Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information

March 2007

Ministry of Economy, Trade and Industry

Table of Contents

For more information, please contact

Information Economy Division of Commerce and Information Policy Bureau at Ministry of Economy, Trade and Industry of Japan

Phone: 81-3-3501-0397 (direct line)

1. Purpose and Scope of the Guidelines

These Guidelines, which are based on the "Policies Concerning the Protection of Personal Information" decided by the Japanese Cabinet on the 2nd of April 2004 in accordance with Paragraph 1 of Article 7 of the Act on the Protection of Personal Information (Act No. 57 of 2003; hereinafter referred to as "the Act") and specify pursuant to Article 8 of the Act the necessary matters concerning the matters set forth by the Act, are formulated as practical guidelines to support the activities performed by entities and others to ensure the proper handling of personal information in sectors, over which the Ministry of Economy, Trade and Industry holds jurisdiction, and specific sectors (hereinafter referred to as "economic and industrial sectors"), in which the Minister of Economy, Trade and Industry is designated as a competent minister pursuant to Paragraph 1 of Article 36 of the Act.

Although the Guidelines are the criteria when the Minister of Economy, Trade and Industry enforces the Act, certain parts of the Guidelines as are related to employees' personal information (in relation to employment management) was noted the consistency with the Guidelines Concerning Measures to be Taken by Entities to Ensure the Proper Handling of Personal Information Relating to Employment Management (Announcement No. 259 of 2004 by the Ministry of Health, Labour and Welfare). (Refer to [2-2-3-3. Supervision of Workers (an issue related to Article 21 of the Act)] for the definition of "employees" and "workers"). Therefore, such parts of the Guidelines were jointly formulated and enforced by the Minister of Health, Labour and Welfare and the Minister of Economy, Trade and Industry.

The noncompliance with the provisions which contain the term "must" in the Guidelines can be deemed the violation of the Act by the Minister of Economy, Trade and Industry. On the other hand, the noncompliance with the provisions which contain the term "preferable" can not be deemed the violation of the Act (refer to 3.). However, in line with the basic principle of the Act (Article 3 of the Act) that in consideration of the fact that personal information should be handled cautiously under the philosophy of respecting the personalities of individuals, proper handling of personal information should be promoted, it is desired to make efforts as far as possible for observing even the provisions which contain the term "preferable" from the viewpoint of promoting protection of personal information. Nonetheless, in light of the purport of the purpose of the Act (Article 1 of the Act) that the usefulness of personal information should be considered when the personal information is protected, it does not restrict even activities necessary for public interests and reasonable business activities.

The parts described in the Guidelines as case examples show typical examples in both, an instance which comes under the provision and an instance which does not come, for helping people understand. Those descriptions do not aim to cover all case examples. Practically an examination is necessary in each individual case. Also only some types of business are covered but not all types.

Additionally, in view of the nature and the method of utilization of personal information as well as the particularity of business realities, when it is expressly necessary to ensure the proper handling of personal information in cases which correspond to the category of economic and industrial sectors, the Minister of Economy, Trade and Industry may take further measures separately. Also the authorized personal information protection organizations (organizations authorized under Paragraph 1 of Article 37 of the Act; the same shall apply hereinafter) may draw up personal information protection guidelines set forth in

Paragraph 1 of Article 43 of the Act. Moreover, based on its business realities, a trade association, etc. may draw up and revise the guidelines of trade association which are the voluntary rules targeting the member companies of the trade association. When handling personal information in these cases, it is necessary to respond in conformity with the above stated further measures, personal information protection organizations, and guidelines of trade association.

2. Legal Interpretation Guidelines and Case Examples

2-1 Definitions (issues related to Article 2 of the Act)

2-1-1 [Personal Information] (an issue related to Paragraph 1 of Article 2 of the Act)

Paragraph 1 of Article 2 of the Act
In this Act, "personal information" means information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual).

The term “personal information”*1 means “information about an individual” who is living, and which can identify the specific individual (including such information*2 as will allow easy reference to other information and will thereby enable the identification of the specific individual). The “information about an individual” is not limited to such information which can identify the specific individual as name, sex and date of birth etc. but all information which represents facts, judgments, and assessments about personal attribute such as body, assets, kind of occupation and title, and includes assessment information, publicized information by officially printed publications, visual information, and sound information regardless of concealment of information by encryption, etc. (However, it is preferable to take concealment measures by advanced encryption as part of [2-2-3-2. Security Control Measures (issues related to Article 20 of the Act)].

Also, when the information about a dead individual is that about a living individual including a family member of the deceased at the same time, it becomes the information about such living individual.

The scope of “living individual” is not limited to Japanese nationals but includes foreign nationals. Meanwhile, since a juridical person and another organization do not correspond to “an individual”, the information about an organization, including a juridical person, itself is not targeted in the Guidelines (However, the information about officers and employees is personal information.).

*1 The Act distinguishes among three terms of “Personal Information”, 2-1-4. “Personal Data”, and 2-1-5. “Retained Personal Data”, and the duties imposed on entities handling personal information differ from one entity to another. Accordingly, a careful attention is required.

*2 The phrase “will allow easy reference to other information-----” means, for example, a condition in which it is able to access a personal information database, etc. and collate

information within the bounds of usual work, and excludes a condition in which it is difficult to collate information because of the necessity to inquire of other entities.

[Cases corresponding to personal information]

Case 1 Name of the person

Case 2 Combined information of the name of the person and the date of birth, contact point (address, whereabouts, telephone number, and e-mail address), duty position in the company, or information about professional affiliation

Case 3 Image information by which the person can be identified including information recorded in security cameras

Case 4 E-mail address information by which the specific individual can be identified (including a case of even only e-mail address information like keizai_ichiro@meti.go.jp that can be identified as the e-mail address of KEIZAI Ichiro who is belonging to the Ministry of Economy, Trade and Industry - a government organization in Japan)

Case 5 Information that can identify the specific individual by recognizing in supplementing well known information even though it has no description of information by which the specific individual can be identified

Case 6 Employment management information (including employee assessment information by the company)

Case 7 Information about an individual added to the personal information after it is acquired (even though the living specific individual can not be identified when the information is acquired, if the living specific individual can be identified in consequence that new information is added to or collated with the information after acquisition, such information will become personal information at that point.)

Case 8 Publicized information by official gazettes, telephone directory, and directory of government officials, etc. (including the name of the person)

[Cases not corresponding to personal information]

Case 1 Information such as the financial information of a company about an organization, including juridical person, itself (organization information)

Case 2 E-mail address information which is indistinctive whether it is the information of the specific individual or not because of a character string consisting of only symbols and numeric (The abc012345@xyzisp.jp is an example. However, when the information enables the identification of the specific individual by being collated with other information, such information comes under personal information.)

Case 3 Statistical information which does not enable the identification of the specific individual

2-1-2 [Personal Information Database, etc.] (an issue related to Paragraph 2 of Article 2 of the Act)

Paragraph 2 of Article 2 of the Act

In this Act, "a personal information database, etc." means a set of information including personal information as set forth below:

(1) a set of information systematically arranged in such a way that specific personal information can be retrieved by an electronic computer; or

(2) other than those described in the preceding paragraph, a set of information designated by a Cabinet order as being systematically arranged in such a way that specific personal information can be easily retrieved.

Article 1 of the Cabinet Order for the enforcement of the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003; hereinafter referred to as "the Cabinet Order")

The category of information designated by a Cabinet Order under Item 2 of Paragraph 2 of Article 2 of the Act on the Protection of Personal Information (hereinafter called the "Act") is a set of information systematically arranged in such a way that specific personal information can be easily retrieved by organizing personal information contained therein according to certain rules, and has a table of contents, an index, or other arrangements that aids in retrieval.

The term "personal information database, etc." means an assembly of information which includes personal information and is systematically arranged in such a way that specific personal information can be retrieved by a computer, or such an assembly of information, which is not processed by a computer and in a condition where others can easily retrieve, as a medical record and a cumulative guidance record in which personal information processed on paper is organized and classified according to certain rules (for example, the order of the Japanese syllabary, etc.), and has a table of contents, an index, or a code, etc. in order for the easy retrieval of specific personal information.

[Cases corresponding to the personal information database, etc.]

Case 1 E-mail address book which is stored in an e-mail software (where combined information of e-mail address and name is inputted)

Case 2 Electronic file in which user IDs and log information on transactions by users are stored (where a user ID is managed in connection with personal information)

Case 3 Condition in which a worker inputs and organizes business card information by using a spreadsheet software, etc. of a personal computer for business use (no matter who owns it) and other workers, etc. can retrieve it

Case 4 Registration cards of temporary staffs which are organized according to names arranged in the order of the Japanese syllabary and filed with indexing according to the order of the Japanese syllabary by a temporary staffing company

Case 5 Commercially available directory which is classified and organized by names, addresses, and companies

[Cases not corresponding to the personal information database, etc.]

Case 1 Condition in which although a worker leaves his/her business card case being freely retrieved by others, the worker classifies business cards according to an original classification method by which others cannot easily retrieve

Case 2 Returned questionnaire postcards which are not classified and organized according to names and addresses, etc.

2-1-3 [Entity Handling Personal Information] (an issue related to Paragraph 3 of Article 2 of the Act)

Paragraph 3 of Article 2 of the Act

In this Act, "an entity handling personal information" means an entity using a personal information database, etc. for its business; however, the following entities shall be excluded;

(1) The State institutions

(2) Local public bodies

(3) Independent administrative agencies, etc. (which means independent administrative agencies as prescribed in Paragraph 1 of Article 2 of the Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc. (Law No.59, 2003; the same shall apply hereinafter))

(4) Local independent administrative agencies (which means local independent administrative agencies as prescribed in Paragraph 1 of Article 2 of the Local Independent Administrative Agencies Law. (Law No.118, 2003; the same shall apply hereinafter))

(5) Entities specified by a Cabinet order as having a little likelihood to harm the rights and interests of individuals considering the volume and the manner of use of personal information they handle.

Article 2 of the Cabinet Order

An entity specified by a Cabinet Order under Item 5 of Paragraph 3 of Article 2 of the Act shall be an entity that has a total number of specific individuals identified by personal information that makes up personal information databases, etc. used for its business (if all or part of the personal information databases, etc. concerned arranged by another entity only incorporate names, addresses, whereabouts (including any indication on maps or computer

displays to locate addresses or whereabouts) or telephone numbers as personal information and is used for its business without editing or processing, the number of specific individuals identified by the personal information that makes up all or part of the personal information databases, etc. concerned shall be excluded) not exceeding 5,000 on every single day in the last six months.

The term “an entity handling personal information” means a business operator using a personal information database, etc. for its business excluding the state organs, local governments, incorporated administrative agencies, etc. provided in the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003), local independent administrative institutions provided in the Local Incorporated Administrative Agencies Law (Act No. 118 of 2003), and entities having a little likelihood to harm the rights and interests of individuals considering the volume and the manner of utilization of personal information they handle.

The above stated phrase “entities having a little likelihood to harm the rights and interests of individuals considering the volume and the manner of utilization of personal information they handle” means, according to Article 2 of the Cabinet Order, an entity that has a total number of specific individuals* identified by personal information that makes up personal information databases, etc. used for its business not exceeding 5,000 on every single day in the last six months. Whether the total number of individuals is exceeding 5,000 or not is judged from the total number of specific individuals identified by personal information that makes up all personal information databases, etc. managed by the entity. However, the overlapped number of the same individual is excluded.

The term “business” in the above stated phrase “using ------ for its business” means the same kind of act that is executed iteratively and ongoingly with a certain objective and recognized as a business under the generally-accepted social standards, and is not targeting only commercial undertakings.

Even an unincorporated association (voluntary organization) and an individual can come under an entity handling personal information.

* Explanation about the phrase “total number of specific individuals”

When a personal information database, etc. fulfills every conditions stated below, the total number of specific individuals identified by personal information that makes up the personal information databases, etc. concerned is not included in the above stated “total number of specific individuals”.

1) All or part of the personal information database, etc. is prepared by others.

2) Only names, addresses (including whereabouts and any indication on maps or computer displays to locate addresses or whereabouts), and telephone numbers are included in personal information that makes up the personal information databases, etc.

3) When the personal information database, etc. is used for business, the personal information database, etc. itself has no change due to the increase of identified specific individuals by adding new personal information or appending other personal

information.

[Cases not included in the number of specific individuals]

Case 1 Names and telephone numbers listed in a telephone directory provided by a telephone company or a commercially available telephone directory on CD-ROM

Case 2 Names and data indicating the locations of addresses or whereabouts which are stored in a navigation system like a commercially available car navigation system, etc. (even a case where new information such as a driving route is recorded by using functions that are initially equipped in a navigation system, etc. is not included in "the number of specific individuals".)

Case 3 Names and information indicating the locations of addresses or whereabouts on commercially available address maps which are systematically arranged in such a way that a retrieval can be made by names or addresses

[Case not included in the number of specific individuals because the corresponding personal information is not used for business]

Case: Personal information contained in the information which is kept by a business operator in the industries like warehousing and datacenter (housing and hosting service) without being aware of whether such information corresponds to personal information or not (nonetheless, it is included when a business operator can be aware that such information contains personal information through the instruction of an entruster, etc.)

[Case corresponding to the entity handling personal information]

Case: An entity that has a total number of specific individuals identified by personal information that makes up electronic or paper medium personal information databases, etc. exceeding 5,000

2-1-4 [Personal Data] (an issue related to Paragraph 4 of Article 2 of the Act)

Paragraph 4 of Article 2 of the Act In this Act, "personal data" means personal information constituting a personal information database, etc.

The term "personal data"* means personal information constituting "a personal information database, etc." managed by the entity handling personal information.

* The Act distinguishes among three terms of 2-1-1. "Personal Information", "Personal Data", and 2-1-5. "Retained Personal Data", and the duties imposed on entities handling personal information differ from one entity to another. Accordingly, a careful attention is required.

[Cases corresponding to personal data]

Case 1 Backup personal information which is transferred from a personal information database, etc. and stored in another medium

Case 2 Personal information which is typed on forms and slips which are read out from personal information database, etc. processed by a computer

[Case not corresponding to personal data]

Case: Personal information which is described on input forms and slips in before a personal information database, etc. is constituted

* Explanation about handling of telephone directory and car navigation system, etc.

Even when a personal information database, etc. fulfills every conditions stated below, it is undeniable that personal information constituting such a personal information databases, etc. may become personal data. However, as there is a little likelihood to infringe the rights and interests of individuals in light of the manner of utilization of a personal information database, etc., it is interpreted that the duties of entities handling personal information (2-2. Duties of Entities Handling Personal Information, etc.) are not imposed.

1) All or part of the personal information database, etc. is prepared by others.

2) Only names, addresses (including whereabouts and any indication on maps or computer displays to locate addresses or whereabouts), and telephone numbers are included in personal information that makes up the personal information databases, etc.

3) When the personal information database, etc. is used for business, the personal information database, etc. itself has no change due to the increase of identified specific individuals by adding new personal information or appending other personal information.

2-1-5 [Retained Personal Data] (an issue related to Paragraph 5 of Article 2 of the Act)

Paragraph 5 of Article 2 of the Act

In this Act, "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 is specified by a Cabinet order as 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 one year that is specified by a Cabinet order.

Article 3 of the Cabinet Order

Personal data specified by a Cabinet Order under Paragraph 5 of Article 2 of the Act shall be any of the cases as set forth below:

(1) Cases in which the life, body, or property of a person or a third party might be threatened if presence or absence of the personal data concerned is revealed.

(2) Cases in which illegal or unjust acts might be prompted or triggered if the presence or absence of the personal data concerned is revealed.

(3) Cases in which national security might be undermined, mutual trust with foreign countries or international organizations might be damaged, or disadvantages when negotiating with other countries or international organizations might be brought about if the presence or absence of the personal data concerned is revealed.

(4) Cases in which crime prevention, control, investigation or other maintenance of public safety and order might be impeded if the presence or absence of the personal data concerned is revealed.

Article 4 of the Cabinet Order

The period specified by a Cabinet Order under Paragraph 5 of Article 2 of the Act shall be six months.

The term "retained personal data"*1 means such "personal data" over which the entity handling personal information has the authority*2 to respond to all requests from the person or its agent to disclose, to correct, add or delete the content, to discontinue its utilization, to erase, and to discontinue its provision to a third party.

*1 The Act distinguishes among three terms of 2-1-1. "Personal Information", 2-1-4. "Personal Data", and "Retained Personal Data", and the duties imposed on entities handling personal information differ from one entity to another. Accordingly, a careful attention is required.

*2 When an entity handling personal information processes personal data upon request from an entruster and can not disclose, etc. to the person at its discretion due to the lack of an agreement on the personal data concerned, the party who has the authority to disclose, etc. to the person is an entruster not a trustee.

However, the personal data in the following case of 1) and 2) is not "retained personal data".

1) The personal data which harms public or other interests if its presence or absence is known*3

2) The personal data which will be erased (excluding to be updated) within six months

*3 "The personal data which harms public or other interests if its presence or absence is known" represents the following cases.

1) Cases in which the life, body, or property of a person or a third party might be threatened if presence or absence of the personal data is revealed

Case: When the support organization of the victim of domestic violence or child abuse has the personal data in which the assailant (spouse or parental authority person) and the victim (spouse or child) are the persons

2) Cases in which illegal or unjust acts might be promoted or triggered if the presence or absence of the personal data is revealed

Case 1 When in order to prevent the damage from unjustified demand by a so-called sokaiya (corporate racketeer), etc., an entity owns the personal data in which a sokaiya, etc. is the person

Case 2 When an entity owns the personal data in which an individual who complains repeatedly is the person in order to prevent the damage from unjustified demand by a so-called suspicious individual and a vicious claimer (claimant or complainer), etc.

3) Cases in which national security might be undermined, mutual trust with foreign countries or international organizations might be damaged, or disadvantages when negotiating with other countries or international organizations might be brought about if the presence or absence of the personal data is revealed

Case 1 When a manufacturer and an information service provider, etc. own the personal data in which the names of persons who design and develop defense-related weapons, facilities, equipments, and software are recorded

Case 2 When an entity, which accepts the visit of key figures, and its security company own the movements schedule and record of the key figures concerned as the persons

4) Cases in which crime prevention, control, investigation or other maintenance of public safety and order might be impeded if the presence or absence of the personal data is revealed

Case: When an entity which received an inquiry from the police about the matters relevant to investigations or became the subject of a search-and-seizure warrant owns the personal data of those investigated and suspects in the process of responding to the inquiry or the warrant

2-1-6 [Person] (an issue related to Paragraph 6 of Article 2 of the Act)

Paragraph 6 of Article 2 of the Act In this Act, "person" as to personal information means a specific individual identified by personal information.

2-1-7 [Notify the Person]

Paragraph 1 of Article 18 of the Act

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.

In addition, there are descriptions in Paragraph 3 and Item 1 to 3 of Paragraph 4 of Article 18, etc. of the Act.

The phrase "notify the person" means to make the person know directly, and it must be done in such a reasonable and appropriate way that the contents of notice can be understood by the person depending on the nature of business and the status of handling personal information.

[Cases corresponding to the notice to the person]

Case 1 In an interview, to notify verbally or to pass a document like flier, etc.

Case 2 On the phone, to notify verbally or to notify with automatic answering equipment, etc.

Case 3 Between remote parties, to transmit a notice by e-mail or fax, etc. or to send a document through the post, etc.

Case 4 In a telephone-solicitation sale, to notify verbally on a soliciting phone call

Case 5 In online electronic commerce, to transmit a notice by describing in an automatic answering e-mail message for the confirmation of transaction

2-1-8 [Public Announcement]

Paragraph 1 of Article 18 of the Act

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.

In addition, there are descriptions in Paragraph 3 and Item 1 to 3 of Paragraph 4 of Article 18, etc. of the Act.

The phrase "publicly announce" means to have the wide general public know an entity's own intention (to announce so that the general nationals and other unspecified large number of people can know it). Meanwhile, the public announcement must be done in a reasonable and appropriate way depending on the nature of business and the status of handling personal information.

[Cases corresponding to the public announcement]

Case 1 Display on the place where can be reached from the top page of entity's website with a couple of clicks, displaying posters, etc. in an entity's stores and offices, placement and distribution of brochures, etc. and others

Case 2 In store sales, to announce through a notice placed where it can be seen easily in a store

Case 3 In mail-order sales, to announce through a description in a brochure, etc.

2-1-9 [Expressly Show the Purpose of Utilization to the Person]

Paragraph 2 of Article 18 of the Act Notwithstanding the provision of the preceding paragraph, when an entity handling personal information acquires such personal information on a person as is written in an agreement or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. Hereinafter this applies in this paragraph.) as a result of concluding an agreement with the person or acquires such personal information on a person as is written in a document directly from the person, the entity must expressly show the Purpose of Use in advance. However, this provision shall not apply in cases in which the acquisition of personal information is urgently required for the protection of the life, body, or property of an individual.

The phrase "expressly show the Purpose of Utilization to the person" means to clearly present the Purpose of Utilization to the person, and it must be done in such a reasonable and appropriate way that the contents of presentation can be understood by the person depending on the nature of business and the status of handling personal information.

[Cases corresponding to the expressly showing the Purpose of Utilization]

Case 1 To hand or send the person, who is the other party, a contract or other document in which the Purpose of Utilization is clearly written (when the clause about the Purpose of Utilization is written in the document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses) of the conditions of contract or these of utilization, it is necessary to pay attention so that the person can actually see the Purpose of Utilization, for example, in such ways of informing that the Purpose of Utilization is written in the general terms and conditions on the reverse side or describing the clause about the Purpose of Utilization, which is written in the general terms and conditions, etc., also on the face side)

Case 2 On the network, to clearly write the Purpose of Utilization on the page of entity's website to which the person accesses or on the screen of the person's terminal equipment (when the personal information is acquired on the network, it is necessary to pay attention to the layout of the Purpose of Utilization (including links and buttons which are designed to move to the screen where the Purpose of Utilization is displayed with a couple of clicks) so that the

person can see it before, etc. the person clicks the send button, etc.)

2-1-10 [Consent of the Person]

Paragraph 1 of Article 16 of the Act

An entity handling personal information 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 the preceding article.

Paragraph 1 of Article 23 of the Act

An entity handling personal information 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

In addition, there are descriptions in Paragraph 2 and Item 2 to 4 of Paragraph 3 of Article 16, etc. of the Act.

The phrase “the consent of the person” means the concerned person’s declaration of intent in which the person agrees that the personal information about the person is handled according to the method presented by the entity handling personal information (under the assumption that a person is already confirmed to be the person concerned).

Also, the phrase “obtaining the consent of the person” means that the concerned entity handling personal information recognizes the person’s declaration of intent in which the person agrees, and it must be done in such a reasonable and appropriate way that is deemed necessary for the person’s judgment about the consent depending on the nature of business and the status of handling personal information.

Meanwhile, in such case as a child has no ability to understand the results arisen from his/her consent to the handling of personal information, it is necessary to obtain the consent from the attorney-in-fact, etc. of the child.

[Cases obtaining the consent of the person]

Case 1 To confirm that the person expresses its consent verbally or in writing (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses)

Case 2 To receive and confirm a document like an application form in which the person expresses its consent and sign or append its signature and seal

Case 3 To receive an e-mail message, in which the person expresses its consent, from the person

Case 4 A check mark placed by the person in the confirmation box which indicates the consent of the person

Case 5 The person's click of the button which indicates the consent of the person on the screen of website

Case 6 Voice input, input on the touch panel, and input with the button or switch, etc. by the person to express its consent

2-1-11 [Readily Accessible Condition for the Person]

Paragraph 2 of Article 23 of the Act

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 following items or put those matters in a readily accessible condition for the person, the entity may, notwithstanding the provision of the preceding paragraph, provide such personal data concerned to third parties:

Item 3 of Paragraph 4 of Article 23 of the Act

In following the cases, the individual or entity receiving such personal data shall not be deemed a third party for the purpose of application of the preceding three paragraphs:

(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

In addition, there are descriptions in Paragraph 3 of Article 23, etc. of the Act.

The phrase "readily accessible condition for the person" means that there is a condition in which the matters can be easily known, in terms of both time and means, by a person if the person wants to know, and the arrangement for the above condition must be done in such a

reasonable and appropriate way that the contents of matters can be understood by the person depending on the nature of business and the status of handling personal information.

[Cases corresponding to the readily accessible condition for the person]

Case 1 Continued display on the place where can be reached from the top page of website with a couple of clicks and others

Case 2 Continued display of a notice or placement of notice documents at the counter of an office, etc. and others

Case 3 Periodical advertisement on a widely distributed regular publication

Case 4 In online electronic commerce, continued display of the links on the screen of website introducing merchandises

2-1-12 [Accessible Condition for the Person (such condition includes cases in which a response is made without delay at the request of the person)]

Paragraph 1 of Article 24 of the Act With respect to the retained personal data, an entity handling personal information must put the matters enumerated in the following items in an accessible condition for the person (such condition includes cases in which a reply is made without delay at the request of the person):

The phrase "an accessible condition for the person (such condition includes cases in which a response is made without delay at the request of the person)" means to put the matters in a condition where a person can know the matters if the person wants to know by the methods including display on the screen of website, distribution of brochures, and response made without delay at the request of the person. The accurate contents at that time always must be put in a condition where the person can know them. Although even the continued display on the screen of website or at the counter of an office, etc. and others are not necessarily required, it must be done in such a reasonable and appropriate way that the contents of matters can be understood by the person depending on the nature of business and the status of handling personal information.

Meanwhile, as for entities and others which have a volume of responses to inquiries on a routine basis, the continued display on the screen of website is a method which meets the purposes of both 2-1-11. [Readily Accessible Condition for the Person] and 2-1-12. [Accessible Condition for the Person (such condition includes cases in which a response is made without delay at the request of the person)].

[Cases corresponding to the accessible condition for the person]

Case 1 To create an inquiry counter and to establish a system so that a response to an inquiry is made verbally or in writing

Case 2 In store sales, to have the placement of brochures

Case 3 In online electronic commerce, to clearly describe the e-mail address for inquiries

2-1-13 [Provision]

Paragraph 1 of Article 23 of the Act An entity handling personal information must not, except in the following cases, provide personal data to a third party without obtaining the prior consent of the person : In addition, there are descriptions in Paragraph 2 of Article 23, etc. of the Act.

The term “provision” means to put personal data in a condition where its utilization is available. Even in a case where personal data is not provided physically, if personal data is put in a condition where its utilization is available (where an authority to use is given) by using the network, etc., it is regarded as “provision”.

2-2 Duties of Entities Handling Personal Information, etc.

2-2-1 Matters Concerning the Purpose of Utilization of Personal Information (issues related to Article 15 and 16 of the Act)

(1) Specification of the Purpose of Utilization (an issue related to Paragraph 1 of Article 15 of the Act)

Paragraph 1 of Article 15 of the Act When handling personal information, an entity handling personal information must specify the purpose of use of personal information (hereinafter called the "Purpose of Use") as much as possible.

An entity handling personal information must concretely specify the Purpose of Utilization as much as possible. When the Purpose of Utilization is specified, the entity handling personal information must concretely specify as much as possible for what purpose it will finally use personal information instead of just abstractly and generally specifying the Purpose of Utilization (excluding cases corresponding to 2-1-4. “* Explanation about handling of telephone directory and car navigation system, etc.”). Meanwhile, when the Purpose of Utilization is specified, it is not required even to specify the items of personal information to be used, the name of entity from which the personal information was obtained, and others. Concretely, it can be cited that “the shipment of merchandise, notice of new products information, and related after-sales service in XX service*” and others as the Purpose of Utilization. It can be said that such cases, as where the scope of the utilization of personal information of the person is specified to the extent that the person can reasonably imagine in the light of the nature of business provided in the articles of association and endowment, etc. and from the viewpoint of the person identified by personal information and where the scope of the Purpose of Utilization can be imagined by clear indication of the type of business, are good enough. In many cases, however, only the clear indication of the type of business does

not satisfy the requirement of specifying the Purpose of Utilization as much as possible. Also to make such abstract and common contents, as just “the business activity” and “the improvement of customer service”, etc., the Purpose of Utilization is not deemed to specify as much as possible.

Where it is assumed in advance to provide personal information to a third party, the fact must be manifested in the Purpose of Utilization.

When the Purpose of Utilization of employment management information is specified, the specification should not be made just abstractly and generally, but be made concretely and individually to the extent that a person including a laborer, etc. (a laborer who is employed by an entity handling personal information, a laborer who is or was going to be employed by an entity handling personal information, and a laborer who was employed by an entity handling personal information in the past; the same shall apply hereinafter) can reasonably imagine the result of utilization of obtained personal information of the person concerned.

* When the XX service is specified, it is preferable to be specified within the scope that is recognized to contribute to the specification from the viewpoint of the person under the social standards. For example, there is a case where a classification in the level of division and group of Japan Standard Industrial Classification serves as a reference.

[Cases concretely specifying the Purpose of Utilization]

Case 1 “The personal information will be used for the shipment of merchandise, related after-sales service, and notice of new product and service information in XX service.”

Case 2 “The inscribed name, address, and telephone number may be sold as a name list.”

Case 3 For example, in the case of entity which handles information-processing service, the following statement comply with the specification of the Purpose of Utilization: “The trusted personal information will be handled for the execution of information-processing services, including the payroll calculation processing service, address printing service, and slip printing and shipping service, as our business.”

[Cases not concretely specifying the Purpose of Utilization]

Case 1 “For being used for the business activity”

Case 2 “For the improvement of service being provided”

Case 3 “For being used for the marketing activity”

(2) Change of the Purpose of Utilization (an issue related to Paragraph 2 of Article 15 and Paragraph 3 of Article 18 of the Act)

Paragraph 2 of Article 15 of the Act

An entity handling personal information must not change the Purpose of Use beyond the scope which is reasonably considered that the Purpose of Use after the change is duly related to that before the change.

Paragraph 3 of Article 18 of the Act

When an entity handling personal information has changed the Purpose of Use, the entity must notify the person of the changed Purpose of Use or publicly announce it.

It is possible to change the Purpose of Utilization specified according to the above section (1) within the scope which is considered to be not difficult for the person to imagine under the social standards. The changed Purpose of Utilization must be notified to the person[*1] or publicly announced[*2].

Meanwhile, when the change which is considered to be difficult for the person to imagine is made, the consent of the person must be obtained in accordance with Article 16 of the Act.

*1 As for “notified to the person”, refer to 2-1-7.

*2 As for “publicly announced”, refer to 2-1-8.

* The criterion of being within the scope which is considered to be not difficult for the person to imagine

The change beyond the scope of business handling personal information expressed in the Purpose of Utilization can not be made without the consent of the person in advance.

Where a set of typical examples of the handling of personal information is expressed with concreteness in the Purpose of Utilization, the change can be made within the scope which can be presumed from such typical examples.

[Case assumed to be within the scope which is considered to be not difficult for the person to imagine]

Case: To add an item “notice of information about existing products and services” to the Purpose of Utilization expressing “notice of information about our new products and services in XX business”

(3) Restriction by the Purpose of Utilization (an issue related to Paragraph 1 of Article 16 of the Act)

Paragraph 1 of Article 16 of the Act

An entity handling personal information 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 the preceding article.

When an entity handling personal information handles personal information about a person beyond the scope necessary for the achievement of the Purpose of Utilization, the business operator must obtain the consent of the person* in advance.

It does not correspond to the utilization other than for intended purposes to use personal information (sending an e-mail message and making a phone call, etc.) for obtaining the consent of the person, even where such actions are not expressed in the original Purpose of Utilization.

* As for "the consent of the person", refer to 2-1-10.

[Case need of consent]

Case: Case where a company sends, based on information on resume for employment, a catalog of merchandise traded by the company and an application form for purchasing merchandise for the sales promotion of its merchandise

(4) Succession of Business (an issue related to Paragraph 2 of Article 16 of the Act)

Paragraph 2 of Article 16 of the Act

When an entity handling personal information 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.

When an entity handling personal information has acquired personal information as a result of taking over the business of another entity handling personal information in a merger, a split-up of a company, and a transfer of business, etc., it does not correspond to the utilization other than for intended purposes to handle the personal information concerned within the scope necessary for the achievement of the Purpose of Utilization of the personal information concerned before the succession, and accordingly, it is not required to obtain the consent of the persons.

(5) Exclusion of Application (an issue related to Paragraph 3 of Article 16 of the Act)

Even where it is required to obtain the consent of the person in the above section (3) and (4), the provisions of these sections do not apply to the following cases:

(i) Cases based on laws and regulations (an issue related to Item 1 of Paragraph 3 of Article 16 of the Act)

Item 1 of Paragraph 3 of Article 16 of the Act 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

When the handling of personal information is made based on laws and regulations, the provisions of section (3) and (4) do not apply.

As the provisions of laws and regulations providing the basis of the above, Article 218 of the Code of Criminal Procedure (investigation based on warrant) and Subarticle (7) of Article 72 of the Local Tax Law (tax collector's rights of questioning and examination on enterprise tax; there are similar provisions in various tax laws), etc. are conceivable. These provisions have a compelling force and uniformly correspond to this case.

Case: Submission of a payment record to the director of taxation office in accordance with Paragraph 1 of Article 225 of the Income Tax Law, etc.

Meanwhile, although Paragraph 2 of Article 197 of the Code of Criminal Procedure (inquiry necessary for investigation) does not have a compelling force, it corresponds to this case because of the basis existing in laws and regulations. Subarticle 2 of Article 23 of the Practicing Attorney Law (inquiry from bar association) is also conceivable to be an object of this case, nonetheless it should be considered whether the provision of information has necessity and reasonableness which meet the purpose of the said inquiry system.

Case 1 Response to the investigation of subsidiary company by the auditors of parent company in accordance with Paragraph 3 of Article 381 of the Company Law

Case 2 Response to the financial statements audit pursuant to the provisions of Article 396 of the Company Law and Subarticle 2 of Article 193 of the Securities and Exchange Law

Case 3 When a selling entity provides information on purchasers of the product, etc. to a manufacturing and importing entity based on the provision of Paragraph 3 of Article 38 of the Consumer Product Safety Law* in a case where the manufacturing and importing entity recalls, etc. a product in accordance with an order (hazard prevention order) pursuant to Paragraph 1 of Article 39 of the Act

* The 2006 revision of the Consumer Product Safety Law is scheduled to be enforced in the spring of 2007.

(ii) Protection of the life, body, or property of an individual (an issue related to Item 2 of Paragraph 3 of Article 16 of the Act)

Item 2 of Paragraph 3 of Article 16 of the Act The provisions of the preceding two paragraphs shall not apply to the following cases: (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

When there is a possible infringement of concrete rights and interests such as the life, body, or property of an individual (including a juridical person) and when the utilization of personal information is necessary to protect them and when it is difficult to obtain the consent of the person (excluding cases in which it is substantially possible to protect the rights and interest concerned by other methods), the provisions of section (3) and (4) do not apply.

Case 1 When the blood type and family members' contact information, etc. of a person are provided to doctors or nurses in emergency situations such as a sudden illness

Case 2 When information about a person who intentionally interferes with business is exchanged among private companies

Case 3 When a selling entity, a repairing entity, or an installing entity, etc. provides information on purchasers of the product, etc. to a manufacturing entity, etc. in a case where because of a product accident[*1] or an urgent danger that may cause harm to human life or body despite no product accident, a manufacturing entity, etc. recalls[*2] a consumer product

*1 Among accidents that occurred along with the use of consumer product, either (1) an accident in which a harm to the life or body of ordinary consumer has occurred or (2) an accident in which a consumer product has been lost or damaged and which may cause harm to the life or body of ordinary consumer is the product accident but excluding accidents which were clearly not caused by the defect of consumer product (Paragraph 4 of Article 2 of the Consumer Product Safety Law).

*2 The term recall means a response by an entity to minimize the enlarged likelihood of the occurrence of accidents due to a consumer product. More concretely, it means the implementation of (1) calling attention of consumers (appropriate provision of information to consumers about the risk of a product accident), (2) recall from the stage of distribution and sales, and (3) exchange, improvement (including inspection, repair, and replacement of parts), or taking-over of a product owned by a consumer.

(iii) Improvement of public health, etc. (an issue related to Item 3 of Paragraph 3 of Article 16 of the Act)

Item 3 of Paragraph 3 of Article 16 of the Act

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

(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

When the handling of personal information is specially necessary for improving public health or promoting the sound growth of children who are still developing both mentally and physically and when it is difficult to obtain the consent of the person (excluding cases in which it is substantially possible to improve public health or promote the sound growth of children by other methods), the provisions of section (3) and (4) do not apply.

Case 1 Case in which information on the result of thorough examination and the situation of consultation, etc. about the public health service including health examination and cancer checkup implemented by an insurer, etc. like a health insurance society, etc. is provided, in concealing individual names, to researchers, etc. for the epidemiology study or the statistical survey aimed at the making of health enhancement policies and the improvement of the effectiveness of health enhancement programs

Case 2 Case in which in order to address a schoolchild's problematic behavior including truancy and delinquency in collaboration by pertinent institutions including a child consultation center, a school, and a medical institution, information on the schoolchild concerned is exchanged among pertinent institutions concerned

(iv) Cooperation with a state organ, etc. (an issue related to Item 4 of Paragraph 3 of Article 16 of the Act)

Item 4 of Paragraph 3 of Article 16 of the Act

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

(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

When a state organ, etc. needs to obtain cooperation from a private company, etc. in executing the affairs prescribed by laws and regulations and when it is recognized that obtaining the person's consent on the utilization other than for intended purposes by the cooperating private company, etc. are likely to impede the execution of the affairs concerned, the provisions of section (3) and (4) do not apply.

Case 1 When a business operator, etc. provide personal information in response to an investigation on a voluntary basis by an official taxation office, etc.

Case 2 When a business operator, etc. provide personal information in response to a request from the police on a voluntary basis

2-2-2 Matters Concerning the Acquisition of Personal Information (issues related to Article 17 and 18 of the Act)

(1) Proper Acquisition (an issue related to Article 17 of the Act)

Article 17 of the Act An entity handling personal information must not acquire personal information by a fraudulent or other dishonest means.

An entity handling personal information must not acquire personal information by wrongful means like a deception, etc. Any person who acquired by a fraud, etc., used, or disclosed, for a purpose of unfair competition, the secretly kept personal information that was useful for business and not publicly known can be imposed a criminal penalty (an imprisonment with work for not more than five years or a fine of not more than five million yen) in accordance with Article 21 of the Unfair Competition Prevention Law (Act No. 47 of 1993).

[Cases acquiring personal information by wrongful means]

Case 1 When family member's personal information, which is irrelevant in light of the condition of acquirement, such as the income situation of parents is acquired from a child, who does not have sufficient ability to understand, without the consent of the child's parents

Case 2 When personal information was acquired by forcing someone into the violation of the restriction of provision to a third party stipulated in Article 23 of the Act

Case 3 When personal information is acquired from another business operator by instructing the business operator to acquire personal information by wrongful means such as above Case 1 and 2

(2) Notice or Public Announcement of the Purpose of Utilization (an issue related to Paragraph 1 of Article 18 of the Act)

Paragraph 1 of Article 18 of the Act 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.

It is preferable that an entity handling personal information publicly announces[*1] the Purpose of Utilization in advance when the entity handling personal information acquires personal information. If not publicly announced, the entity handling personal information must promptly notify the person[*2] of the Purpose of Utilization or publicly announce it after the acquisition (excluding cases corresponding to 2-1-4. "* Explanation about handling of telephone directory and car navigation system, etc.").

Regarding the personal data that had been retained before the Act was enforced, as no action was made to acquire personal information at the time of the enforcement of the Act, the provision of Article 18 of the Act does not apply. However, regarding the familiarization of the person with matters concerning retained personal data, measures stipulated in Paragraph 1 of Article 24 of the Act need to be taken at the time of the enforcement of the Act (refer to 2-2-5-1.).

*1 As for "publicly announces", refer to 2-1-8.

*2 As for "notify the person", refer to 2-1-7.

[Cases need of notice to the person or public announcement]

Case 1 To acquire the personal information which is voluntarily publicized by the person on the Internet

Case 2 To acquire personal information from the Internet, official gazettes, and directory of government officials, etc.

Case 3 To acquire the personal information which is voluntarily provided by the person in such occasions as an inquiry or complaint by telephone (excluding a case in which personal information is acquired only for the purpose of personal identity verification or reply to an inquiry)

Case 4 To receive the provision of personal information to a third party

Case 5 To acquire personal information in trust to handle personal information

(3) Direct Acquisition in a Written Document, etc. (an issue related to Paragraph 2 of Article 18 of the Act)

Paragraph 2 of Article 18 of the Act
Notwithstanding the provision of the preceding paragraph, when an entity handling personal information acquires such personal information on a person as is written in an agreement or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. Hereinafter this applies in this paragraph.) as a result of concluding an agreement with the person or acquires such personal information on a person as is written in a document directly from the person, the entity must expressly show the Purpose of Use in advance. However, this provision shall not apply in cases in which the acquisition of personal information is urgently required for the protection of the life, body, or property of an individual.

When an entity handling personal information acquires personal information directly from the person in such ways as to write in a document, etc., to input data on a user entry screen, and others, the business operator must expressly show the Purpose of Utilization to the person* in advance. Meanwhile, although the said duties are not imposed even in a case where personal information is acquired verbally, based on Paragraph 1 of Article 18 of the Act in that case, the entity handling personal information must publicly announce the Purpose of Utilization in advance, otherwise promptly notify the person of the Purpose of Utilization or publicly announce it. Also where an urgent requirement for the protection of the life, body, or property of an individual, it is not necessary to expressly show the Purpose of Utilization to the person in advance, however, based on Paragraph 1 of Article 18 of the Act in that case, the entity handling personal information must promptly notify the person of the Purpose of Utilization or publicly announce it after the acquisition of personal information.

* As for "expressly show the Purpose of Utilization to the person", refer to 2-1-9.

[Cases in which the Purpose of Utilization must be expressly showed to the person in advance]

Case 1 To acquire personal information written in a contract or an application directly from the person

Case 2 To acquire personal information written in a questionnaire directly from the person

Case 3 To acquire personal information written in a postcard to participate in a prize competition directly from the person

(4) Change of the Purpose of Utilization (an issue related to Paragraph 3 of Article 18 of the Act)

Paragraph 3 of Article 18 of the Act
When an entity handling personal information has changed the Purpose of Use, the entity must notify the person of the changed Purpose of Use or publicly announce it.

When an entity handling personal information changed the Purpose of Utilization within the scope which is considered to be not difficult for the person to imagine under the social standards, the business operator must notify the person[*1] of the changed Purpose of Utilization or publicly announce[*2] it (refer to 2-2-1. (2)).

*1 As for "notify the person", refer to 2-1-7.

*2 As for "publicly announce", refer to 2-1-8.

(5) Exclusion of Application (an issue related to Paragraph 4 of Article 18 of the Act)

In the following cases, the provisions of above section (2), (3), and (4) do not apply:

(i) Likelihood to harm the rights or interests of the person or a third party (an issue related to Item 1 of Paragraph 4 of Article 18 of the Act)

Item 1 of Paragraph 4 of Article 18 of the Act

The provisions of the preceding three paragraphs shall not apply to the following cases:

(1) Cases in which notifying the person of the Purpose of Use or publicly announcing it might harm the life, body, property, or other rights or interests of the person or a third party

When notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the life, body, property, or other rights or interests of the person or a third party, the provisions of above section (2), (3), and (4) do not apply.

Case: When in order to prevent the damage from unjustified demand by a so-called sokaiya (corporate racketeer), etc., an entity acquires information about the individual person in charge in the sokaiya concerned and mutually exchanges such information with other entities and when notifying the person of the Purpose of Utilization or publicly announcing it are likely to entail that the informer who is a third party is harmed by the sokaiya, etc. concerned with unjustified resentment

(ii) Likelihood to harm the rights, etc. of the entity handling personal information concerned (an issue related to Item 2 of Paragraph 4 of Article 18 of the Act)

Item 2 of Paragraph 4 of Article 18 of the Act

The provisions of the preceding three paragraphs shall not apply to the following cases:

(2) Cases in which notifying the person of the Purpose of Use or publicly announcing it might harm the rights or legitimate interests of the entity concerned handling personal information

When the rights or interests of the entity handling personal information are likely to be infringed because the matters relating to company secret, etc. become apparent to other companies by notifying the person of the Purpose of Utilization or publicly announcing it, the provisions of above section (2), (3), and (4) do not apply.

Case: When the matters relating to company secrets, including the content of new product being developed by the entity handling personal information concerned and the sales know-how of the business operator, become apparent by the content of the Purpose of Utilization which is notified or publicly announced

(iii) Cooperation with a state organ, etc. (an issue related to Item 3 of Paragraph 4 of Article 18 of the Act)

Item 3 of Paragraph 4 of Article 18 of the Act

The provisions of the preceding three paragraphs shall not apply to the following cases:

(3) Cases in which it is necessary to cooperate with a state institution or a local public body in executing the operations prescribed by laws and in which notifying the person of the Purpose of Use or publicly announcing it might impede the execution of the operations concerned

When a state organ, etc. needs to obtain cooperation from a private company, etc. in executing the affairs prescribed by laws and regulations and when notifying the person of the Purpose of Utilization obtained from the state organ, etc. or publicly announcing it by the cooperating private company, etc. are likely to impede the execution of the affairs concerned, the provisions of above section (2), (3), and (4) do not apply.

Case: When the police, without an open search for a named suspect, provide personal information about the suspect only to the entity handling personal information which the suspect is expected to visit and when notifying the suspected person of the Purpose of Utilization or publicly announcing it by the entity handling personal information concerned which obtained such personal information from the police are likely to greatly impede the investigative activities

(iv) Purpose of Utilization is Clear (an issue related to Item 4 of Paragraph 4 of Article 18 of the Act)

Item 4 of Paragraph 4 of Article 18 of the Act

The provisions of the preceding three paragraphs shall not apply to the following cases:

(4) Cases in which it is considered that the Purpose of Use is clear in consideration of the circumstances of the acquisition

When it is considered that the Purpose of Utilization is clear in consideration of the circumstances under which personal information is acquired, the provisions of above section (2), (3), and (4) do not apply.

Case 1 When personal information such as address and telephone number is acquired at the sale or provision of merchandise or service, etc. and when the Purpose of Utilization is only intended to sell or provide the merchandise or service, etc. concerned without fail

Case 2 When exchanging business cards as a common practice is an acquisition of personal information including name, professional affiliation, title, and contact point in a document directly from the person and when the Purpose of Utilization is intended for the future contact (However, the utilization of

business card for the purpose of direct mail, etc. may not correspond to the clear Purpose of Utilization, and accordingly, a careful attention is required.)

2-2-3 Management of Personal Data (an issue related to Article 19 to 22 of the Act)

2-2-3-1 Maintenance of the Accuracy of Data (an issue related to Article 19 of the Act)

Article 19 of the Act

An entity handling personal information must endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of the Purpose of Use.

An entity handling personal information must endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of the Purpose of Utilization by preparing the procedures of collation and confirmation when personal information is inputted into a personal information database, etc., preparing the procedures of collection, etc. when an error, etc. is found, updating the matters recorded, and setting storage period, etc. (excluding cases corresponding to 2-1-4. "* Explanation about handling of telephone directory and car navigation system, etc.").

In this case, it is not necessary to uniformly or constantly update personal data that is retained, and it is sufficient with ensuring the accuracy and recency within the scope of necessity depending on the respective Purposes of Utilization.

2-2-3-2 Security Control Measures (an issue related to Article 20 of the Act)

Article 20 of the Act

An entity handling personal information must take necessary and proper measures for the prevention of leakage, loss, or damage, and for other control of security of the personal data.

An entity handling personal information must take systematic, human, physical, and technical security control measures for the prevention of leakage, loss, or damage, and for other security control of the personal data (excluding cases corresponding to 2-1-4. "* Explanation about handling of telephone directory and car navigation system, etc."). At the same time, considering the magnitude of the infringement of rights and interests that the person incurs when the personal data of the person is leaked, lost, or damaged, etc., the necessary and proper measures must be taken depending on the risks attributable to the nature of business and the status of handling personal information, etc. In doing so, it is preferable to take security control measures depending on the property of medium that records personal data. Meanwhile, as for credit card information, it is preferable to take measures stated in the Annex "Handling of Personal Information Including Credit Card Information".

[Cases which can not be deemed to take necessary and proper security control measures]

Case 1 When an entity handling personal information leaves a condition in which the personal data that is assumed not to be opened is exposed to unspecified large

number of people on the screen of the business operator's website

Case 2 When an entity handling personal information leaves a condition in which a worker who became not required to access personal data any longer due to the change of organization can access personal data and when the worker leaked personal data

Case 3 When it become impossible to provide a service to the person due to the loss or damage of personal data that was registered by the person in order to be provided the service continuously since it was failed to recover the personal data damaged by a system failure because the backuped data was also damaged although it was believed the backup was made

Case 4 When a worker who is not allowed to access the personal information database obtained the personal data and leaked it because an access control to the database was not made

Case 5 When a medium into which personal data was backuped was taken out in a condition where such medium was left available to be taken out by a person who was not allowed to take out

[Cases which do not correspond to the violation of duties regarding security control measures (also do not correspond to the violation of duties regarding the supervision of workers or the supervision of trustees)]

Case 1 Case in which the personal data described as a cover address was disclosed to a third party due to a misdelivery when trusted the home delivery or mailing of package, etc. which did not contain personal information

Case 2 Case in which a commercially available directory (that was never processed by a business operator) that everyone can easily buy at a book store was disposed of without being processed by a paper shredder, etc. or given to a junk dealer in order to dispose of it

Systematic security control measures

The systematic security control measures mean to clearly establish the responsibility and authority of workers regarding security control (refer to Article 21 of the Act), to prepare and apply regulations and procedure manuals (hereinafter referred to as "regulations, etc."), and to confirm the status of implementation.

[Matters to be taken as systematic security control measures]

1) Preparing the organization structure to take security control measures for personal data

2) Preparing the regulations, etc. which provides security control measures for personal data and operating in accordance with the regulations, etc.

3) Preparing the means by which the status of handling personal data can be looked through

4) Assessing, reviewing, and improving the security control measures for personal data

5) Responding to accident or violation

[Exemplifications of the means which are preferable to be taken for the practice of each item of above matters]

1) Exemplifications of the means which are preferable to be taken for the practice of "Preparing the organization structure to take security control measures for personal data"

- Clarification of the role and responsibility of worker

* It is preferable to concretely stipulate the role and responsibility of worker regarding the security control of personal data in the internal regulations including regulations for segregation of duties and regulations for official authority, contract, and job description, etc.

- Establishment of the so-called Chief Privacy Officer (CPO)

- Establishment of the responsible official for the operation and the limitation of operators in the handling of personal data (operations including acquisition and entry, transfer and transmission, utilization and processing, storage and backup, and erasure and disposal)

- Establishment of the responsible official for the operation of information system handling personal data and the limitation of operators (including system administrator)

- Clarification of the roles and responsibilities of respective departments which are involved in the handling of personal data

- Establishment of the responsible official for audit

- Preparation of the implementation system of audit

- Preparation of the system to report to and inform the representative executives, etc. when the fact or sign of violation of the regulations, etc. regarding the handling of personal data is known

- Preparation of the system to report to and inform the representative executives, etc. when an accident of leakage, etc. (leakage, loss, or damage) of personal data has happened or when the possibility of such accident is assessed to be high

* It is preferable that such system cooperates with the complaint processing system because sometimes information about the leakage of personal data is

provided from the outside through the corporate contact representative or the complaint processing service (refer to Article 31 of the Act).

- Preparation of the system to provide information to the person who is possibly affected by a leakage accident, etc.

- Preparation of the system to report to the competent minister and the authorized personal information protection organizations at the time of leakage accident, etc.

2) Exemplifications of the means which are preferable to be taken for the practice of "Preparing the regulations, etc. which provides security control measures for personal data and operating in accordance with the regulations, etc."

- Preparation of the regulations, etc. regarding the handling of personal data and the operation in accordance with them

- Preparation of the regulations, etc. regarding the security control measures for information system handling personal data and the operation in accordance with them

  * For more detailed descriptions of these matters, refer to later described [Examples of matters which are preferable to be described in the regulations, etc. regarding the handling of personal data]

- Preparation of the regulations, etc. regarding the security control of buildings, rooms, and storage lockers, etc. relating to the handling of personal data and the operation in accordance with them

- Preparation of the criterion of selecting trustees and the standard entrustment contract, etc. when the handling of personal data is trusted and the operation in accordance with them

- Retention of audit trails* which indicate that the operation procedures were properly performed based on the established regulations, etc.

  * Such items as application for the utilization of information system regarding personal data, application for authorization to confer special authority to a certain worker, list of information system users and their authorities, record of entering and leaving a building, etc., record of access to personal data (for example, record of who made what manipulation), and list of persons who took the educational training course, etc. are conceivable as audit trails which are preferable to be retained.

3) Exemplifications of the means which are preferable to be taken for the practice of "Preparing the means by which the status of handling personal data can be looked through"

- Preparation of the personal data handling ledger which records items to be acquired, Purpose of Utilization which was clearly expressed or publicly

announced, place of storage, way of storage, persons who have authority to access, and time limit on utilization as well as other information necessary for the proper handling of personal data

- Maintenance of updated condition through the periodical confirmation of the content of personal data handling ledger

4) Exemplifications of the means which are preferable to be taken for the practice of "Assessing, reviewing, and improving the security control measures for personal data"

- Planning of audit program and the implementation of audit (internal or external audit) based on the program

- Summarizing the results of the implementation of audit and reporting to the representative executives

- Periodical review and improvement of the security control measures in response to the audit report from the responsible official for audit, the change of the social standards, and the progress of information technology

5) Exemplifications of the means which are preferable to be taken for the practice of "Responding to accident or violation"

- Establishment of the procedures in the following steps from (A) to (F)

  However, it is conceivable that it is not necessary to make a response along with the followings when a commercially available directory (that was never processed by a business operator) that everyone can easily buy at a book store was lost, etc.

  (A) Fact-finding and probing into the cause

  (B) Defining the boundary of the scope that will be affected

  (C) Examining and implementing the measures to prevent a recurrence

  (D) Contacting the person who is possibly affected

  It is preferable to apologize to the person for the accident or violation and to contact the person as much as possible in order to prevent a secondary damage.

  However, for instance as below, it is conceivable that a contact to the person can be omitted when the rights and interests of the person are not infringed and it seems that there is no or extremely little likelihood of infringement in the future, too.

  - When the personal data that was lost, etc. was immediately recovered without being seen by a third party

- When the concealment measures such as advanced encryption are taken

- When nobody except the business operator which made leakage, etc. can identify the specific individual (when the leaked data takes form of personal data only by being collated with the personal data that the business operator retains)

(E) Reporting to the competent minister, etc.

a. Cases in which an entity handling personal information is a target business operator of the authorized personal information protection organizations

A target entity handling personal information (hereinafter referred to as "target business operator") which is a target of the businesses of the authorized personal information protection organizations can, in stead of reporting to the Minister of Economy, Trade and Industry (a competent minister), report to the authorized personal information protection organization to which the target business operator belongs. The authorized personal information protection organizations periodically report the overall condition of accidents or violations made by target business operators to the Ministry of Economy, Trade and Industry. However, in the following cases, it is preferable to immediately report to the Minister of Economy, Trade and Industry (a competent minister) on a case-by-case basis.

- When the personal data covering the sensitive issues ((a) issues relating to thought, creed, and religion, (b) issues that cause social discriminations such as race, nation, family origin, and registered domicile (excluding the case of information only about the prefecture where the registered domicile exists), physical and mental disorder, criminal record, and others, (c) issues relating to the actions of group activities such as labor's right to organize, collective bargaining, and others, (d) issues relating to the exercise of political right such as participation in a mass demonstration, exercise of the right of petition, and others, and (e) issues relating to health care and sexual life, etc.) was leaked.

- When the personal data including credit information and credit card number, etc. was leaked and there is a high likelihood that the secondary damages happen

- When the accidents of leakage, etc. (specially the same kind of accident) have happened repeatedly in the same business operator

- In addition, when the authorized personal information protection organizations deem necessary

b. Cases in which an entity handling personal information is not a target business operator of the authorized personal information protection organizations

An entity handling personal information reports to the Minister of Economy, Trade and Industry (a competent minister).

Meanwhile, regardless of whether the entity handling personal information is a target business operator of the authorized personal information protection organizations or not, it is preferable to report to the pertinent institution such as an industrial association, etc. to which the business operator belongs in addition to reporting to a competent minister.

(F) Publicly announcing all the facts and the measures to prevent a recurrence, etc.

From the viewpoint of preventing a secondary damage and avoiding the occurrence of similar accident case, etc., when an accident case such as the leakage of personal data, etc. has happened, it is important to publicly announce all the facts and the measures to prevent a recurrence, etc. as much as possible.

However, for instance as below, it is conceivable that the public announcement of all the facts, etc. can be omitted when there is no need to publicly announce from the viewpoint of preventing a secondary damage. Meanwhile, even in such case, from the viewpoint of avoiding the occurrence of similar accident case, it is preferable that the information regarding the accident case concerned is shared among entities in the same business, etc.

- When all the persons who are possibly affected were informed
- When the personal data that was lost, etc. was immediately recovered without being seen by a third party
- When the concealment measures such as advanced encryption are taken
- When nobody except the business operator which made leakage, etc. can identify the specific individual (when the leaked data takes form of personal data only by being collated with the personal data that the business operator retains)

[Examples of matters which are preferable to be described in the regulations, etc. regarding the handling of personal data]

In the following, in line with the flow, which consists of (1) acquisition and entry, (2) transfer and transmission, (3) utilization and process, (4) storage and backup, and (5) erasure and disposal, of the handling of personal data, the examples of matters that are preferable to be described in the regulations, etc. regarding respective constituents of

the above flow are enumerated.

(1) Acquisition and entry

1) Clarification of the responsible official for operation

- Clarification of the responsible official for operation when personal data is acquired

- Clarification of the responsible official for operation when the acquired personal data is entered into an information system (hereinafter collectively referred to as “acquisition and entry”)

2) Clarification of the procedures and implementation in accordance with the procedures

- Clarification of the procedures in acquisition and entry

- Implementation of acquisition and entry in accordance with the established procedures

- Implementation of entry work in a building or a room (hereinafter referred to as “building, etc.”) where an unauthorized person can not enter

- Limitation, based on the operational necessity, of the computer terminals into which personal data can be entered

- Limitation, based on the operational necessity, of the functions that are installed in computer terminals into which personal data can be entered (for instance, to make the computer terminals, into which personal data can be entered, impossible to be connected with external record medium such as CD-R and USB Memory, etc.)

3) Identification, authentication, and authorization of operators

- Limitation, based on the operational necessity, of operators who can make the acquisition and entry of personal data

- Identification of operators by authentication with ID and password or by biometric authentication, etc.

- Limitation of authorities given to operators

- Record of authorities given to operators who make the acquisition and entry works of personal data

4) Confirmation of operators and their authorities

- Clarification of the procedures and implementation in accordance with the procedures and confirmation of the status in which the identification, authentication, and authorization of operators are implemented

- Record of access and storage of access record as well as confirmation of the presence or absence of work beyond authorities

(2) Transfer and transmission

1) Clarification of the responsible official for operation

- Clarification of the responsible official for operation when personal data is transferred and transmitted

2) Clarification of the procedures and implementation in accordance with the procedures

- Clarification of the procedures in the transfer and transmission of personal data

- Implementation of transfer and transmission in accordance with the established procedures

- Concealment such as encryption of personal data when the personal data is transferred and transmitted (for instance, when personal data is transmitted through the public circuit)

- Confirmation of mailing address and receipt when transferring (for instance, utilization of delivery-certified mail, etc.)

- Confirmation of destination number and receipt when faxing, etc.

- Prohibition of leaving documents with personal data in a fax machine, etc.

- Proper management of encryption keys and passwords

3) dentification, authentication, and authorization of operators

- Limitation, based on the operational necessity, of operators who can make the transfer and transmission of personal data

- Identification of operators by authentication with ID and password or by biometric authentication, etc.

- Limitation of authorities given to operators (for instance, when personal data is transmitted through the computer network, the operator who make a transmission does not need the authority to view and change the content of

personal data.)

- Record of authorities given to operators who make the transfer and transmission works of personal data

4) Confirmation of operators and their authorities

- Clarification of the procedures and implementation in accordance with the procedures and confirmation of the status in which the identification, authentication, and authorization of operators are implemented

- Record of access and storage of access record as well as confirmation of the presence or absence of work beyond authorities

(3) Utilization and process

1) Clarification of the responsible official for operation

- Clarification of the responsible official for operation when personal data is utilized and processed

2) Clarification of the procedures and implementation in accordance with the procedures

- Clarification of the procedures in the utilization and process of personal data

- Implementation of utilization and process in accordance with the established procedures

- Implementation of utilization and process in a building, etc. where an unauthorized person can not enter

- Limitation, based on the operational necessity, of the computer terminals in which personal data can be utilized and processed

- Limitation, based on the operational necessity, of the functions that are installed in computer terminals in which personal data can be utilized and processed (for instance, to make the computer terminals, in which personal data can only be viewed, impossible to be connected with external record medium such as CD-R and USB Memory, etc.)

3) Identification, authentication, and authorization of operators

- Limitation, based on the operational necessity, of operators who make the utilization and process of personal data

- Identification of operators by authentication with ID and password or by biometric authentication, etc.

- Limitation of authorities given to operators (for instance, the operator who is required only to view personal data as its work does not need the authority to copy and duplicate personal data.)

- Record of authorities (for instance, copy, duplicate, print, delete, and change, etc.) given to operators who make the utilization and process of personal data

4) Confirmation of operators and their authorities

- Clarification of the procedures and implementation in accordance with the procedures and confirmation of the status in which the identification, authentication, and authorization of operators are implemented

- Record of access and storage of access record as well as confirmation of the presence or absence of work beyond authorities

(4) Storage and backup

1) Clarification of the responsible official for operation

- Clarification of the responsible official for operation when personal data is stored and backuped

2) Clarification of the procedures and implementation in accordance with the procedures

- Clarification of the procedures* in the storage and backup of personal data

  * When personal data is processed by an information system, the backup of not only personal data but also an operating system (OS) or applications might become necessary.

- Implementation of storage and backup in accordance with the established procedures

- Concealment such as encryption of personal data when the personal data is stored and backuped

- Proper management of encryption keys and passwords

- Lockup control of the places where the mediums recording personal data are stored

- Management of the key of the room or storage locker where the mediums recording personal data are stored

- Storage of the mediums recording personal data in a remote place

- Implementation of a test to recover data from the backup of personal data
- Record of various phenomena and troubles regarding the backup of personal data

3) Identification, authentication, and authorization of operators

- Limitation, based on the operational necessity, of operators who make the storage and backup of personal data
- Identification of operators by authentication with ID and password or by biometric authentication, etc.
- Limitation of authorities given to operators (for instance, when personal data is backuped, the operator who does this work does not need the authority to view and change the content of personal data.)
- Record of authorities (for instance, implementation of backup and management of the key of storage locker, etc.) given to operators who make the storage and backup of personal data

4) Confirmation of operators and their authorities

- Clarification of the procedures and implementation in accordance with the procedures and confirmation of the status in which the identification, authentication, and authorization of operators are implemented
- Record of access and storage of access record as well as confirmation of the presence or absence of work beyond authorities

(5) Erasure and disposal

1) Clarification of the responsible offcial for operation

- Clarification of the responsible official for operation when personal data is erased
- Clarification of the responsible official for operation when equipments that store personal data and devices that record personal data are disposed of

2) Clarification of the procedures and implementation in accordance with the procedures

- Clarification of the procedures in erasure and disposal
- Implementation of erasure and disposal in accordance with the established procedures

- Implementation of erasure and disposal works in a building, etc. where an unauthorized person can not enter

- Limitation, based on the operational necessity, of the computer terminals in which personal data can be erased

- Complete erasure of data before mediums and equipments in which personal data is recorded are returned to leasing companies (for instance, overwriting mediums with meaningless data once or several times)

- Physical destruction of mediums in which personal data is recorded (for instance, destroying them with a shredder or a media shredder, etc.)

3) Identification, authentication, and authorization of operators

- Limitation, based on the operational necessity, of operators who can make the erasure and disposal of personal data

- Identification of operators by authentication with ID and password or by biometric authentication, etc.

- Limitation of authorities given to operators

- Record of authorities given to operators who make the erasure and disposal of personal data

4) Confirmation of operators and their authorities

- Clarification of the procedures and implementation in accordance with the procedures and confirmation of the status in which the identification, authentication, and authorization of operators are implemented

- Record of access and storage of access record as well as confirmation of the presence or absence of work beyond authorities

Human security control measures

The human security control measures mean to conclude the nondisclosure agreement of the personal data that is specified as operational secret with workers and to educate and train them.

[Matters to be taken as human security control measures]

1) Concluding the nondisclosure agreement with workers when signing the employment contract and concluding the nondisclosure agreement between an entruster and trustee in the entrustment contract, etc. (including the contract of supply of temporary laborer)

2) Implementing familiarization of workers with internal regulations, etc., as well as education and training of them

Meanwhile, as for the manager's supervision about the observance of the established regulations, etc., refer to Article 21 of the Act.

[Exemplifications of the means which are preferable to be taken for the practice of each item of above matters]

1) Exemplifications of the means which are preferable to be taken for the practice of "Concluding the nondisclosure agreement with workers when signing the employment contract and concluding the nondisclosure agreement between an entruster and trustee in the entrustment contract, etc. (including the contract of supply of temporary laborer)"

- Conclusion of the agreement of nondisclosure when hiring workers and concluding the entrustment contract

  * It is preferable to make the nondisclosure clause in the employment contract and the entrustment contract, etc. remain in effect for a certain period after the expiration of contracts.

  * It is conceivable to stipulate the duties of nondisclosure about personal information in the in-house regulations such as the working rules, etc. Meanwhile, when stipulating the duties of nondisclosure about personal information in the in-house regulations, specially, it is necessary to observe the provisions of labor related laws including Article 89 and 90 of the Labor Standards Law.

  * Even when the confidentiality agreement targeting the trade secret is concluded concurrently with the conclusion of the nondisclosure agreement of personal information, because of the differences between the personal information protection and the trade secret protection in purposes and scopes, it is preferable to make sharp distinction between the agreement about the personal information protection and the confidentiality agreement about the trade secret from the viewpoint of the sense of assent of workers (regardless of whether these agreements are separate documents or not).

- Preparing the regulations regarding the measures against the violation of the nondisclosure agreement

  * It is preferable that the contract, etc. contains the provisions on the scope of the relevant persons who can access the information system which handles personal data and who may enter the building, etc. where personal data is stored, though those persons are not the workers who handle personal data, as well as the condition of access. Meanwhile, those who are not the workers who handle personal data include the relevant persons in the development and maintenance of information system, the persons in charge of cleaning up, and the security guards, etc.

2) Exemplifications of the means which are preferable to be taken for the practice of "Implementing familiarization of workers with internal regulations, etc., as well as education and training of them"

- Familiarizing the internal regulations, etc. providing the roles and responsibilities of workers regarding the security control of personal data and information system

- Implementing to educate and train about the roles and responsibilities of workers regarding the security control of personal data and information system

- Confirming that the necessary and proper education and training to workers are implemented

Physical security control measures

The physical security control measures mean the measures of the control for entering and leaving a building (room) and of the prevention of personal data theft, etc.

[Matters to be taken as physical security control measures]

1) Implementing the control for entering and leaving a building (room)

2) Preventing theft, etc.

3) Physically protecting equipments and devices, etc.

[Exemplifications of the means which are preferable to be taken for the practice of each item of above matters]

1) Exemplifications of the means which are preferable to be taken for the practice of "The control for entering and leaving a building (room)"

- Implementation of the work handling personal data in a room that is physically protected by the control for entering and leaving a building (room)

- Installation of the information system, etc. handling personal data in a room, etc. that is physically protected by the control for entering and leaving a building (room)

2) Exemplifications of the means which are preferable to be taken for the practice of "Preventing theft, etc."

- Prohibition of leaving documents, mediums, and portable computers, etc. with personal data on a desk or in a car, etc.

- Prevention of peek by starting a screen saver with a password, etc. when leaving desk

- Locked storage of medium with personal data

- Separate storage between the personal data containing name, address, e-mail address, etc. and other personal data

- Prohibition of leaving the operation manual of information system handling personal data on a desk

3) Exemplifications of the means which are preferable to be taken for the practice of "Physically protecting equipments and devices, etc."

- Physical protection of the equipments and devices, etc. handling personal data from the security control threat (for instance, theft, destruction, and damage) and from the environmental threat (for instance, water leakage, fire, and power stoppage)

Technical security control measures

The technical security control measures mean such technical measures to provide the security control for personal data as access control to personal data and the information system handling it, countermeasures against unauthorized software, and monitoring information system.

[Matters to be taken as technical security control measures]

1) Identification and authentication for access to personal data

2) Control of access to personal data

3) Management of authority to access personal data

4) Record of access to personal data

5) Countermeasures against unauthorized software regarding an information system handling personal data

6) Measures when transferring and transmitting personal data

7) Measures when confirming the operation of information system handling personal data

8) Monitoring an information system handling personal data

[Exemplifications of the means which are preferable to be taken for the practice of each item of above matters]

1) Exemplifications of the means which are preferable to be taken for the practice of "Identification and authentication for access to personal data"

- Implementation of the identification and authentication of a person who has a proper authority to access personal data for the confirmation of proper access to personal data (for instance, authentication with ID and password or biometric authentication, etc.)

  * When IDs and passwords are used, it is preferable to take such measures as establishment of password expiration date, restriction of the reuse of same or similar password, establishment of the minimum number of password characters, and suspension of ID with which login was failed more than certain times.

- Implementation of the identification and authentication of a computer terminal and an e-mail address, etc. that can be used by a person who has an authority to access personal data (for instance, MAC address authentication, IP address authentication, and authentication by electronic certificate or secret sharing technology, etc.)

2) Exemplifications of the means which are preferable to be taken for the practice of "Control of access to personal data"

- Minimizing the number of persons to whom the authority to access personal data is given

- Implementation of access control based on identification (The condition, in which anybody can access a file with a password, has an access control but not an identification. In such condition, it is necessary that those who know the password should be specified and that the password should be properly changed whenever a person who is authorized to access is changed.)

- Minimizing the authorities to be given to a person who has an authority to access

- Restriction of the number of concurrent users of the information system storing personal data

- Restriction of the utilization time of the information system storing personal data (for instance, to make it impossible to access an information system during the period of time after business hours including holiday, etc.)

- Protection of the information system storing personal data from unauthorized accesses (for instance, to establish firewall and router, etc.)

- Prevention of the unauthorized utilization of an application that can access personal data (for instance, to mount an authentication system on an application system, to install an necessary application system only in the computer that is used by a person based on the operational requirement, and to make a computer display only functions necessary for operations in menus, etc.)

  * It is preferable to control the access of even a privileged user of an information system so that the user can not directly access personal data if the user does not need to know the content of personal data in the administration

of information system.

* For the control of the access of privileged user, it is conceivable to use, for example, a Trusted OS, a Secure OS, and a product providing access control function.

- Verification of the effectiveness of the access control function that was introduced to an information system handling personal data (for instance, verification of the presence or absence of the vulnerability of web application)

3) Exemplifications of the means which are preferable to be taken for the practice of "Management of authority to access personal data"

- Proper and periodical implementation of the management of authority that permit a person to access personal data (for instance, to perform an adequate examination for the aptitude of an operator conducting the registration of persons who regularly access personal data, and to make only the operator who passed the examination be able to conduct the registration work, etc.)

- Implementation of the control to make the volume of access to an information system handling personal data necessity minimum

4) Exemplifications of the means which are preferable to be taken for the practice of "Record of access to personal data"

- Record of successes and failures in accessing or manipulating personal data (for instance, when it is unable to record the access to or manipulation of personal data, record of successes and failures in accessing or manipulating an information system)

- Proper protection of collected record from leakage, loss, and damage

  * It is necessary to pay attention to that sometimes the record of information system handling personal data may correspond to personal information.

5) Exemplifications of the means which are preferable to be taken for the practice of "Countermeasures against unauthorized software regarding an information system handling personal data"

- Introduction of an antivirus software

- Application of a correction software for security measures (so-called a security patch) to an Operating System (OS) and applications

- Confirmation of the effectiveness and stability of countermeasures against unauthorized software (for instance, confirmation of the update of pattern file and correction software)

6) Exemplifications of the means which are preferable to be taken for the practice of "Measures when transferring (transport, mailing, and home delivery service, etc.) and transmitting personal data"

- Measures when being lost or stolen at the time of transferring (for instance, concealment of personal data stored in a medium by encryption, etc.)

- Concealment of personal data by encryption, etc. when the personal data is transmitted (for instance, data transfer, etc. including an entry or access by the person or a worker and a transmission of file attached to an e-mail message, etc.) through a network (for instance, internet or wireless LAN, etc.) where there is a possibility of sniffing

7) Exemplifications of the means which are preferable to be taken for the practice of "Measures when confirming the operation of information system handling personal data"

- Prohibition of the utilization of personal data as test data when confirming the operation of information system

- Verification that when an information system is changed, the security of information system and operational environment is not damaged by the changes

8) Exemplifications of the means which are preferable to be taken for the practice of "Monitoring an information system handling personal data"

- Periodical monitoring of the condition of use of information system handling personal data

- Monitoring of the condition of access (including the detail of manipulation) to personal data

  * It is necessary to pay attention to that sometimes the record of monitoring result on information system handling personal data may correspond to personal information.

2-2-3-3 Supervision of Worker (an issue related to Article 21 of the Act)

Article 21 of the Act When an entity handling personal information has an employee handle personal data, it must exercise necessary and appropriate supervision over the employee concerned to ensure the control of security of the personal data concerned.

An entity handling personal information, in order to make a worker observe the security control measures based on Article 20 of the Act, must exercise necessary and appropriate supervision over the worker (excluding cases corresponding to 2-1-4. "* Explanation about handling of telephone directory and car navigation system, etc."). At the same time, considering the magnitude of the infringement of rights and interests that the person incurs

when the personal data of the person is leaked, lost, or damaged, etc., the necessary and proper measures must be taken depending on the risks attributable to the nature of business and the status of handling personal information, etc.

Meanwhile, the term "a worker" means a person who is engaged in the business of an entity handling personal information under the direct or indirect instruction and supervision of the business operator within the organization of the business operator, and includes not only a hired employee (permanent employee, contract employee, part-time employee, and temporary employee, etc.) but also a director, an executive officer, an administration officer, an auditor, an inspector, and a dispatched employee, etc.

[Cases in which necessary and appropriate supervision is not exercised over the workers]

Case 1 When personal data was leaked as a result of not confirming periodically in the predetermined time interval whether the worker worked in accordance with the regulations, etc. stipulating the security control measures for personal data

Case 2 When a notebook computer or an external recording medium where personal data was contained was stolen and the personal data was leaked as a result of letting a behavior of taking above mentioned computer or medium out in violation of the internal regulations, etc. continue unchecked although such a behavior had been repeated

[Points to keep in mind when monitoring workers]

When the video or online monitoring of workers (hereinafter referred to as "monitoring") is implemented as the supervision of workers and trustees regarding the handling of personal data or as part of other security control measures, the following points should be kept in mind.

On this occasion, when the important matters regarding the handling of personal information relating to employment management are specified, it is preferable to inform to labor unions, etc. in advance and hold consultations with them as necessary. Also, once such important matters are specified, it is preferable to familiarize laborers, etc. with them.

Meanwhile, the important matters regarding the handling of personal information relating to employment management, which are provided in the Guidelines and Item 1 of Paragraph 9 of Article 3 of the Guidelines Concerning Measures to be Taken by Entities to Ensure the Proper Handling of Personal Information Relating to Employment Management (Announcement No. 259 of 2004 by the Ministry of Health, Labour and Welfare), are the matters as are related to monitoring.

- To specify in advance the purpose of monitoring, that is to say, the Purpose of Utilization of personal information to be acquired, and to expressly show it to workers as well as to stipulate it in the in-house regulations

- To establish the responsible official for the implementation of monitoring and its authority

- To establish in advance the proposed in-house regulations that stipulate the implementation of monitoring, and to provide through announcement on them in the company beforehand

- To confirm or audit whether the monitoring is properly implemented

2-2-3-4 Supervision of Trustees (an issue related to Article 22 of the Act)

Article 22 of the Act When an entity handling personal information entrusts an individual or entity with the handling of personal data in whole or in part, it must exercise necessary and appropriate supervision over the trustee to ensure the control of security of the entrusted personal data.

When an entity handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it must exercise necessary and appropriate supervision over the trustee to ensure the observance of the security control measures based on Article 20 of the Act (excluding cases corresponding to 2-1-4. "* Explanation about handling of telephone directory and car navigation system, etc."). At the same time, considering the magnitude of the infringement of rights and interests that the person incurs when the personal data of the person is leaked, lost, or damaged, etc., the necessary and proper measures must be taken depending on the risks attributable to the nature of business and the status of handling personal information, etc.

The "necessary and appropriate supervision" includes that an entrustment contract contains the measures which are mutually agreed upon by both parties of entruster and trustee as necessary and appropriate measures regarding the handling of personal data, and that it is confirmed periodically in the predetermined time interval whether such measures are properly executed.

Meanwhile, when a party who is in a dominant bargaining position is an entruster, the entruster must not impose on the trustee such an unfair burden as unilaterally inflicting on the trustee the obligation concerning the person's claim for damage compensation in disregard of the burden sharing concerning the security control measures.

In addition, when an entruster does not exercise "necessary and appropriate supervision" over a trustee and the trustee reentrusts, the original entruster may well take the responsibility on itself if some sort of trouble arises due to an inappropriate handling by the entity which was reentrusted. Accordingly, a careful attention is required.

[Cases in which necessary and appropriate supervision is not exercised over the trustees]

Case 1 When the handling of personal data was entrusted to an outside entity without periodically grasping the status of security control measures for the personal data at the time and after a contract was concluded and when the trustee leaked the personal data

Case 2 When a trustee leaked personal data as a result that an entruster did not instruct the trustee on the content of the security control measures that was established regarding the handling of personal data

Case 3 When an entity which was reentrusted leaked personal data as a result that although an entruster did not instruct a trustee about the conditions of reentrustment and failed to confirm the status of the trustee's handling of personal data, the trustee reentrusted the entity

[Matters which are preferable to be contained in a contract when the handling of personal data is trusted]

- Clarification of the responsibilities of entruster and trustee
- Matters regarding the security control of personal data
  - Matters regarding the prevention of the leakage of personal data and the prohibition of the fraudulent use of personal data
  - Prohibition of process and use beyond the scope of entrustment contract
  - Prohibition of copy and duplicate beyond the scope of entrustment contract
  - Contract period
  - Matters regarding the return, erasure, and disposal of personal data after the expiration of an entrustment contract
- Matters regarding reentrustment
  - Report in writing to an entruster when reentrusting
- Content and frequency of report regarding the status of handling personal data to an entruster
- Confirmation that the provisions of contract are observed (for instance, an information security audit, etc. is included)
- Measures when the provisions of contract are not observed
- Matters regarding report and communication when a security incident or accident occurs

2-2-4 Provision to A Third Party (an issue related to Article 23 of the Act)

(1) Principle (an issue related to Paragraph 1 of Article 23 of the Act)

Paragraph 1 of Article 23 of the Act An entity handling personal information 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

An entity handling personal information must not provide personal data to a third party without obtaining, in advance[*1], the consent of the person[*2] (excluding cases corresponding to 2-1-4. "* Explanation about handling of telephone directory and car navigation system, etc."). When the consent is obtained, depending on the nature of business and the status of handling personal information, the content within the reasonable and appropriate scope that is deemed necessary for the person's judgment about the consent must be expressly showed.

*1 The phrase "in advance" means "in advance of the provision of personal data to a third party".

*2 As for "obtaining the consent of the person", refer to 2-1-10.

[Cases deemed a provision to a third party] (However, excluding the cases of each Item of Paragraph 4 of Article 23 of the Act)

Case 1 When exchanging personal data between a parent company and a subsidiary company, among fellow subsidiary companies, and among group companies

Case 2 When exchanging personal data between a headquarters for a franchise organization and franchisees

Case 3 When exchanging the specific personal data among persons or entities in the same business

Case 4 When providing the personal data of an individual residing in Japan to a foreign company

[Cases not deemed a provision to a third party] (However, being restricted by the Purpose of Utilization)

Case: To provide personal data to the other departments within the same entity

Meanwhile, in the following cases, the personal data can be provided to a third party without the consent of the person.

(i) Cases in which the provision of personal data is based on laws and regulations

(The cases are similar to those in 2-2-1. (5) (i).)

[Additional case]

Case: When a target business operator submits materials upon the request of an authorized personal information protection organization to submit materials, etc. based on Paragraph 2 of Article 42 of the Act

(ii) Cases in which there is a possible infringement of concrete rights and interests such as the life, body, or property of an individual (including a juridical person) and when the provision of personal data is necessary to protect them and when it is difficult to obtain the consent of the person (excluding cases in which it is substantially possible to protect the rights and interest concerned by other methods)

(The cases are similar to those in 2-2-1. (5) (ii).)

(iii) Cases in which the provision of personal data is specially necessary for improving public health or promoting the sound growth of children who are still developing both mentally and physically and when it is difficult to obtain the consent of the person (excluding cases in which it is substantially possible to improve public health or promote the sound growth of children by other methods)

(The cases are similar to those in 2-2-1. (5) (iii).)

(iv) Cases in which a state organ, etc. needs to obtain cooperation from a private company, etc. in executing the affairs prescribed by laws and regulations and when it is recognized that obtaining the person's consent on the submission of personal data by the cooperating private company, etc. to the state organ, etc. concerned are likely to impede the execution of the affairs concerned

(The cases are similar to those in 2-2-1. (5) (iv).)

(2) Opt-out (an issue related to Paragraph 2 of Article 23 of the Act)

Paragraph 2 of Article 23 of the Act 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 following items or put those matters in a readily accessible condition for the person, the entity may, notwithstanding the provision of the preceding paragraph, provide such personal data concerned to third parties:

(1) The fact that the provision to third parties is the Purpose of Use

(2) The items of the personal data to be provided to third parties

(3) The means or method of provision to third parties

(4) The fact that the provision of such personal data as will lead to the identification of the person concerned to third parties will be stopped at the request of the person

When a business operator has an opt-out in the provision to a third party[*1], the entity handling personal information can, notwithstanding the provision of the preceding paragraph, provide personal data to a third party without the consent of the person.

However, as the provision to a third party corresponds to the utilization other than for intended purposes when the Purpose of Utilization specified by the provision of Paragraph 1 of Article 15 of the Act does not include the matters regarding the provision of personal data to a third party, the provision to a third party based on opt-out can not be made.

When providing personal data to a third party by the method of opt-out, it is preferable that an entity handling personal information as a provider avoids forbidding a providee to disclose the place to obtain the personal data, for example, selling a directory contingent on not disclosing the place to obtain the directory.

[Cases of opt-out]

Case 1 House map maker (producing a house map by examining doorplates or mailboxes and selling it (provision to the unspecified large number of people as a third party))

Case 2 Database service provider (producing a directory for a direct-mail advertising, etc. and selling it)

*1 The phrase “opt-out in the provision to a third party” means to discontinue, at the request of a person, the provision to a third party in addition to notifying, in advance of the provision, the person[*2] of all the matters listed in the following item 1) to 4) or putting those matters in a readily accessible condition for the person[*3].

*2 As for “notifying the person”, refer to 2-1-7.

*3 As for “readily accessible condition for the person”, refer to 2-1-11.

1) The fact that the provision to a third party is the Purpose of Utilization

2) Items of the personal data to be provided to a third party

Case 1 Name, address, and telephone number

Case 2 Name and goods buying history

3) Means or method of provision to a third party

Case 1 Publishing as a book

Case 2 Displaying in the Internet

Case 3 Handing the printout

4) The fact that the provision to a third party will be discontinued at the request of the person

(3) A party not corresponding to a third party (an issue related to Paragraph 4 of Article 23 of the Act)

As a party receiving personal data is not corresponding to a third party in the cases of the following items (i) to (iii), an entity handling personal information can provide information, without the consent of the person or having an opt-out in the provision to a third party, to such a party.

(i) Entrustment (an issue related to Item 1 of Paragraph 4 of Article 23 of the Act)

Item 1 of Paragraph 4 of Article 23 of the Act In following the cases, the individual or entity receiving such personal data shall not be deemed a third party for the purpose of application of the preceding three paragraphs: (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

When an entity handling personal information entrust an operation regarding the handling of personal data in whole or in part with a trustee, the trustee is not corresponding to a third party.

A responsibility for the supervision of trustee is imposed on an entity handling personal information (an issue related to Article 22 of the Act).

Case 1 When personal data is passed for the entrustment of information-processing such as data entry, etc.

Case 2 When a department store passes personal data to a home delivery company for the delivery of ordered goods

(ii) Succession of business (an issue related to Item 2 of Paragraph 4 of Article 23 of the Act)

Item 2 of Paragraph 4 of Article 23 of the Act

In following the cases, the individual or entity receiving such personal data shall not be deemed a third party for the purpose of application of the preceding three paragraphs:

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

When personal data is transferred due to the succession of business in a merger, a split-up of a company, and a transfer of business, etc., the party to which the personal data is transferred is not corresponding to a third party.

Even after the succession of business, personal data must be used within the scope of the Purpose of Utilization which existed before the personal data was transferred.

When a company provides personal data owned by the company to an another company in response to the investigation by the another company at the stage of bargaining prior to the conclusion of contract for the succession of business, such provision of personal data can be a provision to a third party. Accordingly, a careful attention is required.

Case 1 When personal data is passed to a new company created by a merger or a split-up of a company

Case 2 When personal data is passed to a transferee company in accordance with the transfer of business

(iii) Joint use (an issue related to Item 3 of Paragraph 4 of Article 23 of the Act)

Item 3 of Paragraph 4 of Article 23 of the Act

In following the cases, the individual or entity receiving such personal data shall not be deemed a third party for the purpose of application of the preceding three paragraphs:

(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

When personal data is used jointly between specific parties, if information on the following items 1) to 4) is, in advance[*1], notified to the person[*2] or put in a readily accessible condition for the person[*3] and the fact of joint use is made clear, the party to which the personal data is transferred is not corresponding to a third party. Also, when a specific entity jointly uses the personal data that has been already acquired by that entity with other entities, the entity which has already acquired the personal data must jointly use within the scope of the Purpose of

Utilization that was specified pursuant to the provision of Paragraph 1 of Article 15 of the Act.

Meanwhile, the judgment whether it is a joint use or an entrustment is made according to the form of the handling of personal data. Even when a trustee is included in the scope of the joint users, a relationship between the entruster and the trustee is not corresponding to a joint use and the entruster has no immunity from a duty to supervise the trustee. For example, when an event is held by group companies, it will be a joint use that a parent company (administrative company) gathers customer information from subsidiary companies and sends out the note of invitation to an exhibition. However, when an event is held by a company, it will be an entrustment but a joint use that the company provides customer information to a mailing service company for dispatching the note of invitation even though the mailing service company is one of group companies included in the scope of the joint users.

*1 The phrase “in advance” means “in advance of the joint use of personal data”.

*2 As for “notified to the person”, refer to 2-1-7.

*3 As for “readily accessible condition for the person”, refer to 2-1-11.

[Cases in which a joint use is conducted]

Case 1 When information is jointly used within the scope of the Purpose of Utilization in order for the offering of comprehensive service by group companies

Case 2 When personal data is jointly used within the scope of the Purpose of Utilization between a parent company and a subsidiary company and among fellow subsidiary companies

Case 3 When personal data is jointly used with a foreign company within the scope of the Purpose of Utilization

1) Items of the personal data to be jointly used

Case 1 Name, address, and telephone number

Case 2 Name and goods buying history

2) Scope of the joint users (although it is required that the range is clear for the person, an individual enumeration might be unnecessary sometimes as long as the range is clear.)

3) Users’ Purpose of Utilization (every Purpose of Utilization of personal data that is jointly used)

4) Name of an individual or business operator who accepts a request for disclosure as well as a complaint and makes efforts to handle it, has an authority to disclose, correct, and discontinue to utilize, etc. the content of personal data, etc., and is responsible for the management, including security control, of personal data (among joint users, a business operator, who primarily has the authority of

accepting and handling a complaint as well as disclosing and correcting, etc. personal data, is called a "responsible individual or entity", and a "responsible individual or entity" does not mean a responsible official within a joint user.)

Paragraph 5 of Article 23 of the Act

When an entity handling personal information changes the purpose for which the personal data is used or the name of the individual or entity responsible for the management of the personal data as are mentioned in Item 3 of the preceding paragraph, the entity must, in advance, notify the person of the content of the change or put it in a readily accessible condition for the person.

Although the above 1) and 2) can not be changed, 3) and 4) can be changed within the scope which is considered to be not difficult for the person to imagine[*1] under the social standards. Prior to the change, the content of the change must be notified to the person[*2] or put in a readily accessible condition for the person[*3].

*1 As for "within the scope which is considered to be not difficult for the person to imagine", refer to 2-2-1. (2).

*2 As for "notified to the person", refer to 2-1-7.

*3 As for "readily accessible condition for the person", refer to 2-1-11.

(4) Issue related to personal data regarding employment management

Among the provisions of personal data to a third party (excluding cases corresponding to Item 1 to 4 of Paragraph 1 of Article 23 of the Act), as for the one regarding employment management, it is preferable to pay attention to matters listed in the following items. At the same time, the necessary and proper measures must be taken depending on the nature of business and the status of handling personal information, etc. regarding employment management.

The above stated the provision of personal data to a third party regarding employment management means a case in which when an employee is temporarily transferred to a subsidiary company, the personal data regarding employment management like information on the personnel evaluation of the employee concerned is provided to the subsidiary company and a case in which when a temporary personnel is dispatched, the personal data regarding employment management like information on the capability of engineer is provided. Therefore, such provision, as to a party who aims to make a database of information, provided by a company, on personal data including the names and positions of employees of the company as well as to publish and sell it, is not corresponding to the provision of personal data to a third party regarding employment management.

- The fact that a providee prohibits its workers from leaking and fraudulently using the personal information that was obtained by the workers through the handling of personal data concerned

- To obtain, in advance, the written consent of a business operator when the personal data concerned is reprovided

- To clarify the period of the storage, etc. of personal data in a providee

- The fact that personal data is returned and destroyed or deleted after the Purpose of Utilization is achieved as well as that a business operator confirms that those processes are properly and surely carried out

- To prohibit a providee from copying or duplicating personal data (excluding those actions aiming at the backup necessary for security control)

2-2-5 Public Announcement of Matters Concerning Retained Personal Data and Disclosure, Correction, and Discontinuance of the Utilization of Retained Personal Data, etc. (issues related to Article 24 to 30 of the Act)

2-2-5-1 Public Announcement of Matters Concerning Retained Personal Data, etc. (an issue related to Article 24 of the Act)

(1) Familiarization of the person with matters concerning retained personal data (an issue related to Paragraph 1 of Article 24 of the Act)

Paragraph 1 of Article 24 of the Act

With respect to the retained personal data, an entity handling personal information must put the matters enumerated in the following items in an accessible condition for the person (such condition includes cases in which a reply is made without delay at the request of the person):

(1) The name of the entity concerned handling personal information

(2) The Purpose of Use of all retained personal data (except in cases falling under any of Items 1 to 3 of Paragraph 4 of Article 18)

(3) Procedures to meet requests made pursuant to the provisions of the next paragraph, Paragraph 1 of the next article, Paragraph 1 of Article 26, or Paragraph 1 or Paragraph 2 of Article 27 (including the amount of charges if set under Paragraph 2 of Article 30)

(4) In addition to those mentioned in the preceding three items, such matters, specified by a Cabinet order, as being necessary for ensuring the proper handling of retained personal data

Article 5 of the Cabinet Order

Matters specified by a Cabinet Order under Item 4 of Paragraph 1of Article 24 of the Act shall be the matters as set forth below:

(1) The place where a complaint concerning the handling of retained personal data by the entity handling personal information concerned is lodged.

(2) If the entity handling personal information concerned is a target entity of an authorized personal information protection organization, the name of the authorized personal

information protection organization concerned and the place where settlement of the complaint is lodged.

With respect to the personal data, an entity handling personal information must put information on the following items 1) to 4) in an accessible condition for the person (such condition includes cases in which a response is made without delay at the request of the person)[*1] (excluding cases corresponding to 2-1-4. "* Explanation about handling of telephone directory and car navigation system, etc.").

Regarding the personal data that had been retained before the Act was enforced, no action was made to acquire personal information at the time of the enforcement of the Act, accordingly, as the provision of Article 18 of the Act does not apply, measures stipulated in Paragraph 1 of Article 24 of the Act need to be taken at the time of the enforcement of the Act.

*1 As for "accessible condition for the person (such condition includes cases in which a response is made without delay at the request of the person)", refer to 2-1-12.

1) Name of entity handling personal information

2) Purpose of Utilization of all retained personal data (However, the certain cases[*2] are excluded. The "Purpose of Utilization" is the same as that about personal information used in Article 15 and succeeding articles of the Act.)

*2 The phrase "certain cases" means the following:

   a) When notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the life, body, property, or other rights or interests of the person or a third party (The cases are similar to those in 2-2-2. (5) (i).)

   b) When notifying the person of the Purpose of Utilization or publicly announcing it are likely to infringe the rights or interests of the entity handling personal information (The cases are similar to those in 2-2-2. (5) (ii).)

   c) When a state organ, etc. needs to obtain cooperation from a private company, etc. in executing the affairs prescribed by laws and regulations and when notifying the person of the Purpose of Utilization obtained from the state organ, etc. or publicly announcing it by the cooperating private company, etc. are likely to impede the execution of the affairs concerned (The cases are similar to those in 2-2-2. (5) (iii).)

3) Amount of charges[*3] regarding the notice of the Purpose of Utilization of retained personal data and the disclosure of retained personal data (only when charges were set) and procedures to request disclosure, etc.[*4]

*3 The charges regarding the request for disclosure pursuant to Article 16 of the Law Concerning Access to Information held by Administrative Organs (Act No. 42 of 1999) and Item 1 of Paragraph 1 of Article 13 of the Cabinet Order for the enforcement of the Law (Cabinet Order No. 41 of 2000) are 300 yen (The charges for executing disclosure occur separately.).

*4 The phrase “to request disclosure, etc.” means to request notice of the Purpose of Utilization of retained personal data, disclosure of retained personal data, correction, addition, or deletion of the content of retained personal data, discontinuance of the use or erasure of retained personal data, or discontinuance of the provision to a third party of retained personal data.

4) Place where a complaint or inquiry concerning the handling of retained personal data is lodged (When an entity handling personal information belongs to an authorized personal information protection organization[*5], the name of the organization and the place to be lodged are included.)

*5 Explanation about the “authorized personal information protection organization” system

In this system, the competent minister authorizes a private organization that conducts a business for the purpose of ensuring the proper handling of personal information. It is intended, by the establishment of this system, to ensure the reliability of the business concerned and promote the protection of personal information by private organizations (refer to Article 37 and succeeding articles of the Act)

(Reference)

Paragraph 1 of Article 37 of the Act

A corporation (which includes an unincorporated organization with a specified representative or manager; this applies to (B) of Item 3 of the next article) that intends to conduct any of the businesses enumerated in the following items for the purpose of ensuring the proper handling of personal information by an entity handling personal information, may be authorized as such by the competent minister:

(1) The handling under Article 42 of complaints about the handling of personal information of such entities handling personal information as are the targets of the business (hereinafter called "target entities")

(2) The provision of information for target entities about the matters contributing to ensuring the proper handling of personal information

(3) In addition to those mentioned in the preceding two items, any business necessary for ensuring the proper handling of personal information by target entities

Paragraph 2 of Article 37 of the Act

An entity intending to receive authorization under the preceding paragraph must apply to the competent minister as prescribed by a Cabinet order.

Paragraph 3 of Article 37 of the Act

When having granted authorization under Paragraph 1, the competent minister must officially announce that effect.

Paragraph 1 of Article 42 of the Act

When an authorized personal information protection organization is requested by a person, etc. to solve a complaint about the handling of personal information by a target entity, corresponding to the request, the organization must give the person, etc. necessary advice, investigate the facts concerning the complaint and request the target entity to solve the complaint promptly by notifying the target entity concerned of the content of the complaint.

Paragraph 2 of Article 42 of the Act

When an authorized personal information protection organization considers it necessary for solving complaints lodged under the preceding paragraph, the organization may request the target entity concerned to explain in writing or by mouth, or request it to submit relevant materials.

Paragraph 3 of Article 42 of the Act

When a target entity has received a request under the provision of the preceding paragraph from an authorized personal information protection organization, the target entity must not reject the request without justifiable reason.

(2) Notice of the Purpose of Utilization of retained personal data (an issue related to Paragraph 2 and 3 of Article 24 of the Act)

Paragraph 2 of Article 24 of the Act

When an entity handling personal information is requested by a person to notify him or her of the Purpose of Use of such retained personal data as may lead to the identification of the person concerned, the entity must meet the request without delay. However, this provision shall not apply to cases falling under either of the following items:

(1) Cases in which the Purpose of Use of such retained personal data as may lead to the identification of the person concerned is clear under the provision of the preceding paragraph

(2) Cases falling under any of items (1) to (3) of Paragraph 4 of Article 18

Paragraph 3 of Article 24 of the Act

When an entity handling personal information has decided not to notify the Purpose of Use of such retained personal data as is requested under the preceding paragraph, the entity must notify the person of that effect without delay.

When an entity handling personal information is requested by a person to notify him or her of the Purpose of Utilization of such retained personal data as may lead to the identification of himself or herself, excluding the cases listed in the following items (i) to (iv), the business

operator must notify the person* without delay. Meanwhile, even when an entity handling personal information has decided not to notify the Purpose of Utilization, the business operator must notify the person of that effect without delay (excluding cases corresponding to 2-1-4. "* Explanation about handling of telephone directory and car navigation system, etc.").

* As for "notify the person", refer to 2-1-7.

(i) Cases in which the Purpose of Utilization of such retained personal data as may lead to the identification of a person itself is clear due to the measures in accordance with the preceding section (1)

(ii) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the life, body, property, or other rights or interests of the person or a third party

(The cases are similar to those in 2-2-2. (5) (i).)

(iii) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to infringe the rights or interests of the entity handling personal information

(The cases are similar to those in 2-2-2. (5) (ii).)

(iv) Cases in which a state organ, etc. needs to obtain cooperation from a private company, etc. in executing the affairs prescribed by laws and regulations and when obtaining the consent of the person by notifying the person of the Purpose of Utilization obtained from the state organ, etc. or publicly announcing it by the cooperating private company, etc. is likely to impede the execution of the affairs concerned

(The cases are similar to those in 2-2-2. (5) (iii).)

2-2-5-2 Disclosure of Retained Personal Data (an issue related to Article 25 of the Act)

Paragraph 1 of Article 25 of the Act

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 (such disclosure includes notifying the person that the entity has no such retained personal data as may lead to the identification of the person concerned. This applies hereinafter.), the entity must disclose the retained personal data concerned without delay by a method prescribed by a Cabinet order. However, in any of the following cases, the entity may keep all or part of the retained personal data undisclosed:

(1) Cases in which disclosure might harm the life, body, property, or other rights or interests of the person or a third party

(2) Cases in which disclosure might seriously impede the proper execution of the business of the entity concerned handling personal information

(3) Cases in which disclosure violates other laws

Article 6 of the Cabinet Order

The method specified by a Cabinet Order under Paragraph 1 of Article 25 of the Act shall be the provision of documents (or the method agreed upon by the person requesting disclosure, if any).

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 itself (If no such retained personal data exists, notifying the person of that effect is included.), the business operator must disclose the retained personal data concerned to the person without delay by the method of the provision of documents (or the method agreed upon by the person requesting disclosure, if any[*1]) (excluding cases corresponding to 2-1-4. "* Explanation about handling of telephone directory and car navigation system, etc.").

Meanwhile, when the procedures for disclosure are separately set forth by the provisions of other laws and regulations, such procedures for disclosure as are separately set forth have a priority. With respect to the procedures to meet the request for the disclosure of employment management information, an entity handling personal information must endeavor, after the consultation with labor unions, etc. in advance if necessary, to specify the matters concerning the disclosure of the retained personal data that is envisaged not to disclose because the disclosure of all or part of the retained personal data that is requested by the person to disclose falls under the case in which the proper execution of the business is likely to be seriously impeded, and to take such measures as to familiarize laborers, etc. with it.

*1 Explanation about "the method agreed upon by the person requesting disclosure, if any"

This phrase means that the various methods including an e-mail message and a telephone call are appropriate as the methods of disclosure if a person who made a request agrees upon them and that a method by the provision of documents is appropriate even without such person's agreement. When a person who made a request for disclosure did not specify the particular method of disclosure and did not express an objection to the method offered by an entity handling personal information (including a case in which a reply to an inquiry is made by the same telephone call, after necessary personal identity verification, etc., when a request for disclosure is made by telephone), it can be considered that such person agreed upon the method concerned. It is conceivable as a way to obtain an agreement from a person who made a request that an entity handling personal information chooses a method among some methods desired by such person after the business operator concerned offered the methods of disclosure.

However, when the disclosure results cases falling under any of the following items (i) to (iii), the entity handling personal information is able not to disclose all or part of retained personal data. In this instance, the business operator must notify the person[*2] of that effect.

*2 As for "notify the person", refer to 2-1-7.

(i) When disclosure is likely to harm the life, body, property, or other rights or interests of the person or a third party

Case When the disclosure of disease name, etc. by a medical institution is likely to worsen the psychophysical condition of the person

(ii) When disclosure is likely to seriously impede the proper execution of the business of an entity handling personal information

Case 1 When the disclosure of all grading information by a examination-implementing institution likely to seriously impede the maintenance of examination system

Case 2 When disclosure is likely to seriously impede the execution of business including a case in which the operation of responding to other inquiries can not keep going as the repeated request from the same person for the disclosure of the same matter that needs a complex response practically occupies an inquiry counter

(iii) When disclosure violates other laws and regulations

Case When the disclosure of personal data that contains the record of a financial institution's report to the competent minister on transactions pursuant to Paragraph 1 of Article 54 of the Act for Punishment of Organized Crimes, Control of Crime Proceeds and Other Matters violates the provision of Paragraph 2 of that article

2-2-5-3 Correction of Retained Personal Data, etc. (an issue related to Article 26 of the Act)

Paragraph 1 of Article 26 of the Act

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, except in cases in which special procedures are prescribed by any other laws for such correction, addition, or deletion, make a necessary investigation 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.

Paragraph 2 of Article 26 of the Act

When an entity handling personal information has corrected, added, or deleted all or part of the retained personal data as requested 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.

When an entity handling personal information is requested by a person to correct, add, or delete retained personal data on the ground that the retained personal data contains errors and is contrary to the fact, the business operator in principle[*1] must make a correction, etc.[*2] If a correction, etc. is performed, the business operator must notify the person of the content of the correction, etc. without delay (excluding cases corresponding to 2-1-4. "* Explanation about handling of telephone directory and car navigation system, etc.").

Meanwhile, when the special procedures are set forth by the provisions of other laws and regulations, such special procedures have a priority.

*1 The "principle": When a correction, etc. is not necessary in light of the Purpose of Utilization or when the pointing out that there is an error is not correct, it is not necessary to make a correction, etc. However, in that case, an entity handling personal information must notify the person[*3] without delay that a correction, etc. will not be made.

*2 The term "correction, etc." means the correction, addition, or deletion[*4] of the content of retained personal data.

*3 As for "notify the person", refer to 2-1-7.

*4 The term "deletion" means to exclude unnecessary information.

[Case no need of making a correction]

Case When the object of correction, etc. is information about not a fact but an evaluation

2-2-5-4 Discontinuance of the Utilization of Retained Personal Data, etc. (an issue related to Article 27 of the Act)

Paragraph 1 of Article 27 of the Act

Where an entity handling personal information 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 Article 17, 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.

Paragraph 2 of Article 27 of the Act

Where an entity handling personal information 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.

Paragraph 3 of Article 27 of the Act

When an entity handling personal information has stopped using or has erased all or part of the retained personal data as requested under Paragraph 1 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 preceding paragraph 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.

When an entity handling personal information is requested by a person, for the reason of the violation of procedures[*1], to make a discontinuance of the utilization, etc.[*2] of retained personal data, the business operator in principle[*3] must take the measures concerned. Meanwhile, if a discontinuance of the utilization, etc. is performed, the business operator must notify the person[*4] of that effect without delay (excluding cases corresponding to 2-1-4. "* Explanation about handling of telephone directory and car navigation system, etc.").

*1 The phrase "violation of procedures" means utilization other than for intended purposes without consent, wrongful acquisition, or provision to a third party without consent.

*2 The phrase "discontinuance of the utilization, etc." means discontinuance of the utilization, erasure[*5], or discontinuance of the provision of personal data to a third party.

*3 The "principle": When a discontinuance of the utilization, etc. is exceeding the extent necessary for redressing the violation or when the pointing out that there is the violation of procedures is not correct, it is not necessary to make a discontinuance of the utilization, etc. However, in that case, the entity handling personal information must notify the person without delay that a discontinuance of the utilization, etc. will not be made. Meanwhile, even when it is requested to erase all of retained personal data, if the violation of procedures can be redressed by the discontinuance of the utilization, the duties are deemed to be fulfilled by taking such measures. Accordingly, it is not always necessary to execute the requested measures as they are.

*4 As for "notify the person", refer to 2-1-7.

*5 The term "erasure" means to make the retained personal data unavailable as retained personal data and includes making it impossible to identify the specific individual from the retained personal data concerned and other measures in addition to the deletion of the retained personal data concerned.

2-2-5-5 Explanation of reasons (an issue related to Article 28 of the Act)

Article 28 of the Act

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 Paragraph 3 of the preceding article 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.

When an entity handling personal information notifies the person* that the business operator will not take the measures or will take different measures in cases of public announcement, disclosure, correction, or discontinuance of the utilization of retained personal data, etc., the business operator must endeavor to explain the reasons in conjunction with notifying.

* As for “notifies the person”, refer to 2-1-7.

2-2-5-6 Procedures to Meet Requests for Disclosure and Others (issues related to Article 29 of the Act)

Paragraph 1 of Article 29 of the Act

An entity handling personal information may, as prescribed by a Cabinet order, determine procedures for receiving requests that may be made pursuant to the provisions of Paragraph 2 of Article 24, Paragraph 1 of Article 25, Paragraph 1 of Article 26 or Paragraph 1 or Paragraph 2 of Article 27 (such requests are hereinafter called “a request for disclosure and others” in this article). In such a case, any person making a request for disclosure and others shall comply with the procedures concerned.

Paragraph 2 of Article 29 of the Act

An entity handling personal information may request a person making a request for disclosure and others to show sufficient items to identify the retained personal data in question. In this case, the entity must provide the information useful for the identification of the retained personal data in question or take any other appropriate measures in consideration of the person's convenience so that the person can easily and accurately make a request for disclosure and others.

Paragraph 3 of Article 29 of the Act

A person may, as prescribed by a Cabinet order, make a request for disclosure and others through a representative.

Paragraph 4 of Article 29 of the Act

When an entity determine the procedures for meeting requests for disclosure and others under the provisions of the preceding three paragraphs, the entity must take into consideration that the procedures will not impose excessively heavy burden on the persons making requests for disclosure and others.

Article 7 of the Cabinet Order

Matters concerning procedures for receiving requests for disclosure and others that an entity handling personal information may determine pursuant to the provision of Paragraph 1 of Article 29 of the Act shall be as set forth below:

(1) The place where requests for disclosure and others are to be filed

(2) Format of the documents (including records made by an electronic method, magnetic method or any other methods not recognizable to human senses) to be submitted and other methods of making requests for disclosure and others at the time of making requests for disclosure and others

(3) Methods of identifying a person making requests for disclosure and others as the principal or representative prescribed in the following article

(4) Methods of collecting charges set forth in Paragraph 1 of Article 30 of the Act

Article 8 of the Cabinet Order

The representative who may make requests for disclosure and others pursuant to the provision of Paragraph 3 of Article 29 of the Act shall be a representative set forth below:

(1) Attorney-in-fact of a minor or an adult ward

(2) Representative delegated by the person with making requests for disclosure and others.

(1) An entity handling personal information can determine the matters listed in the following items (i) to (iv) concerning procedures for receiving requests for disclosure and others[*1]. Also, when an entity handling personal information determined procedures for receiving requests for disclosure and others, the business operator must put those procedures in an accessible condition for the person (such condition includes cases in which a response is made without delay at the request of the person)[*2] (refer to the above 2-2-5-1.). Meanwhile, when an entity handling personal information determined procedures for receiving requests for disclosure and others within a reasonable scope, if a person making a request for disclosure and others does not comply with the procedures, the business operator can refuse to execute a disclosure and others.

*1 The phrase “requests for disclosure and others” means notice of the Purpose of Utilization of retained personal data, disclosure of retained personal data, correction, addition, or deletion of the content of retained personal data, discontinuance of the utilization or erasure of retained personal data, and discontinuance of the provision of retained personal data to a third party.

*2 As for “accessible condition for the person (such condition includes cases in which a response is made without delay at the request of the person)”, refer to 2-1-12.

(i) Place where requests for disclosure and others are to be received

(ii) Format of the documents (including records made by an electronic method, a magnetic method, or any other methods not recognizable to human senses) to be submitted at the time of making requests for disclosure and others as well as other methods of receiving requests for disclosure and others (including a method of receiving by mailing or faxing, etc.)

(iii) Methods of identifying a person making requests for disclosure and others as the principal or its representative ((A) attorney-in-fact of a minor or an adult ward, (B) representative delegated by the person with making requests for disclosure and others) (However, the method of identifying must be appropriate depending on the nature of business, the status of handling retained personal data, and the method of receiving requests for disclosure and others, etc. Furthermore, a business operator must take into consideration that the methods will not impose excessively heavy burden on the person making requests for disclosure and others such as not asking many information for identifying the person beyond necessity compared to the personal data retained by the business operator.)

Case 1 In the case of principal (visiting): driver's license, health insurance identification card, basic residents' registration card with a photo, passport, alien registration card, pension booklet, and seal-registration certificate together with a registered seal

Case 2 In the case of principal (online): ID together with a password

Case 3 In the case of principal (telephone): certain information registered (date of birth, etc.) and callback

Case 4 In the case of principal (sending (mailing and faxing, etc.)): copy of driver's license and copy of residence certificate

Case 5 In the case of principal (sending (mailing and faxing, etc.)): After receiving a copy of official certificate such as driver's license and health insurance identification card from a customer, etc., the entity handling personal information send the documents to the address of the customer, etc. described in the copy of the official certificated concerned by registered mail.

Case 6 In the case of representative (visiting): power of attorney showing the right to represent (when a parental authority person is an attorney-in-fact of a minor, copy or partial copy of a family register or copy of residence certificate in those which both a principal and its representative are described and their family relationship is indicated) as well as any of the following documents of a principal and its representative; driver's license, health insurance identification card, passport, alien registration card, pension booklet, and attorney registration number for an attorney

(iv) Methods of collecting charges that the entity handling personal information collects when notifying the Purpose of Utilization of retained personal data or disclosing retained personal data

Meanwhile, if the entity handling personal information does not determine the methods of receiving requests for disclosure and others, the business operator shall accept any style of application.

(2) An entity handling personal information can ask a person to submit the matters (address, ID, password, and membership number, etc.) necessary for identifying the person's own data so that the business operator can smoothly take procedures for disclosing, etc.

Meanwhile, the business operator must consider the person's convenience such as providing information contributing to the identification of the person's own data and others so that the person can easily identify its own data.

(3) When an entity handling personal information determines procedures to meet requests for disclosure and others, the business operator must consider not to impose such excessively heavy burden on the person as demanding cumbersome documents beyond necessity or limiting a counter receiving requests, separately from the offices executing other operations, to the place where is unnecessarily inconvenient.

2-2-5-7 Charges (an issue related to Article 30 of the Act)

Paragraph 1 of Article 30 of the Act When an entity handling personal information is requested to notify the Purpose of Use under Paragraph 2 of Article 24 or to make a disclosure under Paragraph 1 of Article 25, the entity may collect charges for taking the action concerned. Paragraph 2 of Article 30 of the Act When an entity handling personal information collects charges under the provision of the preceding paragraph, the entity must determine the amounts of charges within the scope considered reasonable in consideration of actual costs.

When an entity handling personal information is requested to notify the Purpose of Utilization of retained personal data or to make a disclosure of retained personal data, the business operator can determine the amount of charges for taking the measure. Also, when the amount of charges was determined, a business operator must put it in an accessible condition for the person (such condition includes cases in which a response is made without delay at the request of the person.)* (refer to the above 2-2-5-1.).

Meanwhile, when an entity handling personal information collects charges, the business operator must determine the amounts of charges within the scope considered reasonable in consideration of actual costs (refer to 2-2-5-1. (1) (III)).

* As for "accessible condition for the person (such condition includes cases in which a response is made without delay at the request of the person)", refer to 2-1-12.

2-2-6 Processing of Complaints (an issue related to Article 31 of the Act)

Paragraph 1 of Article 31 of the Act An entity handling personal information must endeavor to appropriately and promptly handle complaints about the handling of personal information.

Paragraph 2 of Article 31 of the Act

An entity handling personal information must endeavor to establish a system necessary for achieving the objective mentioned in the preceding paragraph.

An entity handling personal information must endeavor to appropriately and promptly process complaints about the handling of personal information. Also, in order to appropriately and promptly processes complaints, a business operator must endeavor to establish a necessary system such as creation of a complaints processing counter or institution of procedures for processing complaints. Nonetheless, it is not necessary to comply with even an impossible demand.

Meanwhile, when a necessary system is established, it is able to refer to the JISQ10002 "Quality management-Customer satisfaction-Guidelines for complaints handling in organizations" of the Japan Industrial Standards.

2-2-7 Transition Measures (an issue related to Article 2 to 5 of the Supplementary Provisions of the Act)

(Transition Measures Concerning a Consent of a Person)

Article 2 of the Supplementary Provisions of the Act

Where a person has given consent to the handling of his or her personal information before this Act is enforced, and where the consent is equivalent to the consent that allows the personal information to be handled for a purpose other than the Purpose of Use specified under Paragraph 1 of Article 15, then it shall be deemed that there is such consent as is prescribed in Paragraph 1 or 2 of Article 16.

Article 3 of the Supplementary Provisions of the Act

Where a person has given consent to the handling of his or her personal information before this Act is enforced, and where the consent is equivalent to the consent that allows the personal data to be provided to third parties under Paragraph 1 of Article 23, then it shall be deemed that there is such consent as is prescribed in the same paragraph.

(Transition Measures Concerning Notices)

Article 4 of the Supplementary Provisions of the Act

If an individual has been notified, before this Act is enforced, of the matters that shall be notified to the individual or be put in a readily accessible condition for the individual under Paragraph 2 of Article 23, then it shall be deemed that the notice concerned has been given under the provision of the same paragraph.

Article 5 of the Supplementary Provisions of the Act

If an individual has been notified, before this Act is enforced, of the matters that shall be notified to the individual or be put in a readily accessible condition for the individual under Item 3 of Paragraph 4 of Article 23, then it shall be deemed that the notice concerned has been given under the provision of the same paragraph.

Even though the "consent of the person" in 2-2-1. (3), 2-2-1. (4), and 2-2-4. (1) Was obtained prior to enforcement of this Act, it shall be deemed that there was such consent as was based on the Act.

Also even though the "notify the person" in 2-2-4. (2) and 2-2-4. (3) (iii) was performed prior to enforcement of this Act, it shall be deemed that the person was notified in accordance with the Act.

Meanwhile, regarding the personal data that had been retained before the Act was enforced, as no action was made to acquire personal information at the time of the enforcement of the Act, the provision of Article 18 of the Act (Notice of the Purpose of Utilization at the time of acquisition, etc.) does not apply (refer to 2-2-2. (2)). However, regarding the familiarization of the person with matters concerning retained personal data, measures stipulated in Paragraph 1 of Article 24 of the Act need to be taken at the time of the enforcement of the Act (refer to 2-2-5-1.(1)).

2-3 Handling of Personal Information in Research Institutions Attached to Private Organizations, etc.

Item 3 of Paragraph 1 of Article 50 of the Act

With respect to entities handling personal information, being the entities enumerated in each of the items below, if all or part of the purpose of handling personal information is a purpose respectively prescribed in each of the items, the provisions of the preceding chapter shall not be applied.

(3) Colleges, universities, other institutions or organizations engaged in academic studies, or entities belonging to them: The purpose for academic studies

There is a case that the personal information is handled even in the research activities of a research institution attached to a private organization, etc. When the main purpose of the institution concerned is for academic studies and when the purpose of its activities concerned is to be used for academic studies, the Act is not applied to the institution pursuant to Item 3 of Paragraph 1 of Article 50 of the Act. Therefore, with respect to institutions, which perform research activities including the handling of personal information, attached to private organizations, etc. in economic and industrial sectors, the idea of Item 3 of Paragraph 1 of Article 50 of the Act is made clear as follows.

A private company's research institution, etc. that is just aiming at product development, even though such an institution has the name of "XX Institute", does not correspond to "institutions engaged in academic studies" prescribed by the Act because the research institution concerned

can not be deemed to conduct activities, the main purpose of which is academic studies.

* Idea of Item 3 of Paragraph 1 of Article 50 of the Act

The "colleges, universities, or other institutions engaged in academic studies" stipulated in Item 3 of Paragraph 1 of Article 50 of the Act are the institutions that have academic studies (discovery of new laws and principles, establishment of analysis and methodology, systematization of new knowledge and methods to apply it, and development of up-to-date academic fields, etc.) for their main purpose.

When all or part of the purpose of handling personal information in such institutions is a purpose to be used for academic studies, the duties of entities handling personal information are not imposed on the institutions concerned.

[Case in which the application of the Act is exempted]

Case When all or part of the purpose of using personal information in an institution attached to an organization that has academic studies for its main purpose is for academic studies

[Cases in which the application of the Act is not exempted]

Case 1 When the purpose of using personal information in an institution attached to an organization that has academic studies for its main purpose is only for the analysis of information on product development (not including the purpose for academic studies)

Case 2 An institution attached to an organization that has no academic studies for its main purpose

3. Policies about "Recommendations", "Orders", and "Urgent Orders"

Paragraph 1 of Article 34 of the Act

When an entity handling personal information has violated any of the provisions of Article 16 to Article 18, Article 20 to Article 27, or Paragraph 2 of Article 30, the competent Minister may recommend that the entity handling personal information concerned cease the violation concerned and take other necessary measures to correct the violation if a competent Minister considers it necessary for protecting the rights and interests of individuals.

Paragraph 2 of Article 34 of the Act

Where an entity handling personal information having received a recommendation under the provision of the preceding paragraph does not take the recommended measures without justifiable reason, and where the competent minister considers that the infringement on the important rights and interests of individuals is imminent, the competent minister may order the entity handling personal information concerned to take the recommended measures.

Paragraph 3 of Article 34 of the Act

Notwithstanding the provisions of the preceding two paragraphs, where an entity handling personal information has violated any of the provisions of Article 16, Article 17, Articles 20 to 22, or Paragraph 1 of Article 23, and where the competent minister considers it necessary to take measures urgently as there is the fact of infringement of the important rights and interests of individuals, the competent minister may order the entity handling personal information concerned to cease the violation concerned and take other necessary measures to redress the violation.

Article 56 of the Act

An entity who violates orders issued under Paragraph 2 or 3 of Article 34 shall be sentenced to imprisonment of not more than six months or to a fine of not more than 300,000 yen.

Paragraph 1 of Article 58 of the Act

If any representative of a corporation (which includes an unincorporated organization with a specified representative or manager; this applies hereinafter in this paragraph), or any agent, employee or other workers of a corporation or of an individual commits any of the violations prescribed in the preceding two articles concerning the business of the corporation or individual, then not only shall the performer be punished but also the corporation or individual shall be sentenced to the fine prescribed in the corresponding article.

Paragraph 2 of Article 58 of the Act

When the provision of the preceding paragraph applies to an unincorporated organization, its representative or manager shall represent the unincorporated organization in its acts of lawsuits, and the provisions of the laws concerning criminal suits in which a corporation is a defendant or suspect shall be apply mutatis mutandis.

The Minister of Economy, Trade and Industry's "recommendation (Paragraph 1)", "order (Paragraph 2)", and "urgent order (Paragraph 3)" stipulated in Article 34 of the Act shall be issued after judging whether the entity handling personal information took necessary measures, etc. in accordance with the Guidelines or not.

That is, the noncompliance with the provisions that contain the term "must" in the Guidelines can be deemed a violation of the provisions of Article 16 to 18, Article 20 to 27, or Paragraph 2 of Article 30 of the Act. When it is judged that a violation was committed and when it is found necessary for the protechon of the rights and interests of individuals, a "recommendation" is actually made. On the other hand, although noncompliance with the provisions which contain the term "preferable" in the Guidelines can not be deemed to violate the provisions of Article 16 to 18, Article 20 to 27, or Paragraph 2 of Article 30 of the Act, the entity handling personal information is desired to make efforts as far as possible for observing even such provisions from the viewpoint of promoting protection of personal information.

An "order" is not issued just due to the noncompliance with a "recommendation" but is limited to a case where it is found that the serious infringement of the rights and interests of individuals is imminent when the entity handling personal information did not take the

measures concerning the recommendation without justifiable ground. Meanwhile, in order to clarify whether the entity handling personal information complied with a "recommendation" or not, the Minister of Economy, Trade and Industry shall set a period during which the measures concerning the "recommendation" should be taken and then issue the "recommendation".

An "urgent order" is issued without any preceding "recommendation" where an entity handling personal information has violated any of the provisions of Article 16, Article 17, Article 20 to 22, or Paragraph 1 of Article 23 and when it is found necessary to take measures urgently as there is the fact of serious infringement of the rights and interests of individuals.

Meanwhile, in order to clarify whether an entity handling personal information complied with an "order" and "urgent order" or not, the Minister of Economy, Trade and Industry shall set a period during which the measures concerning the "order" and "urgent order" should be taken and then issue the "order" and "urgent order". Where the measures were not taken during the period concerned, the "penal provisions (Article 56 and 58 of the Act)" shall be applied.

4. Review of Guidelines

The society's attitude to the protection of personal information may differ according to the change in social condition and public awareness as well as the advancement of technology, etc. It shall be tried to conduct a review of the Guidelines every year based on the change of various environments such as the condition after the enforcement of the Act.

5. Matters and Standards as Useful References for Entities Handling Personal Information to Perform Appropriately and Effectively Their Duties

It is preferable that an entity handling personal information establishes, implements, maintains, and improves the management system for the protection of personal information, depending on its operation size and activities.

Meanwhile, an entity handling personal information can refer to the following matters and standards, respectively: the JISQ15001 "Personal information protection management systems - Requirements" of the Japan Industrial Standards when preparing such a system; the JISX5070 "Security techniques - Evaluation criteria for IT security" of the Japan Industrial Standards, the JISQ27001 "Information technology - Security techniques - Information security management system - Requirements" of the Japan Industrial Standards, the JISQ27002 "Information technology - Security techniques - Code of practice for information security management" of the Japan Industrial Standards, the "E-Government Recommended Ciphers List" of the CRYPTREC (Cryptography Research and Evaluation Committees), and the ISO/IEC18033 (international standards of encryption algorithms), etc. when implementing the security control measures for personal data; and the "Information Security Audit System" of the Ministry of Economy, Trade and Industry when confirming the status of implementation of the security control measures for personal data.

Also an entity handling personal information is desired to create, by using the matters listed in the following items as references, a "statement on the policy or principle concerning the protection of personal information (so-called privacy policy or privacy statement, etc.)" and

publicly disclose this such as by displaying it on the business operator's website or place it where it can be seen easily in the business operator's store.

1) Matters concerning the proper handling of personal information in consideration of the nature and size of business

(A) Purpose of Utilization of personal information to be acquired (relating to Article 18 of the Act)

(B) <Case of provision to a third party without the consent of the person> (relating to Paragraph 2 and 3 of Article 23 of the Act)

- The fact that the provision to a third party is included in the Purpose of Utilization
- Items of the personal data to be provided to a third party
- Means or methods of provision to a third party
- The fact that the provision to a third party will be discontinued at the request of the person

(C) <Case of joint use> (relating to Paragraph 4 and 5 of Article 23 of the Act)

- The fact that personal data is used jointly between specific individuals or entities
- Items of the personal data to be used jointly
- Scope of the joint users
- Joint users' Purpose of Utilization
- Name of the individual or entity among joint users responsible for the management of personal data

(D) Matters concerning retained personal data listed in the following items (relating to Article 24 of the Act)

- Name of the business operator itself
- Purpose of Utilization of all retained personal data
- Procedures to meet "requests for disclosure and others" (only when procedures were established)
- Amount of charges regarding the notice of the Purpose of Utilization of retained personal data and the disclosure of retained personal data (only when charges were set)

- Place where a complaint is lodged (If the business operator itself is a target entity of an authorized personal information protection organization*, the name of the authorized personal information protection organization concerned and the place where settlement of the complaint is lodged are included.)

(E) Matters concerning procedures to meet requests for disclosure and others (relating to Article 29 of the Act)

- Format of an application form (only when format was determined)
- Procedures for receiving requests (only when procedures were determined)
- Provision of the information contributing to the identification of retained personal data

(F) Matters concerning a counter that receives inquiries and complaints (relating to Paragraph 5 Article 23, Paragraph 1 of Article 24, Paragraph 1 of Article 29, and Article 31 of the Act)

2) To comply with the Act on the Protection of Personal Information

3) Matters concerning the security control measures for personal information

4) Matters concerning the continued improvement of management system

* The phrase “a target entity of an authorized personal information protection organization” means an entity handling personal information that is a member (affiliated company) of an authorized personal information protection organization or a business operator, etc. that is under the contractual relationship, etc., in which an authorized personal information protection organization performs the complaints processing service and others, with the organization concerned.

In addition to the typical case examples described in the Guidelines, more concrete case examples will be shown in the “Questions and Answers about Personal Information Protection Guidelines, etc.” However, the case examples in the Questions and Answers do not aim to cover all case examples, and practically an examination is necessary in each individual case.

The Questions and Answers are displayed on the page of “Personal Information Protection” in the website of the Ministry of Economy, Trade and Industry and are planned to be updated as needed.

(The page of “Personal Information Protection” in the website of the Ministry of Economy, Trade and Industry)

http://www.meti.go.jp/policy/it_policy/privacy/index.html

Annex

Handling of Personal Information Including Credit Card Information

When the personal information including credit card information such as card number and expiration date (hereinafter referred to as "credit card information, etc.") was leaked, there is a high likelihood that such secondary damage as spoofing purchase by the wrongful use of credit card information, etc. happens. Therefore, it is preferable that in addition to a credit card company, a business operator conducting sales, etc. using payment by credit card, a business operator performing service which concerns sales, etc. using payment by credit card, and a business operator who is trusted to perform the operation with the handling of credit card information, etc. by the above business operators (hereinafter referred to as "credit sales-related business operator and others") take measures specially listed in the following items as the security control measures for credit card information, etc.

Also, it is preferable that even a business operator, who has a total number of specific individuals identified by personal information that makes up personal information databases, etc. not exceeding 5,000 on every single day in the last six months, complies with the matters prescribed by the Guidelines including to take measures listed in the following items from the viewpoint of protecting credit card information, etc. if the business operator is a credit sales-related business operator and others.

Meanwhile, if there are any provisions regarding credit card companies in the "Guidelines for the Protection of Personal Information in Credit Sector among Industrial Sectors (Announcement No. 436 of 2004 by the Ministry of Economy, Trade and Industry)", a credit card company may follow the case examples of those Guidelines.

1) Implementing the security control measures, which are preferable to be specially taken, for credit card information, etc.

2) Concluding an agreement containing the provisions regarding the protection of credit card information, etc.

3) Notifying or publicly announcing the name of party to which credit card information, etc. is provided when directly acquiring credit card information, etc.

[Exemplifications of the means which are preferable to be taken for the practice of each item of above matters]

1) Implementing the security control measures, which are preferable to be specially taken, for credit card information, etc.

   - Regarding credit card information, etc., to set storage period within the minimum extent necessary for the achievement of Purpose of Utilization, to limit the place for storage, and to destroy properly and immediately after the expiration of storage period

   - To hide a part of credit card number printed in a credit sales slip

   - To implement the measures for the prevention of leakage of credit card information, etc. from credit card reading terminals (for instance, to set the security function

(measures for the prevention of leakage, etc.) for the prevention of skimming on credit card reading terminals, etc.)

- To adopt the best technical method when transferring or transmitting credit card information, etc.

- To implement the monitoring such as access monitoring when allowing another credit sales-related business operator and others to access a personal information database, etc. that contains credit card information, etc.

2) Concluding an agreement containing the provisions regarding the protection of credit card information, etc.

- To stipulate provisions regarding the protection of credit card information, etc. (for instance, to stipulate provisions that request to provide information from the viewpoint of protecting credit card information, etc. and provisions that request to redress the operation of the handling of the information concerned or to terminate the agreement about the operation concerned where it is found that the handling of credit card information, etc. is improper,) when concluding an agreement about the operation of the handling of credit card information, etc.

3) Notifying or publicly announcing the name of party to which credit card information, etc. is provided when directly acquiring credit card information, etc.

- When acquiring credit card information, etc. directly from the person such as acquiring credit card information, etc. directly from the person in Internet transaction, to notify the person of the name of the acquirer, the name of providee, and the storage period, etc. of credit card information, etc. or publicly announce them in addition to expressly showing or notifying the person of the Purpose of Utilization or publicly announcing it in accordance with Paragraphs of Article 18 of the Act