【 Tentative translation : only Japanese text is authentic 】

Guidelines for Personal Information Protection in the Financial Field

Article 1. Purpose (relevant to Article 1 of the Law)

1. This guideline intends to provide a lodestar to attain an appropriate and effective implementation of actions that need to be taken by entities handling personal information, reflecting the characteristics of personal information in the financial field and the way they are used, in order to support activities to ensure the appropriate handling of personal information by such entities in the field (Herein after referred to as "financial field") designated in Paragraph 1, Article 36 of the "Act on the Protection of Personal Information" (Act No. 57 of 2003. Herein after referred to as "the Law"), and fields under the jurisdiction of the Financial Services Agency, taking into consideration the Law, the "Order for Enforcement of the Act on the Protection of Personal Information" (Order No. 507 of 2003. Herein after referred to as "the Order for Enforcement"), and the "Basic Policy on the Protection of Personal Information" (Cabinet Decision on April 2nd, 2004. Herein after referred to as "the Basic Policy").
2. As for respective authorized personal information protection organizations in the financial field (Entities authorized under Paragraph 1 of Article 37 of the Law. The same shall apply herein after.) and entities handling personal information, etc., it is important to lay down additional measures as voluntary rules based on this guideline, to ensure the appropriate handling of personal information in a way that takes into consideration respective entities' situation and to ensure the compliance with the rules both by themselves and by target entities.

   As for entities handling personal information in the financial field, they need to act in accordance with the relevant laws and regulations, etc. on the appropriate management of personal information in order to prevent the wrongful leakage of personal information.
3. Those who are using personal information database, etc. for business in the financial field and are excluded from "an entity handling personal information" by the provision of Item5, Paragraph 3, Article 2 of the Law shall endeavor to comply with the guideline.

Article 2. Definitions, etc. (Article 2 of the Law, Article 1 to 4 of the Order for Enforcement)

1. "Personal information" means information about a living individual which can identify the specific individual by name, date of birth or other description included in the information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual).

   It should be noted that "information about the deceased" handled by entities handling personal information can also constitute information about living individuals such as members of the bereaved family, etc.
2. "A personal information database, etc. " means a set of information including personal information that is systematically arranged in such a way that specific personal information can be retrieved by a computer, or if computer is not used, personal information that is arranged according to a certain set of rules to enable the easy retrieval of specific personal information and thereby are organized systematically, such as in customer card form, etc. set in Japanese character order, and are generally considered to be in a state wherein personal information can be readily attained by list of contents, indexes, and symbols, etc.
3. The "personal information number" prescribed in Article 2 of the Order for Enforcement

shall be determined by "the specific number of individuals identified by the personal information which constitutes the personal information database for the business". Even if the database is managed by others, if the database is used for business, the number of specific individuals that form the personal information database shall also be included in the "number of individuals".

4. "Personal data" means personal information constituting a personal information database, etc. This includes information that has been downloaded from personal information database, etc. to recording medium and information that has been printed out (or copies of the printout).
5. "Retained personal data" means such personal data over which an entity handling personal information has the authority to disclose, to correct, add or delete the content, to suspend its use, to erase, and to suspend its provision to third parties, excluding the data which will be harming public or other interests if its presence or absence is known and the data which will be erased within a period of no longer than six months (excluding revision of data).

"Data which will be harming public or other interests if its presence or absence is known" consists of any data that falls under any of the following items.

① Data that is likely to pose a threat to the life, body, or property of the party or the third party if its presence or absence is known.

② Data that is likely to aid or trigger unlawful or unjust acts if its presence or absence is known.

(e.g.) In cases in which an entity handling personal information holds personal data of a concerned group to prevent damage caused by unjust claim from the so called corporate racketeer.

③ Data that is likely to endanger national security, damage mutual trust relationship with other countries or international organization, or cause disadvantage in the course of negotiation with other countries or international organization if its presence or absence is known.

④ Data that is likely to impede the maintenance of public safety and order such as prevention, suppression or investigation of crime if its presence or absence is known.

(e.g.) In cases in which an entity receives an investigation related inquiry from the police and holds personal data of the suspect in the course of answering the inquiry.

6. " Personal credit data institution" refers to an institution whose business is to provide information on personal debt-paying ability to entities handling personal information that engage in credit business and collect information on personal debt-paying ability.
7. As prescribed in the respective preceding paragraphs, unless stated otherwise, the terms in this guideline is in conformity with the definition of the Law and the Order for Enforcement.

Article 3. Specification of the Purpose of Use (relevant to Article 15 of the Law)

1. Entities handling personal information in the financial field shall comply with Article 15 of the Law and shall specify the Purpose of Use as much as possible so as to enable the person to reasonably guess what type of business the personal information will be used for and the purpose of its use.

Specifically, an abstract Purpose of Use such as "(the information) will be used in a purpose required by our company" shall not be considered as sufficiently specific "Purpose of Use". It is desirable to specify the Purpose of Use after presenting the financial instruments or services that will be provided, the following can be considered as examples.

(Examples)

- Cases in which our company accepts deposits.

- Cases in which our company makes decision regarding credit extension, and credit exposure management.
- Cases in which our company underwrites insurance, and cases in which it pays insurance money and insurance benefits.
- Cases in which we conduct sales and soliciting activities for our services and financial instruments provided by our company or our affiliate company or our business partner.
- Cases in which our company, or affiliated company or our business partner, offers subscription of insurance.
- Cases in which we conduct market research and research and development of financial instruments and services within our company.
- Cases in which we check the qualification for purchasing specific financial instruments and services

2. In the case in which the Purpose of Use for specific personal information is limited by laws and regulations, an entity handling personal information in the financial field shall clearly indicate so.
3. In the case in which an entity handling personal information in the financial field acquires personal information in the course of conducting credit business, the entity shall need to acquire the person's consent regarding the Purpose of Use, and the provision on the Purpose of Use in the contract, etc. shall be printed clearly apart from other provisions in the contract. In this case, the entity should not exploit its advantageous business position and force the person to agree with the Purpose of Use that allows using personal information attained in the course of conducting credit business for other business than credit extension such as sending direct mails for financial instruments as a condition of credit extension. The person can reject the Purpose of Use pertaining to sending of direct mails.
4. In the case where an entity handling personal information in financial field provides personal information to personal credit data institution in the course of conducting credit business, the entity will state this clearly in the Purpose of Use. Furthermore, the entity needs to acquire the consent of the person on clearly stated Purpose of Use.

Article 4 Regarding the Format of Consent (relevant to Article 16 and 23 of the Law)

When acquiring the consent of the person prescribed in Article 16 and 23 of the Law, entities handling personal information in the financial field shall, in principle, do so by document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. Hereinafter this applies).. If an entity is using a previously prepared document for consent, it is desirable for the provisions on handling of personal information to be clearly distinguished from other provisions and ensure that the person understands the provision on handling of personal information by changing the size of letters and expression of sentences, etc.. Or, it is desirable to confirm by method that clearly reflects the person's intent, such as by setting a check box in the previously prepared document for consent that needs to be ticked by the person etc.

Article 5 Restriction by the Purpose of Use (relevant to Article 16 of the Law)

1. According to Article 16 of the Law, an entity handling personal information in financial field must not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Use specified under Article 15 of the Law.
2. When an entity handling personal information in financial field has acquired personal information as a result of taking over the business of another entity handling personal

information in a merger or otherwise, the acquiring entity must not handle the personal information concerned, without obtaining the prior consent of the persons, beyond the scope necessary for the achievement of the Purpose of Use of the personal information concerned before the take-over.

3. The provisions of the preceding two paragraphs shall not apply to the following cases:

① Cases in which the handling of personal information is based on laws

(Examples)

- Cases in which tax authorities conduct an interrogative inspection pursuant to Paragraph 1, Article 234, Income Tax Law (Act No.33 of 1965) and crime cases in which accepting voluntary investigations conducted by revenue official or revenue agent pursuant to Article 1, National Tax Crime Control Law (Act No.67 of 1900)
- Cases in which answering inquiries relevant to investigation based on Article 197, Code of Criminal Procedure (Act No.131 of 1948)
- Cases in which reporting suspicious transaction pursuant to Paragraph 1, Article 9, Act on Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007)

② Cases in which the handling of personal information is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person.

(Example)

- Cases in which collecting information on illegal activities committed by the so- called corporate racketeer or gangsters.

③ Cases in which the handling of personal information is specially necessary for improving public hygiene or promoting the sound growth of children and in which it is difficult to obtain the consent of the person.

(Example)

- Cases in which exchanging information for the purpose of research, etc. on prevention and curing of diseases

④ Cases in which the handling of personal information is necessary for cooperating with a state institution, a local public body, or an individual or entity entrusted by one in executing the operations prescribed by laws and in which obtaining the consent of the person might impede the execution of the operations concerned

(Example)

- Cases in which accepting voluntary investigations conducted by tax authorities for the purpose of realizing fair taxation, rather than investigations based on individual interrogative inspection rights.

Article 6 Regarding Sensitive Information

1. An entity handling personal information in the financial field shall not acquire, use, or provide to third party, information on political views, religion (meaning thoughts and creed), participation in union activities, race, family origin and registered domicile, health care, sex life and past criminal records (hereinafter referred to as “sensitive information”) other than the cases listed below.

① Cases in which the provision of personal data is based on laws, etc.

② Cases in which the provision of personal data is necessary for the protection of the life, body, or property of an individual

③ Cases in which the provision of personal data is specially necessary for improving public hygiene or promoting the sound growth of children

④ Cases in which the provision of personal data is necessary for cooperating with state

institution, a local public body, or an individual entity entrusted by one in executing the operations prescribed by laws.

⑤ Cases in which acquiring, using, and providing sensitive information to a third party within the purview of political or religious groups or labor unions affiliated to the employee within the range necessary for the execution of administrative procedures for tax collection at source, etc. is necessary.

⑥ Cases in which acquiring, using, and providing sensitive information to a third party within the range necessary for the execution of the transfer of rights and obligations arising from inheritance procedures is necessary.

⑦ Cases in which acquiring, using, and providing sensitive information to a third party within the range necessary for the execution of business operation based on the consent of the person, in order to secure an appropriate conduct of business operation in insurance and other financial field businesses, is necessary.

⑧ Cases in which the use of biometrical information, falling under the category of sensitive information for personal identification and based on the person's consent, is necessary.

2. An entity handling personal information in the financial field shall handle the information with great caution when acquiring, using or providing sensitive information on the grounds prescribed in the respective items of the previous paragraph to the third party, not to acquire, use or provide the information in a manner that does not comply with the grounds prescribed in the respective items.

Article 7 Proper Acquisition (relevant to Article 17 of the Law)

1. An entity handling personal information in the financial field must act in accordance with Article 17 of the Law and must not acquire personal information by a fraudulent or other dishonest means. When an entity acquires personal information from a third party, it should not unjustly infringe the person's interest, and the entity should not acquire personal information from a third party knowing that the personal information has been leaked from the party who conducted unjust actions such as wrongful acquisition of personal information.

Article 8 Notice of the Purpose of Use at the Time of Acquisition, etc. (relevant to Article 18 of the Law)

1. According to Paragraph 1, Article 18 of the Law, it is stated that, when having acquired personal information, an entity handling personal information must, except in cases in which the Purpose of Use has already been publicly announced, promptly notify the person of the Purpose of Use or publicly announce the Purpose of Use.

   As for the method of "notification", in principle an entity handling personal information in financial filed should do so in writing.

   As for the method of making "public announcements," an entity handling personal information in the financial field must do so according to its business' manner of conducting product sales, etc. and in an appropriate manner such as releasing the information on its home page, or posting the document at the counter of its office, or making the document readily available at the counter, etc.

2. According to Paragraph 2, Article 18 of the Law, notwithstanding the provision of the preceding paragraph in the Law, when an entity handling personal information acquires such personal information on a person as is written in an agreement or other document as a result of concluding an agreement with the person, the entity must expressly show the Purpose of Use in advance. In the credit business, it is desirable for the entity handling personal information in the financial field to gain the consent of the person regarding the Purpose of

Use by setting a check box in the document that clearly indicates the Purpose of Use.
Also, in the credit business, when gaining consent regarding the Purpose of Use at the time of offer, this personal information which has gained the person's consent at the time of offer, does not need to be "notified or publicly announced" pursuant to Paragraph 1, Article 18 of the Law. However, as for information acquired after this, the notification and public announcement of the Purpose of Use is necessary unless the Purpose of Use has been publicly released in advance.

3. According to Item 4, Paragraph 4, Article 18 of the Law, in cases when "it is considered that the Purpose of Use is clear in consideration of the circumstances of the acquisition", notification, public announcement or clear indication are excluded from the application.
An example of cases wherein "it is considered that the Purpose of Use is clear in consideration of the circumstances of the acquisition" is in a case wherein documents have been requested by phone, etc. and information provided by the requestor regarding his or her name and address is used only for the purpose of sending the requested documents.

Article 9 Maintenance of the Accuracy of Data (relevant to Article 19 of the Law)

In accordance with Article 19 of the Law, an entity handling personal information in the financial field must endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of the Purpose of Use.
Thus, entities must determine the retention period of the retained personal data according to their Purpose of Use such as fixing the retention period for personal information for depositors or insurance contractors will be within a certain period after the expiry of the contract, etc. Personal data will be deleted following this period.
However, this shall not apply to cases in which retention period is otherwise provided by other laws and regulations, etc.

Article 10 Security Control Measures (relevant to Article 20 of the Law and the Basic Policy)

1. An entity handling personal information in the financial field must take necessary and suitable measures on development of implementation structure pertaining to security control measures and basic guidelines and development of rules pertaining to security control measures, for the prevention of leakage, loss, or damage, and for other control of security of the personal data that it handles. The necessary and appropriate measures must include "Institutional Security Control Measures," "Human Security Control Measures," "Technological Security Control Measures" which are laid out according to the respective levels of acquisition, usage and retention of personal data.
2. "Institutional Security Control Measures" in this article refer to framework development and implementation measures for entities handling personal information such as clearly stating the responsibility and powers of the employee concerned to ensure the control of security of the personal data (refer to Article 21 of the Law) and developing and implementing rules, etc. on security control and conducting inspection and audit of their performance status, etc.
3. "Human Security Control Measures" in this article mean supervising the employees to realize security control of personal data by concluding contract on non disclosure of personal data with employees and by educating and training employees.
4. "Technological Security Control Measures" in this article mean technological measures on security control of personal data, such as controlling access to personal data and information systems that handle personal data and monitoring information systems, etc.
5. As an undertaking to develop Basic Guidelines and Rules Pertaining to Security Control

Measures of Personal Data, an entity handling personal information in the financial field, must implement the "Institutional Security Control Measures" as listed below.

(Institutional Security Control Measures)

(1) Development of Rules, etc.

①Development of basic guidelines pertaining to security control measures for personal data

②Development of rules pertaining to security control measures for personal data

③Development of rules pertaining to inspection and audit for the handling situation for personal data

④Laying down rules pertaining to outsourcing

(2) Rules pertaining to security control at respective control stages

① Rules for acquiring and inputting stages

② Rules for using and processing stages

③ Rules for retention stage

④ Rules for transferring and sending stages

⑤ Rules for deleting and disposing stages

⑥ Rules for responding to cases of information leakage

6. As an undertaking to develop implementation structures pertaining to security control measures of personal data, an entity handling personal data in the financial field, must implement the "Institutional Security Control Measures," "Human Security Control Measures," and "Technological Security Control Measures" as listed below.

(Institutional Security Control Measures)

① Assigning employees responsible for controlling personal data, etc.

② Developing security control measures in rules of employment, etc.

③ Operation complying with rules pertaining to security control measures for personal data

④ Developing measures to confirm the handling situation for personal data

⑤ Developing and implementing inspection and audit framework for the handling of personal data

⑥ Developing framework to respond to instances of leakage

(Human Security Control Measures)

① Concluding contracts on non disclosure of personal data with employees

② Clarifying employees' roles and responsibilities, etc.

③ Familiarizing, educating, training employees on security control measures

④ Confirming employees' compliance with personal data management procedures

(Technological Security Control Measures)

① Identifying and authenticating personal data users

② Controlling access and setting up management classifications for personal data

③ Managing access authority for personal data

④ Setting up preventative measures against leakage and damage to personal data

⑤ Recording and analyzing access to personal data

⑥ Recording and analyzing operational status of information systems handling personal data

⑦ Monitoring and auditing information system handling personal data

Article 11 Supervision of Employees (relevant to Article 21 of the Law and the Basic Policy)

1. Complying with Article 21 of the Law, an entity handling personal data in the financial field, must exercise the necessary and appropriate supervision over the employee and establish an appropriate internal management framework to ensure the control of security of

the personal data.

2. "Employee" in this article refers to those who are under the direct or indirect supervision and command of an entity within the institution of the entity handling personal information and are engaged in the entity's operation. This includes not only those who are in employment relationships (permanent employee, contract employee, temporary employee, part-time worker, non-regular worker, etc.) but also those who are not in employment relationship with the entity (executive director, executive officer, director, inspector, dispatched member, etc.).
3. Entities handling personal information in the financial field must exercise necessary and appropriate supervision over the employee by establishing the following frameworks.
   ① Conclude contracts at the time of employment that ensures the employee will not use or let the third party know personal data the employee may have acquired in the course of conducting its business or after the employee's resignation from the business for purposes other than those stated in the Purpose of Use.
   ② Clarify the roles and responsibilities of the employees, familiarize employees with their control of security obligation, and conduct education and training by way of formulating rules pertaining to appropriate handling of personal data.
   ③ Develop an inspection and auditory framework for personal data protection by employees and lay down a confirmation framework to check on their compliance with the items prescribed in the internal security control measures to prevent employees from taking out personal data.

Article 12 Supervision of Trustees (relevant to Article 22 of the Law and the Basic Policy)

1. When an entity handling personal information in the financial field entrusts an individual or entity with the handling of personal data in whole or in part, according to Article 22 of the Law, it must exercise necessary and appropriate supervision over the trustee to ensure the control of security of the entrusted personal data.
2. "Entrust" includes all contracts that specify the entity handling personal information in the financial field to outsource the whole or part of the handling of personal data to other entity or individual, regardless of the form or type of the contract.
3. Entities handling personal information in the financial field are required to select an entity or an individual who is recognized to handle personal data appropriately and to make sure that measures for control of security of personal data are put into practice at the entity or by the individual who has been entrusted with the handling of personal data. When the operation has been reallocated to two or more entities or individuals, the trustee must supervise whether the newly designated entity is conducting sufficient supervision.
   Specifically, an entity handling personal information in the financial field is requested to:
   ① Include the formulation of basic guidelines and rules pertaining to development of institutional frameworks and security controls in the standards for selecting trustees, and select trustees according to this standard, and regularly revise the standard, in order to ensure the personal data's control of security.
   ② Include measures for control of security that specifies trustees' responsibilities in cases of leakage of condition and information on re-entrustment, and that prohibits leakage, appropriation, falsification and use for purposes other than those stated in the Purpose of Use of the personal data at the trustee, and that specifies entruster's rights for supervision, audit, and collection of reports in the entrustment contract. And confirm the observance with measures for control of security prescribed in the entrustment contract on a regular or as needed basis, and revise the measure.

Article 13 Restriction of Provision to Third Parties (relevant to Article 23 of the Law)

1. According to Article 23 of the Law, an entity handling personal information in the financial field, must not, except in the following cases provide personal data to a third party without obtaining the prior consent of the person:
   ① Cases in which the provision of personal data is based on laws.
   ② Cases in which the provision of personal data is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person.
   ③ Cases in which the provision of personal data is specially necessary for improving public hygiene or promoting the sound growth of children and in which it is difficult to obtain the consent of the person.
   ④ Cases in which the provision of personal data is necessary for cooperating with a state institution, a local public body, or an individual or entity entrusted by one in executing the operations prescribed by laws and in which obtaining the consent of the person might impede the execution of the operations concerned.

   (Note) For examples for ①-④, see Paragraph 3, ①-④, Article 5.

   Also, the consent regarding provision to third parties will be obtained in a written document, in principle.

   Through the entry of the document, it will be understood that the person's consent is attained after the person's recognition regarding the following:
   ① Third parties to whom the personal data will be provided
   ② The Purpose of Use of the third party who has received the data
   ③ The contents of the information that will be provided to the third party
2. Regarding "third parties"

   "Third party" refers to physical persons, juridical persons and other groups that are not entities or individual handling personal information who provide the personal data, or the persons to whom the personal data pertains.
3. Provision to personal credit data institutions

   When providing personal data to personal credit data institutions, since the information will be provided to the member companies of the personal credit data institution, via the institution, an entity handling personal information responsible for providing personal data to personal credit data institution, shall attain the consent of the person.

   When attaining the person's consent, the person needs to be able to make a judgment regarding the consent after clearly recognizing the personal data will be provided to the member companies of the personal credit information institution via the institution. Thus, the entity will indicate in the document to attain the (person's) consent matters prescribed in Paragraph 1, the fact that personal data will be provided to the member companies of the institution, and the list of those who will be using personal data as the member companies of the institution.

   The list of "those who will be using personal data as member companies of the institution" needs to objectively and clearly indicate the denotation of "those who will be using personal data as the member companies of the institution", and the list will show this with sufficient concreteness that allows the person to decide whether to agree or disagree by means such as listing the names of the member companies, listing the home page address (matters prescribed in Article 23, such as contact address of the complaint handling section) that publicizes the institution's rules and names of member companies. Also, in the rules regarding the personal credit data institution that will be shown to the person, it will be

appropriate to clearly indicate the qualification for joining the institution and the denotation of the member companies, and to expressly state the measures for sanction against the breach of observance with confidentiality obligation and breach of obligation for laying down framework for control of security confidentiality, from the view point of appropriate management of personal data and prevention of information use for purpose other than those stated in the Purpose of Use.

As for information regarding the debt service capacity of those who are in need of funds attained from personal credit information institutions, an entity handling personal information in the financial field will handle such information in a prudent manner so as not to use the information for purposes other than investigating the debt service capacity of those who are in need of funds.

4. In the 2nd Paragraph of Article 23 of the Law

In the 2nd Paragraph of Article 23 of the Law, with respect to personal data intended to be provided to third parties, where an entity handling personal information agrees to suspend, at the request of a person, the provision of such personal data as will lead to the identification of the person concerned, and where the entity, in advance, notifies the person of the matters enumerated in the respective items of the paragraph or put those matters in a readily accessible condition for the person, the entity may provide such personal data concerned to third parties.

"A readily accessible condition for the person" refers to a situation where the person can easily know (matters enumerated in the respective items of the Paragraph 2 of Article 23 of the Law) in terms of time and means if the person seeks to know about this. An entity handling personal information in the financial field needs to continuously publicize this in an appropriate manner in accordance with its business situation such as its method of conducting sales of financial products. For instance, methods such as consistently posting documents or making documents readily available at the office counter or posting the information on the internet homepage can be considered.

5. On the Application of Paragraph 2, Article 23 of the Law in Credit Business

Any entity handling personal information in the financial field will not apply Paragraph 2, Article 23 of the Law when providing personal credit information institution information regarding personal debt capacity pertaining to credit business, and shall attain the person's consent complying with Paragraph 3 of the article.

6. On 4th Paragraph, Article 23 of the Law

According to Paragraph 4, Article 23 of the Law, in the following cases, the individual or entity receiving such personal data shall not be deemed a third party:

① Cases in which an entity handling personal information entrust the handling of personal data in whole or in part within the scope necessary for the achievement of the Purpose of Use

② Cases in which personal data is provided as a result of the take-over of business in a merger or otherwise

③ Cases in which personal data is used jointly between specific individuals or entities and in which this fact, the items of the personal data used jointly, the scope of the joint users, the purpose for which the personal data is used by them, and the name of the individual or entity responsible for the management of the personal data concerned is, in advance, notified to the person or put in a readily accessible condition for the person

7. Regarding the 3rd Item in the 4th Paragraph of Article 23 of the Law

In principle, an entity handling personal information shall conduct "notification" as prescribed in 3rd Item in the 4th Paragraph of Article 23 of the Law in writing.

As for the notification of "the scope of the joint users" by entities, it is desirable to individually list the joint users . Also, in cases wherein notifying the person by indicating the denotation of the joint users, joint users are required to be specified, so that it is easy to understand for the person. Specific examples showing what denotation is are as follows:

・The company and its subsidiary which are listed in the Financial Report, etc.

・The company, its consolidated subsidiary, and its equity method affiliate which are listed in the Financial Report, etc.

"The individual or entity responsible for the management of the personal data" prescribed in the 3rd Item, 4th Paragraph, Article 23 of the Law refers to those among joint users who are responsible for the control of security and are the first receiver of complaints. They handle the complaints and also make a decision regarding the disclosure, correction, and suspension of the use of personal information. It should be noted that the purpose of this item is not to release joint users other than those who are responsible for the management of the personal data from responsibilities for control of security.

8. Transitional Measures

As for personal data provided to a third party prior to the enforcement of the Law, if there was an agreement equivalent to the person's consent prescribed in the Paragraph 1, Article 23 of the Law, prior to the enforcement of the Law, the information can be continuously provided to the third party after the enforcement of the Law (Article 3, Supplementary Provision to the Law). As for credit business conducted by an entity handling personal information prior to the enforcement of the Law, in cases wherein person's consent is attained for the provision of the personal data to the personal credit data institution, it is appropriate to publicize the rules of the institution regarding its member qualification and the name of the institution's members prior to the enforcement of the Law.

Article 14 Public Announcement of Matters concerning Retained Personal Data, etc. (relevant to Article 24 of the Law and Article 5, Order for enforcement)

Under Article 24 of the Law, an entity handling personal information in the financial field must put the matters prescribed in the respective items of the first paragraph in the article such as the Purpose of Use, procedures for disclosures on the retained personal data in an accessible condition for the person.,

"Accessible condition for the person" refers to a condition in which the person can gain access to the information if he or she seeks to do so. This needs to be coordinated in an appropriate manner in accordance with the entity's business situation such as sales method of financial instruments, and as examples for the continually publicizing, constantly posting the necessary information in conjunction with the "Pronouncement concerning Protection of Personal Information" prescribed in Article 23 in the homepage, or posting the information at the office counter or make the information readily available at the counter can be considered.

Also, when the provision of the information to the third party is included in the Purpose of Use, this needs to be stated as prescribed in Item 2, Paragraph 1 Article 24, "Purpose of Use of all retained personal data" of the Law.

Article 15 Disclosure (relevant to Article 25 of the Law)

Under Article 25 of the Law, when an entity handling personal information is requested by a person to disclose such retained personal data as may lead to the identification of the person concerned, the entity must disclose the retained personal data concerned without delay. However, according to Item 1, 2 and 3 for Paragraph 1, Article 25, in any of the

following cases, the entity may keep all or part of the retained personal data undisclosed.

① Cases in which disclosure harms the life, body, property, or other rights or interests of the person or a third party

② Cases in which disclosure seriously impedes the proper execution of the business of the entity concerned handling personal information

③ Cases in which disclosure violates other laws

As for ②, cases in which an entity handling personal information receives a request for disclosure for an information added by the entity, such as the entity's credit assessment, etc, or cases in which the disclosure of the retained personal data by an entity prevents adequate implementation of evaluation and tests can be considered. However, cases in which the amount of the retained personal data requested for disclosure is substantial alone will not be sufficient for the above ② to apply.

When an entity handling personal information in the financial field has decided not to disclose all or part of such retained personal data as is requested under the respective items of Paragraph1, Article 25, the entity must notify the person of that effect without delay and conduct an explanation for the reason of the decision by showing the fact that is used as the standard for judgment, and the text of the law which is used as the grounds.

Article 16 Correction, etc. (relevant to Article 26 of the Law and Article 6, Order for enforcement)

According to Article 26 of the Law, when an entity handling personal information is requested by a person to correct, add, or delete such retained personal data as may lead to the identification of the person concerned on the ground that the retained personal data is contrary to the fact, the entity must make a necessary investigation such as confirmation of facts, etc. without delay within the scope necessary for the achievement of the Purpose of Use and, on the basis of the results, correct, add, or delete the retained personal data concerned.

When an entity handling personal information has corrected, added, or deleted all or part of the retained personal data or has decided not to make such correction, addition, or deletion, the entity must notify the person of that effect (including the content of the correction, addition, or deletion if performed) without delay.

If the entity handling personal information in the financial field decides not to make any such corrections, additions, or deletions, the entity must explain their reasoning by indicating the grounds and the supporting facts.

Article 17 Stopping the Use, etc. (relevant to Article 27 of the Law)

1. Where an entity handling personal information in the financial field is requested by a person to stop using or to erase such retained personal data as may lead to the identification of the person concerned on the ground that the retained personal data is being handled in violation of Article 16 or has been acquired in violation of Article17, and where it is found that the request has a reason, the entity must stop using or erase the retained personal data concerned without delay to the extent necessary for redressing the violation. However, this provision shall not bind cases in which it costs a great deal or otherwise difficult to stop using or to erase the retained personal data concerned and in which the entity takes necessary alternative measures to protect the rights and interests of the person.
2. According to Paragraph 2, Article 27 of the Law, where an entity handling personal information in the financial field is requested by a person to stop providing to a third party such retained personal data as may lead to the identification of the person concerned on the

ground that the retained personal data is being provided to a third party in violation of Paragraph 1 of Article 23, and where it is found that the request has a reason, the entity must stop providing the retained personal data concerned to a third party without delay. However, this provision shall not bind cases in which it costs a great deal or otherwise difficult to stop providing the retained personal data concerned to a third party and in which the entity takes necessary alternative measures to protect the rights and interests of the person.

3. According to Paragraph 1, Article 27 of the Law, where an entity handling personal information in the financial field has stopped using or has erased all or part of the retained personal data as requested under Paragraph1 or has decided not to stop using or not to erase the retained personal data or when an entity handling personal information has stopped providing all or part of the retained personal data to a third party as requested under the Paragraph2 of the Article or has decided not to stop providing the retained personal data to a third party, the entity must notify the person of that effect without delay.

Article 18 Explanation of Reasons (relevant to Article 28 of the Law)

When an entity handling personal information notifies a person requesting the entity to take certain measures under Paragraph 3 of Article 24, Paragraph 2 of Article 25, Paragraph 2 of Article 26, or Paragraph3 of the Article 27 that the entity will not take all or part of the measures or that the entity will take different measures, the entity must endeavor to explain the reasons by showing the grounds for making the judgment that the entity will not take the measures or that the entity will take different measures and the supporting facts for the judgment.

Article 19 Procedures to Meet Requests for Disclosure and Others (relevant to Article 29 of the Law and Article 7, 8, Order for enforcement)

1. According to Article 29 of the Law, when an entity handling personal information in the financial field decides on how to accept requests for disclosures, etc, the entity must post the information on the homepage or post the information at the counter of the office or make the information readily available at the counter together with the “Pronouncement concerning Protection of Personal Information” prescribed in Article 23.
2. Based on Paragraph 3 of Article 29 of the Law and Item 3, Article 7 of the Order for Enforcement, in deciding the means to confirm whether the person who requests for disclosure is the representative prescribed in Article 8 of the Order for Enforcement, it should be noted that the confirmation procedures needs to be adequate and appropriate.

   In response to the representative’s request for disclosure stated in Item 2, Article 8 of the Order for Enforcement, it should not be prevented for the entity to directly disclose the information only to the person.

Article 20 Charges (relevant to Article 30 of the Law)

According to Article 30 of the Law, in cases of collecting charges, an entity handling personal information in the financial field must determine the amounts of charges within the scope considered reasonable in consideration of actual costs, by methods such as calculating the rational charges based on the expected average actual costs of the similar disclosure procedures.

Article 21 Handling of Complaints by Entities Handling Personal Information (relevant to Article 31 of the Law)

1. According to Article 31 of the Law, when an entity handling personal information in the

financial field receives a complaint regarding the handling of the personal information, the entity must investigate the complaint and endeavor to appropriately and promptly handle the complaint within a rational period.

2. An entity handling personal information in the financial field must endeavor to establish a system necessary to handle complaints appropriately and promptly such as formulating a manual for handling complaints, setting up a counter to hear complaints, conducting sufficient education and training for employees who will be handling complaints.

Article 22 Responding to Leakages (relevant to the Basic Policy)

1. An entity handling personal information must immediately report the supervisory authority when an accident regarding leakage of personal information occurs.
2. An entity handling personal information must promptly publicize the facts regarding the leakage accident and measures for preventing recurrence of the accident from a viewpoint to prevent secondary damage and avoid recurrence of similar accidents, in the case of an accidental leak of personal information.
3. An entity handling personal information in the financial field must notify the facts of the leakage accident promptly to the person whose personal information has been leaked, when an accidental leak of personal information.

Article 23 Formulation of pronouncement concerning protection of personal information (relevant to Article 18, 24 of the Law, and the Basic Policy)

Taking into consideration the importance of clear explanation of the orientation of efforts towards personal information beforehand, an entity handling personal information in the financial field must formulate a pronouncement on an entity's view and guidelines for personal information protection (the so called privacy policy, privacy statement. In this guideline it will be referred to as "pronouncement concerning protection of personal information") and publicize the pronouncement by means such as posting the following information on the homepage or the counter of the office or make the information readily available at the counter.

① Pronouncements concerning protection of personal information, including statements on observance of relevant laws and regulations, observance of engagement against use of personal information for purpose other than those stated in Purpose of Use, appropriate handling of complaints, etc.

② Clear explanation of procedures for the notification and publicizing of the personal information's Purpose of Use stated in Article 18 of the Law.

③ Clear explanation of procedures for the handling of personal information such as the procedures for disclosure stated in Article 24 of the Law.

④ Counter for the handling of complaints and questions regarding the handling of personal information.

--END--