example, a name, an address, a date of birth, a telephone number, the name of a transaction office, an account number, and the like are possible. In requesting these matters, it should be noted that convenience for a Principal shall be taken into consideration by providing information contributing to identification of such Retained Personal Data so that a Principal can easily and accurately make a Demand, etc. for Disclosure, etc. [Reference provisions, etc.] Article 32 of the Protection Act, 3-5-6 of the General Rules GL, Article 15 of the Finance Sector GL
(6) Method of replying to a Demand, etc. for Disclosure, etc.	(6) Specific example of a "method of replying to a Demand, etc. for Disclosure, etc." (Paragraph 1, Item 6) For example, there are the following methods. (i) By mail, telephone, e-mail, etc. (ii) Depending on information to be disclosed, a reply may not be made on the spot, but later. When disclosing an individual number in response to a request from a Principal, it is necessary to take measures to prevent others from seeing the scene in the case of face-to-face contact with a Principal, and it is desirable to send a document containing the individual number by mail with a tracking function in the case of mailing. [Reference provisions, etc.] Article 32 of the Protection Act, 3-5-6 of the General Rules GL, Article 15 of the Finance Sector GL
2. A Full Member shall decide on the following matters in addition to each item of the preceding paragraph as the procedures for cases where a representative makes a Demand, etc. for Disclosure, etc. A Full Member shall not be precluded from disclosing the relevant personal data directly only to the Principal in response to a Demand, etc. for Disclosure, etc. made by a representative.	

Guidelines for Protection of Personal Information	Explanations
(1) Method for identity verification of a representative	(7) Specific example of "method for identity verification of a representative" (Paragraph 2, Item 1) Verification procedures similar to those in (4) above shall be established.
(2) Method to confirm a representative's authority of representation	(8) Specific examples of a "method to confirm a representative's authority of representation" (Paragraph 2, Item 2) For example, there are the following methods. (i) Except letter of attorney predetermined by the Full Member, no other means are allowed. (ii) Even if a letter of attorney, etc. is submitted, when any special circumstances suggesting the letter of attorney are found, the information shall not be disclosed until the Principal's intention to grant the authority of representation can be confirmed by telephone, etc. (ii) When the authority of representation cannot be confirmed by the method predetermined by the Full Member, the authority shall not be disclosed. [Reference provisions, etc.] Article 32 of the Protection Act, Article 10 of the Enforcement Order, 3-5-6 of the General Rules GL, Article 15 of the Finance Sector GL
3. A Full Member must, in establishing a procedure for Demand, etc. for Disclosure, etc. based on the provisions of the preceding two paragraphs, give consideration so as not to impose excessive burden on a Principal.	
Article 20. Fees 1. A Full Member may, when having been requested to inform of a utilization purpose pursuant to the provisions of Article 14, Paragraph 2 or when having receiving a demand for disclosure pursuant to the provisions of Article 15, Paragraph 1, collect a fee in relation to taking such action. 2. A Full Member must, in case of collecting a fee pursuant to the provisions of the preceding paragraph, decide on the amount of the fee within a range recognized as reasonable considering actual expenses.	In determining the amount of the fee within the scope deemed reasonable in consideration of actual costs, a Full Member is to endeavor to calculate the fee amount reasonably based on the estimated average actual costs of procedures for disclosure, etc. with similar contents. [Reference provisions, etc.] Article 33 of the Protection Act, 3-5-7 of the General Rules GL
Article 21. A Full Member's Dealing with a Complaint 1. A Full Member must strive to deal appropriately and promptly with a complaint about the handling of Personal Information. 2. A Full Member must strive to establish the system necessary to achieve a purpose under the preceding paragraph through setup of a contact point for receiving complaints, formulation of procedures for dealing with complaints, provision of sufficient education and training to officers and employees engaging in dealing with complaints, and other means.	[Reference provisions, etc.] Article 35 of the Protection Act, 3-6 of the General Rules GL, Article 16 of the Finance Sector GL
Article 22. Response to Personal Information Leakage or Other Incidents 1. In the event of the leakage of any personal information or the leakage of information concerning descriptions, etc. and Personal Identification Codes	(1) Personal Information Leakage or Other Incidents includes accidents due to loss or damage. (2) In the event of incorrect delivery, incorrect transmission, etc. of mails, e-mails, facsimile, and

Guidelines for Protection of Personal Information	Explanations
deleted from personal information used to produce Anonymously Processed Information and information relating to a processing method carried out pursuant to the provisions of Article 36, Paragraph 1 of the Protection Act (hereinafter referred to as "Personal Information Leakage or Other Incidents"), a Full Member is to immediately report that incident to the Financial Services Agency and the Association. If, in addition to Personal Information Leakage or Other Incidents, leakage of specific personal information specified in Article 2, Paragraph 8 of the Act on the Uses of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 27 of 2013) occurs, a Full Member shall also report the incident to the Personal Information Protection Commission. 2. In the event of any of Personal Information Leakage or Other Incidents, a Full Member is to disclose the facts concerning the incident and preventive measures to the public without delay from the perspective of preventing secondary damage or the occurrence of any similar incidents. 3. In the event of any of Personal Information Leakage or Other Incidents, a Full Member is to promptly inform the Principal involved in the relevant incident of the facts concerning the incident.	others, even if the loss of the content, etc. is minor, the incident needs to be made public when secondary damage or similar incidents could occur. (3) When leakage, etc. of specific personal information occurs, it is necessary to make reports, etc. in accordance with measures to be taken in the event of leakage, etc. of specific personal information as stipulated by the Personal Information Protection Commission and the Financial Services Agency. [Reference provisions, etc.] Basic Policy, Article 17 of the Finance Sector GL, Anonymous Processing GL
Article 23. Formulation of the Pronouncement Concerning Protection of Personal Information 1. In consideration of the significance of explaining policies related to Personal Information in advance in an easy-to-understand manner, a Full Member is to formulate the pronouncement concerning its ideas and policies concerning protection of Personal Information (so-called privacy policy or privacy statement, etc.; hereinafter referred to as the "Pronouncement Concerning Protection of Personal Information") and disclose it to the public. 2. For example, the Pronouncement Concerning Protection of Personal Information is to include the following matters. (1) Pronouncement of policies concerning protection of Personal Information, such as the compliance with related laws and regulations, etc., prohibition of utilization of Personal Information for unintended purposes and proper processing of complaints (2) Simple explanation of procedures for notification and public disclosure of the utilization purposes of personal information under Article 18 of the Protection Act (3) Simple explanation of procedures for disclosure, etc. under Article 27 of the Protection Act or other various procedures for handling of Personal Information (4) Contact information on offices processing inquiries and complaints concerning handling of Personal Information 3. A Full Member shall strive to incorporate as many descriptions as possible in consideration of the following points, depending on the characteristics,	(1) The title, form, content, composition, etc. of public disclosure may be at the discretion of each Full Member. (2) Specific examples of a method to disclose to the public For example, there are the following methods. (i) Posting or keeping posters, documents, etc. at the counter of business offices, etc. (ii) Description in and distribution of pamphlets (iii) Posting on an online website Care should be taken to make the disclosed information easy to see and understand for the users, and it is also possible to describe it by item separately in multiple media. For example, it is possible to add a note to the relevant part of the "Pronouncement Concerning Protection of Personal Information" that is currently published, and then provide a link to the website for specific examples of the type of outsourced works and sources of acquiring Personal Information to direct people to the detailed explanation. [Reference provisions, etc.] Article 18 and Article 27 of the Protection Act, Basic Policy, Article 18 of the Finance Sector GL

Guidelines for Protection of Personal Information	Explanations
scale, and actual status of business activities, from the perspective of protecting rights and interests of a Principal, including general consumers, in the Pronouncement Concerning Protection of Personal Information. (1) When a Principal makes a request, a Full Member is to suspend sending of direct email or otherwise voluntarily suspend the utilization of the Retained Personal Data. (2) A Full Member is to endeavor to increase transparency regarding outsourcing, such as clarifying whether it outsources any business or the content of outsourced business if any. (3) A Full Member is to devise means to clarify utilization purposes for the respective Principal, through efforts such as presenting limited utilization purposes separately by the type of customers in consideration of the business contents or voluntarily endeavoring to limit utilization purposes based on each choice by a Principal. (4) A Full Member is to indicate sources and methods of acquiring Personal Information (types of information sources, etc.) as concretely as possible.	(3) Specific examples of "a Full Member is to endeavor to increase transparency regarding outsourcing, such as clarifying whether it outsources any business or the content of outsourced business if any" (Item 2) For example, if it is difficult to list all outsourced clerical works due to their large number, it is considered that giving examples contributes to transparency regarding outsourcing. (Example) The Company outsources a part of our business operations. In addition, business operations in which the Company has outsourcing contractors handle Personal Information include the following operations. - Printing or forwarding of documents to be sent to customers - Provision of professional advice, etc. from the standpoint of law, accounting, etc. - Works related to operation and maintenance of information systems (4) Specific examples of "A Full Member is to indicate sources and methods of acquiring Personal Information (types of information sources, etc.) as concretely as possible." (Item 4) For example, when the number of sources or methods of acquiring Personal Information is large, showing them an example is considered to contribute to protection of rights and interests of a Principal. (Example) Sources of acquiring Personal Information to be obtained by the Company are as follows. - Information directly provided by customers in an application for opening an account, questionnaires, etc. - Information contained in commercially available books such as quarterly corporate reports and executive officers' reports and information published in newspapers and on the Internet - Information heard from customers through the provision of goods and services (* If phone calls are recorded, it is possible to include such information as well)
Article 24. Review of the Guidelines The Guidelines shall be reviewed as necessary.	[Reference provisions, etc.] Article 19 of the Finance Sector GL

Guidelines for Protection of Personal Information	Explanations
Article 25. Report to the Association, etc. 1. The Association may request a Full Member to make a report where appropriate to confirm the Full Member's compliance with the Guidelines. 2. The Association shall provide guidance and recommendations and take other measures necessary to have Full Members comply with the Guidelines. 3. A Full Member must comply with the Guidelines and follow necessary guidance and recommendations provided, and other measures taken by the Association.	[Reference provisions, etc.] Article 53 of the Protection Act

Supplementary Provision

This amendment will come into effect on July 15, 2021.

* Amended sections, etc. are explanations of the following articles, etc.
- Revision: Article 13 (5), Article 13-2 (1), Article 23 (2), Reference provisions, etc.
- Establishment and addition: *1 and* 2 of Article 2 (3), Article 4 (3), proviso to Article 7 (2) and thereafter, and (Note) of (4), Article 8 (7) (v), Article 10 (4) (v), (Note) of (12) and (12-1) of Article 13