

Guidelines on Law Protecting Personal Information in
Economic Industry Sector

October 2004

Ministry of Economy, Trade and Industry

Contents

A. Aim and Scope of Application 1

B. Guidelines on Interpretation of Ordinance/Examples 2

1. Definitions (Article 2) 2

 (1) **Personal Information (Paragraph 1, Article 2)** 2

 (2) **Personal information databases, etc. (Paragraph 2, Article 2)**..... 3

 (3) **Entity handling personal information (Paragraph 3, Article 2)**..... 5

 (4) **Personal data (Paragraph 4, Article 2)** 7

 (5) **Handled personal information (Paragraph 5, Article 2)**..... 8

 (6) **Data subject (Paragraph 6, Article 2)** 10

 (7) **Notification to data subject** 10

 (8) **Disclosure**..... 10

 (9) **“Disclosing purpose of use to the data subject”**..... 11

 (10) **Consent of data subject**..... 12

 (11) **Information is easily accessible to data subject**..... 13

 (12) **“Information is easily accessible to the data subject (including instances in which response is made to demand by the data subject without delay)”**..... 14

 (13) **Provision** 14

2. Duties of entity handling personal information, etc. 15

 (1) **Purpose of use of personal information (Articles 5 to 16)** 15

(2)	Acquisition of personal information (Articles 17 and 18)	20
(3)	Management of personal data (Articles 19 to 22)	25
1)	Ensuring accuracy of data details (Article 19)	25
2)	Safety management measures (Article 20)	25
3)	Supervision of employees (Article 21)	37
4)	Supervision of consignee (Article 22)	38
(4)	Provision to third party (Article 23)	39
(5)	Disclosure of items on handled personal information, disclosure, correction, cessation, etc. of handled personal information (Articles 24 to 30)	46
1)	Disclosure of items on handled personal information (Article 24)	46
2)	Disclosure of handled personal information (Article 25)	50
3)	Correction of handled personal information, etc. (Article 26)	52
4)	Cessation of handled personal information (Article 27)	53
5)	Explanation of reason (Article 28)	54
6)	Procedure implemented in response to demand for disclosure, etc. (Article 29)	55
7)	Handling Charges (Article 30)	58
(6)	Handling of grievances (Article 31)	58
(7)	Transitory Action (Articles 2-5 of Miscellaneous Rules in the Law)	60
3.	Handling of Personal Information at Research Institutes, Etc., of Private Organizations	62
C.	Principles of "recommendation," "order" and "emergency order"	63

D. Review of Guidelines	64
E. Reference Items and Standards in Appropriate and Effective Execution of Obligations, etc., by Entities Handling Personal Information	66

(Enquiries)
Information Economy Division,
Commerce and Information Policy Bureau,
Ministry of Economy, Trade and Industry

Telephone : 03-3501-0397 (Direct)

A. Aim and Scope of Application

This Guidelines sets down requirements related to items prescribed in Article 8 of the Law Protecting Personal Information (Law 57 2003, hereafter referred to as the Law) based on the “Basic Guidelines on Protection of Personal Information” passed by the diet on April 2, 2004 based on Article 7-1 of the Law, and also sets down specific principles supporting activities related to ensuring appropriate handling of personal information by entities in specific fields overseen by Ministry of Economy, Trade and Industry (METI) and fields (hereafter referred to as “economic industry sector”) in which the Minister of Economy, Trade and Industry is designated as the competent minister Article 36-1.

This Guidelines serves as the standards for the Minister of Economy, Trade and Industry to implement the Law. However, consideration was given to consistency with principles related to measures which entities must devise to ensure appropriate handling of personal information on employment management (2004 Ministry of Health, Labour and Welfare Notice 259) for sections on the personal information of employees (information related to employment management). Consequently, such sections in this Guidelines shall be created and enforced jointly by the Minister of Health, Labour and Welfare and Minister of Economy, Trade and Industry.

In this Guidelines, provisions described as “must” indicate that if these provisions are not observed, such act may be regarded as violation of law by the Minister of Economy, Trade and Industry. On the other hand, provisions described as “recommended” indicate that if the provisions are not observed, such act shall not be deemed violation of law (see III.). However, efforts should be made to observed these provisions where possible taking into account that personal information should be handled carefully based on the policy of giving respect to individuality, the basic principle of the Law prescribing appropriate handling of personal information (Article 3), and the promotion of protecting personal information. Activities required for public interest and legitimate business activities however shall not be limited in view of the objectives of the Law (Article 1) which aim at giving consideration to the availability of personal information in the protection of personal information.

Sections described as “Examples” in this Guidelines are intended to aid understanding. Typical examples are indicated for relevant and irrelevant examples, and these do not aim to cover all cases. In reality, there is a need to review each individual case. In addition, it should be noted that though examples of different business sectors are taken up, not all business sectors are covered.

Moreover, for the economic industry sector, in the event of the need to specially ensure appropriate handling of personal information based on the nature of the personal information, using method or specificity of the business circumstance, the Minister of Economy, Trade and Industry may devise further measures separately. Authorized personal information protection organizations (organizations authorized based on Article 37-1 of the Law, hereafter the same)

may also devise personal information protection guidelines specified in Article 43-1 of the Law. In such cases, there is a need for the concerned handling of personal information to observe the corresponding further measures and personal information protection guidelines.

Furthermore, trade associations, etc. may also, based on the actual situation of the concerned business, draw up or revise trade association guidelines, which are voluntary rules intended for companies affiliated with the associations.

B. Guidelines on Interpretation of Ordinance/Examples

1. Definitions (Article 2)

(1) Personal Information (Paragraph 1, Article 2)

Paragraph 1, Article 2

In this Law, “personal information” means information on a person who is alive, which can identify a certain individual by the description of name, date of birth, etc. included in the said information (includes information which can be easily compared with other information to identify that particular individual).

“Personal information”(#1) means “information on an individual who is alive”, and information which can identify a particular person (includes information which can be easily compared with other information to identify that particular individual (#2)). “Information on an individual” is not limited to information which can identify individuals such as name, gender, and date of birth, but all information representing facts, decisions, and evaluations related to attributes such as personal physique, assets, occupation, title, etc. It also includes evaluation information, information disclosed by public literature, etc., visual or audio information whether it be encoded or not.

If information on the deceased is also information on a living person such as surviving family members, it shall be information related to the concerned living individual.

“Individual who is alive” is not limited to Japanese nationals but includes foreigners as well. However, incorporated entities and other organizations are not considered as “individuals”, and are therefore not included in information related to the organization itself such as incorporated entities (however, information on executives and employees, etc. is personal information).

#1 This Law differentiates the use of the terms “personal information”, “(4) personal data”, and “(5) handled personal information”. Note that the duties imposed on entity handling personal information differ for each.

#2“Can be easily compared with other information” means for instance the state of being able

to access personal information database, etc. in the normal work framework for comparison. It excludes states in which comparison is difficult such as when as the need to enquire other entities, or when handling departments differ within the entity.

<Examples of personal information>

Example 1) Name of subject

Example 2) Date of birth, contact (address, replace of residence, telephone number, mail address), title and department at work, etc. Also information which combines these information and name of the data subject.

Example 3) Visual information with which the data subject such as information recorded on security camera can be identified

Example 4) Mail address information which can identify a certain individual (for example, even for information consisting of mail address such as keizai_ichiro@meti.go.jp only, the information indicates that it is the mail address of Keizai Ichiro belonging to the Ministry of Economy, Trade and Industry, a Japan government organization)

Example 5) Even if information which can identify a specific individual is not described, information which can identify a specific individual by identifying with common information

Example 6) Employment management information (including information for companies to evaluate their employees.)

Example 7) Information related to individuals added to individual information after acquisition (even if a living specific individual could not be identified at acquisition, if after acquisition, the living specific individual can be identified as a result of the addition of new information or comparison, the information will become personal information at that point.)

Example 8) Information disclosed in government newspaper, telephone directory, directory of government officials (name of data subject, etc.)

<Examples of non personal information>

Example 1) Information related to organizations such as incorporated entities, for example financial information of companies (organization information)

Example 2) Mail address information which does not indicate whether the information is information of a specific individual merely from the character strings of symbols, numerals, etc. (For example, abc012345@ispisp.jp. However, information which can identify a specific individual by easy comparison with other information is considered personal information.)

Example 3) Statistics information which cannot identify a specific individual

(2) Personal information databases, etc. (Paragraph 2, Article 2)

<u>Paragraph 2, Article 2</u>

In this Law, “personal information database, etc.” is the aggregate of information including personal information and indicates the following.

1. Systematic structure which can search for specific personal information using computers
2. Apart from the above, systematic structure designated by ordinance so that specific personal information can be searched easily

Law Enforcement Ordinance Related to Protection of Personal Information (2003 Ordinance No. 507. Hereafter referred to “Ordinance”.) Paragraph 1

The personal information database designated in Item 2, Paragraph 2, Article 2 is an aggregate of information systematically structured so that specific personal information can be easily searched by organizing the personal information according to certain rules, and has a table of content, glossary, etc. to facilitate search.

“Personal information database, etc.” are aggregates of information including personal information systematically structured so that specific personal information can be searched using computers, or if computers are not used, personal information processed on paper such as medical charts and student records are organized and sorted according to certain rules (for example, alphabetical order, chronological order, etc.), and to facilitate search of specific personal information, table of contents, glossaries, codes, etc. are added so that information can be searched by others easily.

<Examples of personal information database, etc.>

Example 1) Mail address book stored on e-mail software (if information combining mail address and name are entered)

Example 2) Electronic files storing user ID and log information on transactions used by the user (if user ID is managed related to personal information)

Example 3) When employees enter namecard information using table calculation software of PCs for business (owner irrelevant) and sort the information so that it can be searched by other employees, etc. as well

Example 4) When staffing firms sort registration cards according to the alphabetical order of names, add alphabetical order indices and file the information

Example 5) Commercially available who’s who directory sorted by name, address, and company

<Examples of non personal information databases, etc.>

Example 1) When employees enable others to freely search their namecards, but sort these namecards using their own unique categorization method disabling others to search for information easily

Example 2) When returned questionnaire postcards are not sorted according to name, address, etc.

(3) Entity handling personal information (Paragraph 3, Article 2)

Paragraph 3

In this Lawt, “entity handling personal information” means someone providing personal information databases, etc, for business use. However, the following are excluded.

- 1 National organizations
- 2 Local public entities
- 3 Independent administrative agency, etc. (Law on Protection of Personal Information Owned by Independent Administrative Agencies, etc. (2003 Law No. 59)) Independent administrative agencies, etc. prescribed in Paragraph 1, Article 2. Hereafter the same.)
- 4 Local independent administrative agency, etc. (Law on Local Independent Administrative Agency (2003 Law No. 118)) Local independent administrative agencies, etc. prescribed in Paragraph 1, Article 2. Hereafter the same.)
- 5 Entities designated by ordinance as posing little risks of infringing the rights and interests of individuals based on the volume of handled personal information and method of use

Ordinance Article 2

Entities designated by Ordinance in Item 5, Paragraph 3, Article 2 are entities whose total number of specific individuals which can be identified by personal information making up personal information databases, etc. for business purpose does not exceed 5,000 on any day within the past six months (when the whole or part of the concerned personal information database, etc. includes the name or address or place of residence (including display of address or place of residence on maps or computer screen) or telephone number only as personal information in personal information databases constructed by others . When this can be provided for use in the business without the need for editing or processing this, the number of specific individuals identified by personal information making up part or whole of the concerned personal information database, etc.)

“entity handling personal information” means entities providing personal information databases, etc. for business use excluding independent administrative agencies, etc, designated by the Law Protecting Personal Information owned by national organizations, local public organs, and independent administrative agencies, etc. (2003 Law No. 59), local independent administrative agencies designated by the Law on Local Independent Administrative Agencies, etc. (2003 Law No. 118), and entities posing little risks of infringing personal rights and interests based on the volume of handled personal information and method of use.

“entities posing little risks of harming personal rights and interests based on the volume of handled personal information and method of use” here means designated by Ordinance Article 2 as being entities whose total number of specific individuals which can be identified by

personal information making up personal information databases, etc. provided for business purpose does not exceed 5000 on any day within the past six months. Whether the total number exceeds 5,000 or not is determined by the sum of specific individuals identified according to personal information constructing all personal information databases, etc. managed by the concerned entity. However, this does not apply to overlapping portions of the same person. “provided for business use” here means the same type of action carried out repeatedly and continuously for a certain purpose, which at the same time is recognized as a business according to common sense. It is not limited to profit-making business.

Associations (arbitrary organizations) and individuals without corporate status nor right capacity are also considered as entity handling personal information.

“Number of specific individuals”

When the personal information database, etc. meets all the following requirements, the number of specific individuals identified by personal information making up the personal information database, etc. is not included in the above “number of specific individuals”.

- (1) The personal information database, etc. was created by someone else in whole or in part
- (2) The personal information making up the personal information database, etc. includes name, address (including place of residence, and including display of address or whereabouts on maps or computer screen), or telephone number.
- (3) In the provision of the personal information database, etc., the database, etc. shall not be changed by adding new personal information, increasing the identified specific individuals, adding other personal information, etc.

<Examples of not including in the number of specific individuals>

Example 1) Name and telephone number listed in telephone directories provided by telephone companies, listed on commercially available telephone directory CD-ROM, etc.

Example 2) Name, address or data indicating location of whereabouts stored in navigation systems such as commercially available car navigation systems. (Even if new information, etc. such as route, etc. is recorded using functions equipped in the car navigation system ,etc. from the beginning, it shall not be included in the “number of specific individuals”.)

Example 3) Name and address or information indicating location of whereabouts on conventionally available address maps systematically structured to allow search from name or address.

<Examples of not including in the number of specific individuals because not provided for business>

Example) In warehousing and data center (housing, hosting), etc. businesses, if information is kept without perceiving if it corresponds to personal information, personal information included in that information

<Examples of entity handling personal information>

Example) Entities whose sum of specific individuals identified by personal information constructing personal information of electronic media and paper media (hereafter called “media”) exceeds 5,000.

(4) Personal data (Paragraph 4, Article 2)

Paragraph 2, Article 2

In this Law, “personal data” means personal information constructing the personal information database, etc.

“Personal data”(＃) is personal information constructing the “personal information database, etc.” managed by the entity handling personal information.

This Law differentiates the use of the terms “personal information”, “(4) personal data”, and “(5) handled personal information”. Note that the duties imposed on entity handling personal information differ for each.

<Examples of personal data>

Example 1) Personal information for backup saved from the personal information database, etc. to other media

Example 2) Personal information printed on ledgers etc. output from the personal information database, etc. by computer processing

<Examples of non personal data>

Example) Personal information indicated on input ledgers prior to the construction of personal information database, etc.

Handling of telephone directory, car navigation system, etc.

Even if the personal information database, etc. meets all the following requirements, it cannot be denied that the personal information constructing the personal information database, etc. may be personal data. However, as there are little risks of it infringing the rights and interests of individuals based on how it is used, it is interpreted that the duties of entity handling personal information (2. Duties of entity handling personal information) shall not be imposed.

(1) The personal information database, etc. was created by someone else in whole or in part.

(2) The personal information constructing the personal information database, etc. includes name, address (including whereabouts, and including display of address or whereabouts on

maps or computer screen), or telephone number.

(3) In the provision of the personal information database, etc., the database, etc. shall not be changed by adding new personal information, increasing the identified specific individuals, adding other personal information, etc.

(5) Handled personal information (Paragraph 5, Article 2)

Paragraph 5, Article 2

In this Law, “handled personal information” means personal data for which the entity handling personal information is authorized to disclose, revise contents, add or delete, stop use, and erase the data as well as stop providing it to a third party. It excludes information designated by ordinance as data will infringe public benefit and other interests if its existence is brought to light, and information erased within the period of less than one year designated by ordinance.

Ordinance Article 3

Personal data designated by the ordinance of Paragraph 5, Article 2 is as follows.

1. Personal data with risks of causing life-threatening, physical or asset damage to the data subject or a third party if its existence is brought to light
2. Personal data with risks of promoting or inducing illegal or illegitimate acts if its existence is brought to light
3. Personal data with risks of harming national safety, risks of harming trustful relations with other countries or international organizations, or risks of incurring disbenefits in negotiations with other countries or international organizations if its existence is brought to light
4. Personal data with risks of disrupting public safety such as prevention of crime, repression and investigation and maintenance of order if its existence is brought to light

Ordinance Article 4

The period designated by ordinance of Paragraph 5, Article 2 is 6 months.

“handled personal information”(#1) means personal data (#2) for which the entity handling personal information is authorized to respond to all requests from the data subject or its proxy to disclose, revise contents, add or delete, stop use, erase the data as well as stop providing it to a third party. It excludes information designated by ordinance as data will damage public benefit and other interests if its existence is brought to light, and information erased within the period of less than one year designated by ordinance.

#1 This Law differentiates the use of the terms “personal information”, “(4) personal data”, and “(5) handled personal information”. Note that the duties imposed on entity handling personal information differ for each.

#2 If the entity handling personal information has been commissioned to process the personal data, and is unable to disclose the data to the data subject based on its own decision in the absence of any arrangements, the consignor not the consignee has the authority to disclose

the data to the data subject.

However, the following are not considered “handled personal information”:

- (1) Personal information which will harm public benefits and other interests if its existence is brought to light (#3).
- (2) Personal information to be erased within six months (excluding updates).

#3 “infringe public benefits and other interests if its existence is brought to light” means the following.

i. Personal data with risks of causing life-threatening, physical or asset damage to the data subject or third party if its existence is brought to light.

Example) If an organization supporting victims of domestic violence, child abuse, etc. has personal data taking the victimizer (spouse or parent) and victim (spouse or child) as the data subject

ii. Personal data with risks of promoting or inducing illegal or illegitimate acts if its existence is brought to light.

Example 1) If an entity has personal data taking corporate extortionist, etc. as the data subject to prevent undue claims from the corporate extortionist, etc.

Example 2) If an entity has personal data taking as the data subject parties repeating undue claim acts from the so-called suspicious individuals and malicious claimers to prevent these acts from them.

iii. Personal data with risks of impairing national safety, risks of impairing trustful relations with other countries or international organizations, or risks of incurring disbenefits in negotiations with other countries or international organizations if its existence is brought to light

Example 1) If a manufacturer, information service provider, etc. has personal data recording the design and name of developer of defense related weapons, facilities, equipment, software, etc.

Example 2) If the security company of a VIP has schedules and records taking the VIP as the data subject

ix. Personal data with risks of disrupting public safety such as prevention of crime, repression and investigation and maintenance of order if its existence is brought to light

Example) If an entity subject to the investigation related case enquiry by the police or search warrant has personal data taking subjects of the search or suspects as the data subject in the process

(6) Data subject (Paragraph 6, Article 2)

Paragraph 6, Article 2

In this Law, the “data subject” of personal information is a specific individual identified by the personal information.

(7) Notification to data subject

Paragraph 1, Article 18

If an entity handling personal information has acquired personal information, it must promptly notify or disclose to the data subject the purpose of use of the personal information, unless it has disclosed the purpose of use beforehand.

Other details are described in Items 1 to 3, Paragraphs 3 and 4, Article 18, etc.

“Notification to the data subject” means informing the data subject directly. It must be carried out by a reasonable and appropriate method allowing the data subject to perceive the contents, in accordance with the nature of the business operation involved, and conditions in which personal information is handled.

<Examples of notification to the data subject>

Example 1) Informing orally or handing documents such as catalogues, etc. during interviews

Example 2) Informing orally or by automatic answering machine on the telephone

Example 3) Informing by sending e-mails, fax, etc. or sending documents by postal mail between distance parties

Example 4) Oral method during telephone solicitation

Example 5) Sending information by automatic response e-mail for verifying transaction in e-commerce

(8) Disclosure

Paragraph 1, Article 18

If an entity handling personal information has acquired personal information, it must promptly notify or disclose to the data subject the purpose of use of the personal information, unless it has disclosed the purpose of use beforehand.

Other details are described in Items 1 to 3, Paragraphs 3 and 4, Article 18, etc.

“Disclosure” means informing one’s will widely to the public (announcing to the public in general and unspecified majority). However, announcement must be done by a reasonable and appropriate method in accordance with the nature of the business operation involved, and conditions in which personal information is handled.

<Examples of disclosure>

Example 1) Placing the information at a location of one's company homepage which can be accessed from the top page of the homepage by just one operation, posters put up at company stores and offices, distributing pamphlets, etc.

Example 2) In stores, putting up at clearly visible locations

Example 3) In mail order sales, placing information in pamphlets for mail order sales

(9) **"Disclosing purpose of use to the data subject"**

Paragraph 2, Article 18

Regardless of the provisions in the preceding paragraph, the entity handling personal information must disclose the purpose of use to the data subject beforehand when acquiring personal information of the concerned data subject indicated in contracts and other documents (including records produced electronically, magnetically, or with any other method in which data cannot be recognized by the human senses, likewise for the foregoing paragraph) signed when entering an agreement with the data subject, when acquiring personal information of the concerned data subject indicated in writing directly from the data subject. However, this does not apply when requiring the information urgently for the protection of lives, and physical and asset protection.

"Disclosing purpose of use to the data subject" means clearly stating the purpose of use to the data subject. Disclosure must be done by a reasonable and appropriate method which allows the data subject to perceive the details in accordance with the nature of the business operation involved, and conditions in which personal information is handled.

<Examples of disclosing purpose of use>

Example 1) Handing over by hand or sending to the data subject contracts or other documents indicating the purpose of use (documents of contract clauses or conditions of use, etc. (including records produced electronically, magnetically, or with any other method in which data cannot be recognized by the human senses). If the document describes articles on the purpose of use, for example, there is a need for the data subject to be able to actually see the purpose of use by conveying to the data subject that the purpose of use is indicated in the clauses at the back, or indicate articles on the purpose of use indicated at the back in front)

Example 2) On the network, the purpose of use should be indicated on the webpage of the company accessed by the data subject or on the data subject's terminal (when acquiring personal information on the network, the purpose of use must be positioned so that it catches the data subject's eye before the data subject clicks the send button, etc. (including links and

buttons set so that the page moves to the page showing details of the purpose of use by just one operation))

(10) Consent of data subject

Paragraph 1, Article 16

The entity handling personal information must not handle personal information exceeding the range required for achieving the purpose of use specified by the preceding article without obtaining prior consent from the data subject.

Paragraph 1, Article 23

The entity handling personal information must not provide personal data to third parties without the prior consent of the data subject excluding the following cases.

1. When based on ordinance
2. When consent of the data subject is difficult to obtain due to the need for the protection of human life, physical or asset protection
3. When there is especially a need to promote the enhancement of public health and sound growth of children during mental and physical development, but it is difficult to obtain the consent of the data subject
4. When there is a need for national organizations, local public organizations, or entities consigned by these organizations to provide support in the implementation of paperwork designated by ordinance, but there is a risk that obtaining the consent of the data subject may affect the implementation of the concerned paperwork

Other details are described in Items 2 to 4, Paragraphs 2 and 3, Article 16, etc.

The “consent of the data subject” means the indication of acceptance by the concerned data subject to the handling of the data subject’s personal information by the handling method indicated by the entity handling personal information (on the precondition that the data subject can be confirmed to be the concerned data subject).

“Obtaining the consent of the data subject” means the concerned entity handling personal information acknowledging the indication of acceptance by the data subject. This must be done by a reasonable and appropriate method deemed necessary for the data subject to make judgments related to the consent in accordance with the nature of the business operation involved, and conditions in which personal information is handled.

<Examples of obtaining the consent of the data subject>

Example 1) Confirming consent orally or in writing (including records produced electronically, magnetically, or with any other method in which data cannot be recognized by the human senses) from the data subject.

Example 2) Confirming by receiving documents such as consent application forms signed or stamped with the name of the data subject.

Example 3) Receiving mail indicating consent from the data subject.

Example 4) Checking validation spaces indicating consent from the data subject

Example 5) Clicking of the button on webpages indicating consent by the data subject

Example 6) Voice input, touching of touch panels, entering of buttons and switches to indicate consent by the data subject.

(11) Information is easily accessible to data subject

Paragraph 2, Article 23

When the entity handling personal information suspends availability to third parties of personal data which can identify the concerned data subject according to the request of the data subject, the concerned personal data can be provided to third parties regardless of the preceding paragraph if the data subject is informed beforehand, or if the information is easily accessible to the data subject.

Item 3, Paragraph 4, Article 23

In the following case, the entity receiving the concerned personal data shall not correspond to the third party in the application of the regulations of the preceding paragraph 3.

3. In the shared use of personal data between specific entities, when the data subject is notified of this, items of jointly used personal data, scope of entities using the data jointly, purpose of use of the entities using the data, name of the person responsible for the management of the concerned personal data beforehand or the if the information is easily accessible to the data subject.

Other details are described in Paragraph 3, Article 23, etc.

“Information is easily accessible to the data subject” means that when a data subject wants to know something, information is easily accessible to that data subject time-wise and method-wise, by a reasonable and appropriate method which allows the data subject to perceive the details in accordance with the nature of the business operation involved, and conditions in which personal information is handled.

<Examples of information is easily accessible to the data subject>

Example 1) Placing information continuously at a location which can be reached from the top page of a web page with just one operation

Example 2) Putting up information continuously at the counter, etc. of offices

Example 3) Periodic placement of information in periodical publications widely distributed

Example 4) In e-commerce, continuously indicating links at web pages introducing products

(12) “Information is easily accessible to the data subject (including instances in which response is made to demand by the data subject without delay)”

Paragraph 1, Article 24

The entity handling personal information must ensure that information is easily accessible to the data subject (including instances in which response is made to demand by the data subject without delay) in the following cases for handled personal information.

“Information is easily accessible to the data subject (including instances in which response is made to demand by the data subject without delay)” means that the subject must be in a state of being able to learn the accurate details of the desired information at any time by placing information on webpages, distributing pamphlets, responding to the requests of the data subject without delay, etc. Placement of information on webpages or putting up of information at counters of offices need not be done continuously, however, must be done by a reasonable and appropriate method which allows the data subject to perceive the details in accordance with the nature of the business operation involved, and conditions in which personal information is handled.

For entities who normally need to respond to many enquiries, continuous placement of information on the webpage serves as a method of meeting the purpose of both (11) “information is easily accessible to the data subject” and (12) “information is accessible to the data subject” (including instances in which response is made to demand by the data subject without delay”.

<Examples of information is accessible to the data subject>

Example 1) Set up a system which enables inquiries that come in to be responded orally or in writing by the inquiry desk.

Example 2) Put up pamphlets at stores.

Example 3) In e-commerce, clearly indicate the mail address for inquiries.

(13) Provision

Paragraph 1, Article 23

The entity handling personal information must not provide personal data to a third party without the prior consent of the data subject except in the following cases.

Other details are described in Paragraph 2, Article 23, etc.

“Provision” means exposing the personal data to a state in which it can be used. Even if the personal data is not physically provided, enabling use of personal data by using the network, etc.

(by giving authorization to use) is equivalent to “provision”.

2. Duties of entity handling personal information, etc.

(1) Purpose of use of personal information (Articles 5 to 16)

(a) Identification of purpose of use (Paragraph 1, Article 15)

Paragraph 1, Article 15

Entity handling personal information must identify the purpose of use in the handling of personal information where possible.

The entity handling personal information must identify the purpose of use where possible. In the identification of the purpose of use, the entity must identify specifically for what purpose the personal information is eventually used as much as possible at the entity instead of merely identifying the purpose of use subjectively or generally (excluding 1 . (4) #Handling of telephone directory, car navigation systems, etc.). However, this does not call for the identification of even the type of personal information used and the name of provider.

Specifically, some examples include notification of the delivery of products or new product information in XX business (#1), related after-service, etc. If compared to businesses assumed in company contracts and contribution acts, the scope of use of the personal information of a data subject is identifiable as being a degree which can be rationally anticipated as seen from the data subject identified by the personal information, or if the scope of purpose of use can be estimated by clarifying the business type, this may be considered sufficient. However, giving “business activities”, “enhancement of customer services”, etc. as the purpose of use does not pertain to “identifying specifically the purpose of use where possible”. Where provision of personal information to third parties is expected beforehand, this must be specified in the purpose of use.

The purpose of use of employment management information must also be identified specifically and individually to a degree where results of using the acquired personal information of the concerned data subject can be rationally forecasted by the data subject such as workers, etc. (workers used by the entity handling personal information, those attempting to be the workers used by the entity handling personal information, those who attempted this, and those used by the entity handling personal information previously, the same applies below) instead of merely identifying subjectively or generally.

#1 In the identification of XX business, it is ideal to identify to the scope deemed as

contributing to the identification as seen from the data subject from common sense. For instance, the intermediate to minor categories of the Japan Standard Industrial Classification may serve as a reference.

<Examples of specific identification of purpose of use>

Example 1) “Use for notifying information related to the delivery of products in XX business, related after services, and new products and services”

Example 2) “Names, addresses, and telephone numbers indicated may be sold as registers”

Example 3) For instance, in the case of providers of information processing services, “as information processing services such as wage calculation services, address printing services, slip printing and delivery services is our business, we handle consigned personal information” can be taken as the purpose of use has been identified.

<Examples of not specifically identifying purpose of use>

Example 1) “For use for business activities”

Example 2) “For enhancing services provided”

Example 3) “For use for marketing activities”

(b) Changes of purpose of use (Paragraph 2, Article 15, Paragraph 3, Article 18)

Paragraph 2, Article 15

When changing the purpose of use, the entity handling personal information must not exceed the scope rationally recognized as having considerable relation with the purpose of use before the change.

Paragraph 3, Article 18

If the purpose of use has been changed, the entity handling personal information must notify to the data subject or disclose the changed purpose of use.

The purpose of use identified above may be changed within the scope recognized as not difficult to conceive by the data subject from common sense. The changed purpose of use must be notified (#1) to the data subject or disclosed (#2).

#1 Regarding “notification of data subject”, see 1. (7).

#2 Regarding “disclosure”, see 1. (8).

*** Criteria within scope recognized as not difficult for the data subject to conceive**

Changes exceeding the scope of businesses handling personal information indicated in purpose of use cannot be implemented without prior consent from the data subject.

If typical handling methods of personal information are indicated with specificity in the purpose of use, changes can be made within the range which can be estimated from the

representative examples.

<Examples of within scope recognized as not difficult for the data subject to conceive>

Example) For the purpose of use “Information of new products and services in our XX business may be sent by e-mail”, the addition of “information may be sent by postal mail” is allowed.

(c) Restrictions by purpose of use (Paragraph 1, Article 16)

Paragraph 1, Article 16

The entity handling personal information must not handle personal information exceeding the scope required for achieving the purpose of use identified by the preceding regulation without obtaining prior consent of the data subject.

When handling personal information exceeding the scope required for achieving the purpose of use, the entity handling personal information must obtain prior consent (#1) of the data subject.

Use of personal information to obtain consent (sending e-mail, telephoning, etc.) does not pertain to use outside purpose of use even if it is not given as a purpose of use at the beginning.

#1 Regarding “consent of data subject”, see 1. (10).

<Examples requiring consent>

Example) When sending company product catalogue and purchase application form to promote sales of company products based on resume information for finding employment.

(d) Business succession (Paragraph 2, Article 16)

Paragraph 2, Article 16

When the entity handling personal information acquires personal information accompanying the succession of business from other entities handling personal information due to merges, the concerned entity must not handle the concerned personal information exceeding the range required for achieving the purpose of use of the concerned personal information without the prior consent of the data subject.

When the entity handling personal information acquires personal information accompanying the succession of business from other entities handling personal information due to merges, spinoffs into separate company, transfer of operations, etc., the handling of personal

information within the range required for achieving the purpose of use prior to the succession related to the concerned personal information does not constitute use outside the purpose of use, and does not require consent of the data subject

(e) Exemption (Paragraph 3, Article 16)

In the following cases, even if consent of the data subject is required in the above and , the requirement does not apply.

i. When based on ordinance (Item 1, Paragraph 3, Article 16)

Item 1, Paragraph 3, Article 16

The regulation of the preceding paragraph 2 does not apply to the following case.

1. When based on ordinance

Handling of personal information based on ordinance is not subject to the preceding paragraph 2.

Examples of ordinances justifying the above include Criminal Procedure Law Article 21 (Investigation by warrant), Local Tax Law Article 72-63 (existence of regulations similar to authority to inquire and inspect related to enterprise tax, and various tax laws). As these laws are binding, and response is required, these shall apply uniformly.

Example) Submission of payment records to the director of the taxation office based on Income Tax Law, Paragraph 1, Article 225.

On the other hand, the provision of personal information may be applicable even for voluntary cooperation such as Criminal Procedure Law Paragraph 2, Article 197 (investigation requiring search), etc., however, individual judgment is required.

Example 1) Response to investigations on auditor subsidiaries of parent company based on Business Law Article 274-3.

Example 2) Response to financial auditing based on Law on Exceptions of Business Law Related to Private Company Audit, Etc. Article 2, regulations of Securities Exchange Law Article 193-2.

ii. Protection of human life, physical and asset protection (Item 2, Paragraph 3, Article 16)

Item 2, Paragraph 3, Article 16

The provisions of the preceding Paragraph 2 shall not apply in the following case.

2. When there is a need for protection of human life, physical and asset protection, but it is difficult to obtain the consent of the data subject

The preceding Paragraph 2 shall not apply when there is a risk of damage to specific rights and interests in the form of human (including corporate) life or assets, and there is a need to use personal information to protect these, but it is difficult to obtain the consent of the data subject (except when protection of the concerned rights and interests is adequately possible by other methods).

Example 1) When providing the blood type, contact number of family members of the data subject in times of sudden illness and other circumstances to doctors and nurses

Example 2) When information of those intentionally interfering with business is exchanged between private companies

iii. Enhancement of public health, etc. (Item 3, Paragraph 3, Article 16)

Item 3, Paragraph 3, Article 16

The provisions of the preceding paragraph 2 shall not apply in the following cases.

3. When personal information is particularly required for enhancing public health or promoting sound growth of children during mental and physical development, but it is difficult to obtain the consent of the data subject

When personal information is particularly required for enhancing public health or promoting sound growth of children during mental and physical development, but it is difficult to obtain the consent of the data subject (except when enhancement of public health or sound growth of children are adequately possible), this does not apply

Example 1) In the health checkup conducted by insurers such as the health insurance union, etc. health business such as cancer examinations, etc. when the results of close examinations and information of the examination state are provided to researchers, etc. erasing the individual name for epidemiology studies and statistics surveys aiming to draw up health promotion policies and enhancing the business

Example 2) For problematic behavior of children such as school truancy and bad acts, as related organizations such as child counseling centers, schools, and medical work etc. work together, information on the concerned child may be exchanged between the concerned organizations

iv. Support to national organizations, etc. (Item 4, Paragraph 3, Article 16)

Item 4, Paragraph 3, Article 16

The provisions of the preceding paragraph 2 shall not apply in the following case.

4. When national organizations, or local public organizations, or those being consigned requires cooperation for implementing paperwork designated by ordinance, and there are risks that the acquisition of consent from the data subject may interfere with the implementation of the paperwork.

When national organizations require the support of private companies, etc. to implement paperwork designated by ordinance, and the acquisition of consent from the data subject is recognized as having the risk of impeding the implementation of the concerned paperwork for use of personal information outside the specified purpose of use by the cooperating private companies, etc., the provision shall not apply.

Example 1) When entities submit personal information to voluntary surveys by the employees of the tax office, etc.

Example 2) When entities submit person information according to the voluntary requirement of the police.

(2) Acquisition of personal information (Articles 17 and 18)

(a) Appropriate acquisition (Article 17)

Article 17

The entity handling personal information must not obtain personal information by lying and other illegal means.

The entity handling personal information must not obtain personal information by lying and other illegal means.

Those acquiring, using, and disclosing personal information useful for business, managed as confidential, and closed to the public for the purpose of illegal competition by fraud shall be subject to criminal punishment in accordance with the Unfair Competition Prevention Law (2003 Law 47) (imprisonment of less than 3 years or fine of below 3 million yen).

<Example of acquiring personal information by illegal means>

Example 1) When acquiring personal information from children without parent consent nor

sufficient ability to make decisions on family such as income status of parents which has not relation to the acquisition

Example 2) When acquiring personal information by force which violates third party provision restrictions prescribed in Article 23

Example 3) When instructing other entities to acquire personal information using illegal means such as 1) and 2) above, and acquiring personal information from those entities

(b) Notifying or disclosing purpose of use (Paragraph 1, Article 18)

Paragraph 1, Article 18

The entity handling personal information must notify or disclose the purpose of use of personal information promptly when it has acquired personal information, unless it has disclosed the purpose of use beforehand.

Ideally, the entity handling personal information should announce (#1) the purpose of use of personal information before acquiring it. If it has not, it should notify (#2) the data subject the purpose of use or announce it promptly after acquiring the personal information (excluding 1 .

(4) # Handling of telephone directory, car navigation systems, etc.).

Personal information owned from before this Law was enforced is not subject to the provisions of Article 18 since no personal information acquisition act is involved at the time of the enforcement of the Law. However, regarding dissemination of handled personal information related items to the data subject, there is a need to devise measures in Paragraph 1, Article at enforcement (See 5.).

#1 Regarding “disclosure”, see 1. (8).

#2 Regarding “notification of data subject”, see 1. (7).

<Examples requiring notification or disclosure to the data subject>

Example 1) When acquiring personal information which the data subject voluntarily discloses on the Internet

Example 2) When acquiring personal information from the Internet, government newspaper, directory of government officials, etc.

Example 3) When acquiring personal information which the data subject voluntarily provides in enquiries and complains over the phone, etc. (Except when acquiring personal information only for the purpose of responding to the data subject’s confirmation and enquiries.)

Example 4) When receiving personal information from a third party

(c) Acquiring directly by writing, etc. (Paragraph 2, Article 18)

Paragraph 2, Article 18

Regardless of the rule in the preceding paragraph, the entity handling personal information must disclose the purpose of use to the data subject beforehand when acquiring personal information of the concerned data subject indicated in contracts and other documents (including records produced electronically, magnetically, or with any other method in which data cannot be recognized by the human senses, likewise for the following paragraph) signed when entering an agreement with the data subject, when acquiring personal information of the concerned data subject indicated in writing directly from the data subject. However, this does not apply when requiring the information urgently for the protection of lives, and physical and asset protection.

When acquiring personal information directly from the data subject by writing on documents or entering at user input screens, the entity handling personal information must state (#) the purpose of use to the data subject beforehand. This requirements is however not imposed on the acquisition of personal information orally.

“Regarding “Disclosing purpose of use to the data subject”, see 1. (9).

<When there is a need to state the purpose of use to the data subject beforehand>

Example 1) When acquiring personal information on application forms or contracts directly from the data subject

Example 2) When acquiring personal information indicated on questionnaires directly from the data subject

Example 3) When acquiring personal information indicated on postcards applying for quizzes directly from the data subject

(d) Change in purpose of use (Paragraph 3, Article 18)

Paragraph 3, Article 18

If the entity handling personal information has changed the purpose of use, it must notify the data subject or disclose the changed purpose of use.

If the entity handling personal information changes the purpose of use within the scope recognized as being not difficult for the data subject to conceive from common sense, it must notify (#1) the data subject or disclose (#2) the changed purpose of use (See (1)).

#1 Regarding “notification of data subject”, see 1. (7).

#2 Regarding “disclosure”, see 1. (8).

(e) Exclusion of application (Paragraph 4, Article 18)

The followings are not subject to the above (b), (c), and (d).

i. Risks of infringing the rights and interests of the data subject or third party (Item 1, Paragraph 4, Article 18)

Item 1, Paragraph 4, Article 18

The provisions of the preceding paragraph 3 do not apply to the following case.

1. When the notification or disclosure of the purpose of use to the data subject poses the risks of impairing the rights and interests of the data subject or third party such as life, physical and asset damage.

The provisions of the preceding paragraph 3 do not apply when the notification or disclosure of the purpose of use to the data subject poses the risks of infringing the rights and interests of the data subject or third party such as life-threatening, physical and asset damage.

Example) When acquiring information on corporate extortionists making undue claims from third party information suppliers and exchanging information mutually, the notification or disclosure of purpose of use poses the risks of buying resentment from the extortionists, resulting in damage on the part of the third party information supplier

ii. Risks of impairing rights of concerned entity handling personal information (Item 2, Paragraph 4, Article 18)

Item 2, Paragraph 4, Article 18

The provisions of the preceding paragraph 3 do not apply to the following case.

2. When the notification or disclosure of the purpose of use to the data subject poses the risks of infringing the rights or legitimate interests of the concerned entity handling personal information.

The provisions of the preceding paragraph 3 do not apply when the notification or disclosure of the purpose of use to the data subject poses the risks of disclosing corporate secrets to other companies, thus infringing the rights or interests of the concerned entity handling personal information.

Example) When details of the notified or disclosed purpose of use discloses corporate secrets such as development details of new products by the entity handling personal information, marketing knowhow, etc.

iii. Support to national organizations, etc. (Item 3, Paragraph 4, Article 18)

Item 3, Paragraph 4, Article 18

The provisions of the preceding paragraph 3 do not apply to the following case.

3. When national organizations or local public organizations need to provide cooperation for implementing paperwork designated by ordinance, and the notification or disclosure of the purpose of use to the data subject has the risk of interfering with the implementation of the paperwork.

The provisions of the preceding paragraph 3 do not apply when national organizations, etc. require the support of private companies to implement paperwork designated by ordinance, and the notification of the purpose of use of the personal information obtained from the national organizations, etc. or disclosure by the cooperating private companies has the risks of interfering with the implementation of the concerned paperwork.

Example) When providing personal information on the accused without implementing the disclosed arrangement from the police to only the entity handling personal information whom the suspect is expected to maneuver, the notification or disclosure of the purpose of use by the concerned entity handling personal information after receiving the information from the police has the risks of causing major interference in investigations.

iv. Disclosure of using purpose (Item 4, Paragraph 4, Article 18)

Item 4, Paragraph 4, Article 18

The provisions of the preceding paragraph 3 do not apply to the following case.

4. When it is acknowledged that the purpose of use is clear from the acquisition state

The provisions of the preceding paragraph 3 do not apply when it is acknowledged that the purpose of use is clear from the acquisition state of the personal information.

Example 1) When personal information such as address and telephone number is acquired in some cases when selling/providing products/services, and the purpose of use is implementing only sales and provision of the concerned products/services

Example 2) When personal information such as name, affiliate, title, and contact number is obtained directly from the data subject in writing in the routine practice of exchanging namecards, and the purpose of use is keeping in touch in the future (however, it should be

noted that use of namecards for sending direct mail, etc. does not constitute a clear purpose of use.).

(3) Management of personal data (Articles 19 to 22)

1) Ensuring accuracy of data details (Article 19)

Article 19

The entity handling personal information must strive to maintain personal data in an accurate and latest state within the scope required for achieving the purpose of use.

The entity handling personal information must strive to maintain personal data in an accurate and latest state within the scope required for achieving the purpose of use by establishing the procedures for inquiry and verification personal information entered in the personal information database, etc., establishing the procedures for correcting errors found, updating records, setting duration of storage, etc. (excluding 1 .(4) Handling of telephone directory, car navigation systems, etc.).

In this case, there is no need for the personal data owned to be uniform or always the latest state, and the maintenance of accuracy and ensuring that the data is the latest within the scope required according to the purpose of use are sufficient.

2) Safety management measures (Article 20)

Article 20

The entity handling personal information must devise the required and appropriate measures for safety management of personal data against leakage, loss, or damage of the handled personal data.

The entity handling personal information must devise organizational, human, physical, and technical safety management measures to prevent leakage, loss, or damage of the handled personal data (excluding 1 .(4) # Handling of telephone directory, car navigation systems, etc.).

It shall consider the magnitude of damages to rights and interests incurred by the data subject in the event the personal data of the data subject is leaked, goes missing, or is damaged, and devise the necessary and appropriate measures according to risks due to the nature of the business operation involved, and conditions in which personal information is handled. Ideally, safety management measures should be devised according to the nature of the media recording

the personal data.

<Examples of cases where the necessary and appropriate safety management measures have not been devised>

Example 1) When the entity handling personal information neglects the fact that personal data not intended for disclosure is being disclosed to an unspecified majority on the website of the entity.

Example 2) When the entity handling personal information neglects the fact that employees who no longer need to access personal data due to reorganization are able to access the data, and these employees have leaked the personal data.

Example 3) When personal data registered for the data subject to receive continuous services damages due to system malfunction, and the backup which was supposed to have been extracted is also damaged, and the personal data is lost or damaged due to recovery failure, disabling the data subject to receive services.

Example 4) Access control is not implemented on personal data, and employees not granted access acquires the personal data as a result and leak it.

Example 5) The media backing up the personal data are in a state where they can be taken out by unauthorized persons and are taken out.

Organizational safety management measures

Organizational safety management measures are measures which clearly designate the responsibilities and authority of employees on safety management (see Article 21), establish and run provisions and procedures on safety management (hereafter referred to as “provisions, etc.”), and verify the implementation state.

<Cases where organizational safety management measures must be devised>

- (a) Establishment of organizational structure for devising safety management measures for personal data
- (b) Establishment of provisions, etc. designating safety management measures of personal data, and operations following the provisions, etc.
- (c) Establishment of methods which can list the handling state of personal data
- (d) Evaluation, review, and improvement of safety management measures of personal data
- (e) Handling of accidents and violations

<Examples for which establishment of safety management measures is recommended for each item above>

- (a) Recommended in the establishment of organizational structure for devising safety management measures of personal data

* Clarification of the roles and responsibilities of employees

It is advisable to specifically prescribe the roles and responsibilities of employees related to the safety management of personal data in internal provisions such as provisions on the segregation of duties, provisions on administrative authority, etc., contracts, and job descriptions.

* Installation of personal information protection administrators (so called chief privacy officer (COP))

* Installation of work supervisors and restriction of persons in charge of work in the handling of personal data (acquisition, input, transfer, transmission, use, processing, storage, backup, deletion, disposal, etc.)

* Installation of information system administration supervisors handling the information and restriction of persons in charge of work (including system administrators)

* Clarification of roles and responsibilities of departments related to the handling of personal data

* Installation of audit supervisors

* Establishment of audit implementation system

* Establishment of system to report and contact representative, etc. in the event of violations or signs of violations of provisions on handling of personal data

* Establishment of system to report and contact representative, etc. in the event of accidents such as leakage of personal data, etc. or it has been deemed that there are high risks of this

As information on leakage of personal data, etc. may come in from outside via main counters or complaint handling centers, it is ideal to promote linkage with complaint processing systems, etc. (See Article 31)

* Establishment of information provision system to data subjects who may be affected by accidents such as leakage, etc.

* Establishment of systems for reporting to the competent minister and authorized personal information protection organization, etc. in the event of accidents such as leakage

(b) Items recommended in the establishment of provisions designating safety management measures of personal data, and operations conforming to the provisions, etc.

* Establishment of provisions on the handling of personal data, etc. and operations conforming to the provisions

* Establishment of provisions on the safety management measures of information systems handling personal data, etc., and operations conforming to the provisions

For detailed description items on the above, refer to the following <Items to be described in provisions on the handling of personal data, etc.>.

* Establishment of provisions on the safety management of buildings, rooms, safes, etc. related to the handling of personal data, etc., and operations conforming to the provisions

* Establishment of criteria for selecting the consignee when consigning the handling of personal data, and the establishment of consignment contract template, etc.

* Maintenance of audit trail indicating that the work procedure has been implemented

appropriately in accordance with the designated provisions, etc.

Audit trails to be maintained included application forms on the use of information systems in relation to personal data, application form assigning special authority to a certain employee, list of users of information systems and their authority, records of entry/exit into buildings, etc., records of access to personal data (for example, records who performed what operation), list of participants of training, etc.

(c) Items recommended in the establishment of procedures for listing handling state of personal data

- * For personal data, establishment of personal data handling ledgers recording items to be acquired, purpose of use notified, storage place, storage method, those with access rights, deadline of use, and other information required for the appropriate handling of personal data
- * Maintenance of the latest state by the periodic verification of the contents of the personal data handling ledger

(d) Items recommended in the evaluation, review, and improvement of safety management measures for personal data

- * Scheming of audit plans and implementation of audit (internal and external) based on plans
- * Consolidation of audit implementation results and report to representative
- * Periodic review and improvement of safety management measures according to audit reports from audit supervisor, changes in social standards towards personal data, and progress of information technology

(e) Items recommended in handling accidents and violations

- * Announcement of fact relevance, prevention of recurrence, etc.
- * Others, implementation of the following items, etc.
 - a) Fact survey, b) Specification of scope of impact, c) data subjects who may be affected and report to competent minister, etc., d) investigation of causes, e) review and implementation of recurrence prevention, etc.

<Items to be indicated in provisions related to the handling of personal data>

The following are items to be indicated in provisions, etc. according to the flow of the handling of personal data ; (i) acquisition, input, (ii) transfer and transmission, (iii) use and processing, (iv) storage and backup, (v) deletion and disposal, for each of these steps.

(i) Acquisition and input

i) Clarification of work supervisor

- * Clarification of work supervisor when acquiring personal data

- * Clarification of work supervisor when entering acquired personal data in the information system

(Hereafter, referred to as “acquiring/entering”.)

ii) Clarification of procedures and implementation according to procedure

- * Clarification of procedures when acquiring/entering
- * Implementation of acquisition/entering by designated procedure
- * Implementation of input work at buildings and rooms (hereafter referred to as “buildings, etc.”) which cannot be entered by unauthorized persons
- * Restrictions based on the need for terminals which can input personal data in operations
- * Restrictions based on the need for functions assigned to terminals which can input personal data in operations (for example, disabling connection of external recording media such as CD-R, USB memory, etc. for terminals which can input personal data)

iii) Identification, authentication, and authorization of persons in charge of work

- * Restrictions based on need for persons in charge of work which can acquire and enter personal data in operations
- * Identification of persons in charge of work by identification using ID or password, or biometrics
- * Restriction of authority assigned to persons in charge of work
- * Recording of authority assigned to persons in charge of work performing acquisition and input of personal data

iv) Verification of persons in charge of work and their authority

- * Clarification of procedures, implementation according to procedures, and verification of implementation state of identification, authentication, and authorization of persons in charge of work
- * Access recording, storage, and verification of presence of work outside authority

(ii) Transfer/transmission

i) Clarification of persons in charge of work

- * Clarification of persons in charge of work when transferring/transmitting personal data

ii) Clarification of procedure and implementation according to procedure

- * Clarification of procedures when transferring/transmitting personal data
- * Implementation of transfer/transmission by designated procedure
- * Encryption of personal data when transferring/transmitting personal data (for example, when transmitting personal data using public lines), verification of address and receipt during transfer (for example, use of delivery record postal mail, etc.)

Verification of other party number for FAX, etc., and receipt

- * Prohibition of leaving documents recording personal data in the fax machine, etc.

- * Appropriate management of encryption key and password
- iii) Identification, authentication, and authorization of persons in charge of work
- * Restrictions based on the need for persons in charge of work who can transfer/transmit personal data in operations
 - * Authentication by ID and password, identification of persons in charge of work by biometrics, etc.
 - * Restrictions of authority assigned to persons in charge of work (for example, when sending personal data via a computer network, the sender need not have the authority to browse or change the contents of the personal data)
 - * Recording of authority assigned to persons in charge of work performing transfer/transmission work of personal data
- iv) Verification of persons in charge of work and their authority
- * Clarification of procedures, implementation according to procedures, and verification of implementation state of identification, authentication, and authorization of persons in charge of work
 - * Access recording, storage, and verification of presence of work outside authority
- (iii) Use/processing
- i) Clarification of work supervisors
- * Clarification of work supervisor in the use/processing of personal data
- ii) Clarification of procedure and implementation according to procedure
- * Clarification of procedures when using/processing personal data
 - * Implementation of use/processing by designated procedure
 - * Implementation of use/processing at buildings, etc. which cannot be entered by unauthorized persons
 - * Restrictions based on the need for terminals which can input/process personal data in operations
 - * Restrictions based on the need for functions assigned to terminals which can input/process personal data in operations (for example, disabling connection of external recording media such as CD-R, USB memory, etc. for terminals which can input personal data)
- iii) Identification, authentication, and authorization of persons in charge of work
- * Restrictions based on need for persons in charge of work who use/process personal data in operations
 - * Identification of persons in charge of work by identification using ID or password, or biometrics
 - * Restriction of authority assigned to persons in charge of work (for example, persons in charge of work requiring only the browsing of personal data in operations need not have authority for copying person data)

- * Recording of authority assigned to persons in charge of work using/processing personal data (for example, copying, printing, deleting, changing, etc.)

iv) Verification of persons in charge of work and their authority

- * Clarification of procedures, implementation according to procedures, and verification of implementation state of identification, authentication, and authorization of persons in charge of work

- * Access recording, storage, and verification of presence of work outside authority

(iv) Storage/backup

i) Clarification of work supervisors

- * Clarification of work supervisor in the storage/backup of personal data

ii) Clarification of procedure and implementation according to procedure

- * Clarification of procedures when storing/backing up personal data

- #When processing personal data on an information system, there may be a need to not only backup personal data, but also the operating system (OS) and applications.

- * Implementation of storage/backup by designated procedure

- * Encryption of personal data when storing/backing up

- * Appropriate management of encryption key and password

- * Lock control when storing media recording personal data

- * Management of keys of rooms, safes, etc. storing media recording personal data

- * Remove control of media recording personal data

- * Implementation of tests that data can be recovered promptly from personal data backup

- * Recording of various events and failures related to the backup of personal data

iii) Identification, authentication, and authorization of persons in charge of work

- * Restrictions based on need for persons in charge of work who store/backup personal data in operations

- * Identification of persons in charge of work by identification using ID or password, or biometrics

- * Restriction of authority assigned to persons in charge of work (for example, when backing up personal data, the person in charge of the work does not require the authority to browse or change the contents of the personal data)

- * Recording of authority assigned to persons in charge of work performing storage/backup of personal data (for example, implementation of backup, management of safe key, etc.)

iv) Verification of persons in charge of work and their authority

- * Clarification of procedures, implementation according to procedures, and verification of implementation state of identification, authentication, and authorization of persons in charge of work

* Access recording, storage, and verification of presence of work outside authority

(v) Deletion/disposal

i) Clarification of work supervisors

- * Clarification of work supervisor in the deletion of personal data
- * Clarification of work supervisor in the disposal of machines storing personal data and media recording personal data

ii) Clarification of procedure and implementation according to procedure

- * Clarification of procedures when deleting/disposing personal data
- * Implementation of deletion/disposal by designated procedure
- * Implementation of deletion/disposal at buildings, etc. which cannot be entered by unauthorized persons
- * Restrictions based on the need for terminals which can delete personal data in operations
- * Prior to returning media and machines recording personal data to rental companies, delete data completely (for example, overwrite the media with meaningless data once or several times)
- * Physical destruction of media recording personal data (for example, destroy using shredder, media shredder, etc.)

iii) Identification, authentication, and authorization of persons in charge of work

- * Restrictions based on need for persons in charge of work who can delete/dispose personal data in operations
- * Identification of persons in charge of work by identification using ID or password, or biometrics personal data
- * Restriction of authority assigned to persons in charge of work
- * Recording of authority assigned to persons in charge of work performing deletion/disposal of data personal

iv) Verification of persons in charge of work and their authority

- * Clarification of procedures, implementation according to procedures, and verification of implementation state of identification, authentication, and authorization of persons in charge of work
- * Access recording, storage, and verification of presence of work outside authority

Human safety management measures

Human safety management measures mean entering nondisclosure contracts for personal data specified as confidential in operations to employees and providing education and training, etc.

<Items which need to be devised as human safety management measures>

- (a) Entering nondisclosure contracts when signing employment contracts and consignment contracts
- (b) Implementing education and training for employees

For details on supervision to ensure that administrators observe the designated provisions, etc., refer to Article 21.

<Items recommended to be devised for each item>

(a) Recommended items in the entering of nondisclosure contracts when signing employment contracts and consignment contracts

- * Entering nondisclosure contracts in the hiring of employees or when entering consignment contracts

- # It is recommended that nondisclosure provisions in employment contracts and consignment contracts be made effective for a certain period of time after the completion of the contract.

- * Establishment of provisions on measures when nondisclosure contracts are violated

- # It is recommended that contracts, etc. clearly indicate the scope and access conditions of parties with accessibility for persons who may be able to enter buildings storing personal data even if they are employees handling personal data and for persons who may access information systems handling personal data. Parties other than employees handling personal data include those related to the development and maintenance of information systems, cleaning persons, security guard, etc.

(b) Items recommended in the implementation of dissemination, education, and training for employees

- * Disseminate internal provisions, etc. designating the roles and responsibilities of employees related to the safety management of personal data and information systems

- * Implement education and training on the roles and responsibilities of employees related to the safety management of personal data and information systems

- * Verify that the required and appropriate education and training is implemented for employees

Physical safety management measures

Physical safety management measures mean measures such as management of entering and exiting buildings (rooms), and prevention of personal data theft, etc.

<Items which need to be devised as physical safety management measures>

- (a) Implementation of management of entering and exiting buildings (rooms)
- (b) Prevention of thefts, etc.

(c) Physical protection of machines and devices, etc.

<Items recommended to be devised for each item above>

(a) Items recommended in the implementation of management of entering and exiting buildings (rooms)

- * Implementation in rooms which are physically protected by the management of entrance/exit in the handling operations of personal data
- * Installation of information systems, etc. handling personal data in rooms which are physically protected by the management of entrance/exit

(b) Items recommended in the prevention of theft, etc.

- * Prohibition of leaving documents, media, or portable computers, etc. on desks, etc. in absence
- * Starting up of screensavers with password, etc. in absence
- * Locking and storage of media including personal data
- * Separation and storage of personal data indicating name, address, and mail address, and other personal data
- * Prohibition of leaving instruction manuals of information systems handling personal data on desks, etc.

(c) Items recommended in the physical protection of machines, devices, etc.

- * Physical protection of machines and devices handling personal data from safety management threats (for example theft, destruction, damage) and environmental threats (for example water leakage, fire hazard, power failure)

Technical safety management measures

Technical safety management measures are technical safety management for personal data such as access control of personal data and information systems handling personal data, illegal software measures, information system monitoring, etc.

<Items that need to be devised as technical safety management measures>

- (a) Identification and authentication in access of personal data
- (b) Access control to personal data
- (c) Management of access rights for personal data
- (d) Recording of personal data access
- (e) Illegal software measures for information systems handling personal data
- (f) Measures for transferring/transmitting personal data
- (g) Measures for verifying operations of information systems handling personal data
- (h) Monitoring of information systems handling personal data

<Items recommended to be devised for each item above>

(1) Items recommended in identification and authentication when accessing personal data

- * Implementation of identification and authentication that the employee has access rights to confirm that access of personal data is legitimate (for example, authentication using ID and password, biometrics, etc.)

- # When using ID and password, it is recommended that measures be devised such as setting an term of validity for the password, restricting use of the same or similar password, setting the minimum number of characters for a password, suspending IDs failing login for a certain number of times, etc.

- * Implementation of identification and authentication of terminals or addresses, etc. which employees with access rights to personal data can use (for example, MAC address authentication, IP address authentication, authentication using e-certificates and secrecy sharing technologies, etc.)

(2) Items recommended in access control to personal data

- * Minimization of number of employees to be assigned access rights to personal data

- * Access control based on identification (A state where files set with passwords can be accessed by anyone means that access control is implemented but not identified. In this case, parties who know the password are designated, and everytime parties granted access are changed, there is a need to change the password appropriately.)

- * Minimization of access rights assigned to employees

- * Restriction of number of users who can use information systems storing personal data simultaneously

- * Restrictions on the time of use of information systems storing personal data (for example, disabling access of information systems on holidays and non business hours, etc.)

- * Protection from unauthorized access of information systems storing personal data (for example, firewall, router, etc. setting)

- * Prevention of unauthorized use of applications which can access personal data (for example, mounting authentication systems to application systems, installing the required application systems only on computers used by employees required in work, displaying only functions required in work on menus, etc.)

- # Even for special privilege users of information systems, if there is no need to know the contents of personal data for information system management, it is recommended that access be controlled so that the personal data cannot be directly accessed.

- # Regarding access control of special privilege users, for example, use of trusted OS, secure OS, and products realizing access control functions can be given.

- * Verification of validity of access control functions implemented in information systems handling personal data (for example, verification of the vulnerability of web applications)

(c) Items recommended in management of access rights to personal data

- * Appropriate and periodic implementation of authorization management permitting parties who can access personal data (for example, adequately screen if the person in charge of registering those accessing person data is appropriate periodically, and enable only that person to carry out registration, etc.)

- * Implementation of minimum required access control to information systems handling personal data

(d) Items recommended in the recording of access to personal data

- * Recording of accesses to personal data and if operations were successfully or failed (for example, when access to personal data and operations cannot be recorded, record the success and failure of access to information systems)

- * Appropriate protection from leakage, loss and damage of extracted records

 - # Take note that records of information systems handling personal data may correspond to personal information in some cases

(e) Items recommended in the implementation of illegal software measures for information systems handling personal data

- * Implementation of antivirus software

- * Application of modification software for security measures for operating systems (OS) and applications (so called security patch)

- * Verification of validity and stability of illegal software measures (for example, verification of updating of pattern files and modification software)

(f) Items recommended in measures for transfer (transportation, postal mail, express courier services, etc.) and transmission of personal data

- * Measures for loss and theft during transfer (for example, encryption of personal data stored on media)

- * Encryption of personal data when sending (data transfer including input and access by data subjects and employees, attaching files to mail, etc.) personal data over networks (for example, Internet, wireless LAN, etc.) with risks of eavesdropping

(g) Items recommended in measures for verification of operations of information systems handling personal data

- * Prohibition of use of personal data as test data in the verification of operations of

information systems

* Verification that the security of the information system and its operating environment is not impaired due to changes of the information system

(h) Items recommended in the supervision of information systems handling personal data

* Periodic supervision of the using state of information systems handling personal data

* Monitoring of access state to personal data (Including details of operations)

Take note that records of results of monitoring information systems handling personal data may correspond to personal information

3) Supervision of employees (Article 21)

Article 21

The entity handling personal information must conduct the required and appropriate supervision on employees so that safety management of the concerned personal data is promoted in the handling of the personal data by employees.

The entity handling personal information must implement the required and appropriate supervision on employees so that safety management measures based on Article 21 are observed (excluding 1. (4) # Handling of telephone directory, car navigation systems, etc.). At this time, the required and appropriate measures shall be devised in accordance with risks due to the nature of the business operation involved, and conditions in which personal information is handled, taking into account the degree of infringement of rights and interests incurred by the data subject when personal data of the data subject is leaked, lost, or damaged, etc.

“Employees” means those engaged in the activities of companies under the command and supervision of the companies directly or indirectly in the organization of the entity handling personal information. They include not only employees (full time employees, contract employees, short-term contract employees, part-time employees, etc.) but also board members, operating officers, auditors, managers, temp staff, etc.

<When the required and appropriate supervision is not carried out on employees>

Example 1) When employees fail to periodically verify at the designated intervals that operations are carried out in accordance with the provisions, etc. designating the safety management measures of personal data, and as a result, personal data is leaked

Example 2) Even if notebook PCs containing personal data are repeatedly brought out in violation of internal provisions, this act is ignored, and as a result, personal data is lost and leaked

<Precautions on implementation of employee supervision>

The following points should be noted when implementing supervision of employees and consignees related to the handling of personal data, and video and online monitoring on employees as part of safety management measures (hereafter called “monitoring”).

At this time, when designating important items related to the handling of personal information related to employment management, it is recommended that the labor union be notified, etc., and if necessary, discussions should be conducted. When designating key items, it is recommended that the work force, etc. be informed.

Important items on the handling of personal information related to employment management prescribed in Guidelines on Measures to be Devised by Companies (2004 Ministry of Health, Labour and Welfare Notice No. 259) No. 39 (1) to ensure the appropriate handling of personal information related to this guidelines and employment management are items on monitoring.

- * Identify beforehand the aims of monitoring and purpose of use of personal information to be obtained, designate in-house provisions and clarify these to employees.
- * Prescribe the supervisors of monitoring and their authority.
- * When implementing monitoring, establish in-house draft provisions prescribed for the implementation of monitoring beforehand, and promote these thoroughly in the company beforehand.
- * Perform auditing and verification if monitoring is carried out appropriately.

4) Supervision of consignee (Article 22)

Article 22

When the entity handling personal information consigns all or part of the handling of personal data, it must implement the required and appropriate supervision on the consignees to promote safety management of personal data handling consigned.

When the entity handling personal information consigns all or part of the handling of personal data, it must implement the required and appropriate supervision on the consignees to ensure observance of safety management measures based on Article 20 (excluding 1. (4) # Handling of telephone directory, car navigation systems, etc.). At this time, the required and appropriate measures shall be devised in accordance with risks due to the nature of the business operation involved, and conditions in which personal information is handled, taking into account the degree of impairment of rights and interests incurred by the data subject when personal data of the data subject is leaked, lost, or damaged, etc.

“Required and appropriate supervision” means incorporating details consented by both the consignor and consignee in the consignment contract on the handling of personal data as required and appropriate safety management measures, as well as verification that these details are implemented appropriately at the predetermined interval.

If a person in a dominant bargaining position is the consignor, no unreasonable burden must be imposed on the consignee.

If the consignor is not implementing “required and appropriate supervision” on the consignee, and in the event of re-consignment by the consignee, if the re-consignee is implementing handling that is not considered appropriate and some kind of problem has occurred, the consignor may be charged in some cases. Re-consignment must therefore be done carefully.

<If required and appropriate supervision is not implemented on the consignee>

Example 1) In the event of consignment to external providers without periodically identifying the state of safety management measures of personal data when entering contracts and thereafter, and the consignee leaked the personal data

Example 2) When details of safety management measures prescribed on the handling of personal data were not specified to the consignees and as a result, the consignee leaked the personal data

Example 3) When instructions related to re-consignment conditions are not provided to consignees, and at the same time, verification of the handling state of personal data by consignees is neglected, and the consignee re-consigns the processing of personal data, resulting in the leakage of personal data by the re-consignee.

<Items recommended for incorporation in contracts when consigning handling of personal data>

- * Clarification of responsibilities of consignors and consignees
- * Items related to the safety management of personal data
 - * Items on the prevention of personal data leakage and prohibition of fraudulent use
 - * Prohibition of processing and use outside the scope of consignment contract
 - * Prohibition of copying outside the scope of consignment contract
 - * Consignment contract period
 - * Items on the return, deletion, and disposal of personal data after the consignment contract ends
- * Items on re-consignment
 - * Report to the consignor in writing in re-consignment
- * Details and frequency of reports to the consignor on the handling state of personal data
- * Verification that contract provisions are observed (For example, include information security audit.)
- * Measures when contract provisions are not observed
- * Items on reporting and notification when security incidents and accidents occur

(4) Provision to third party (Article 23)

(a) Principle (Paragraph 1, Article 23)

Paragraph 1, Article 23

The entity handling personal information must not provide personal data to third parties without the prior consent of the data subject except in the following cases.

1. When based on ordinance
2. When consent of the data subject is difficult to obtain due to the need for the protection of human life, physical or asset protection
3. When there is especially a need to promote the enhancement of public health and sound growth of children during mental and physical development, but it is difficult to obtain the consent of the data subject
4. When there is a need for national organizations, local public organizations, or entities consigned by these organizations to provide support in the implementation of paperwork designated by ordinance, but there is a risk that obtaining the consent of the data subject may affect the implementation of the concerned paperwork

The entity handling personal information must not provide personal data to third parties without prior (#1) consent (#2) of the data subject (excluding 1. (4) # Handling of telephone directory, car navigation systems, etc.). Consent must also be obtained by a reasonable and appropriate method deemed necessary for the data subject to make judgments related to the consent in accordance with the nature of the business operation involved, and conditions in which personal information is handled.

#1 "Prior" means "prior to the provision of personal data to a third party"

#2 Regarding "Obtaining the consent of data subject", see 1. (10).

<Examples of provision to third parties> (However, excluding each item of Paragraph 4, Article 23.)

Example 1) Exchange of personal data between affiliated companies and group companies

Example 2) Exchange of personal data between the head office and member stores of franchise organizations

Example 3) Exchange of specific personal data between fellow traders

Example 4) Provision of personal data of individuals living in Japan to foreign companies

<Examples of provision to third parties> (However, restricted by purpose of use)

Example) Provision of personal data to other departments within the same company

However, in the following case, personal data can be provided to third parties without the consent of the data subject.

i. When providing personal data based on ordinance

(Example is the same as (1)(e)i .)

<Additional examples>

Example) When authorized personal information protection organizations seek the submission of documents to applicable providers based on Paragraph 2, Article 42, and the providers submit the documents accordingly

ii. When there are risks of violation of specific rights and interests such as human (including corporate) life and assets, and there is a need for the provision of personal data to protect these, but the consent of the data subject is difficult to obtain (except when the said rights and interests can be protected sufficiently by other methods)

(Example is the same as (1)(e)ii.)

iii. When personal data is especially required for the enhancement of public health or sound growth of children during both mental and physical development, but it is difficult to obtain the consent of the data subject (except when enhancement of public health and sound growth of children during both mental and physical development can be done sufficiently by other methods)

(Example if the same as(1)(e)iii.)

iv .When there is a need for national organizations to obtain support of private companies, etc. to implement paperwork designated by ordinance, but there is a risk that obtaining the consent of the data subject in the provision of personal data by the cooperating private company to the concerned national organization may affect the implementation of the concerned paperwork_

(Example if the same as(1)(e)iv.)

(b) Opt-out (Paragraph 2, Article 23)

The entity handling personal information is able to provide personal data to third parties without consent of the data subject if opt-out (#1) in third party provision has been

implemented.

#1 “Opt-out in third party provision” means that prior to provision, the following i. to iv. .

information is notified (#2) to the data subject, or ensure that the information easily accessible to the data subject (#3), and stop provision of information to third parties when requested by the data subject.

#2 Regarding “notification to data subject”, see 1. (7).

#3 Regarding “information easily accessible to the data subject”, see 1.(11).

<Examples of opt-out>

Example 1) Residential area map provider (Prepare and sell residential area maps by investigating doorplates and postbox (third party provision to unspecified majority))

Example 2) Database provider (Prepare and sell name lists for direct mail, etc.)

Paragraph 2, Article 23

When the entity handling personal information is to stop provision to third parties of personal data that can identify the data subject according to the request of the data subject for personal data provided to third parties, and notifies the data subject beforehand on the following items, or ensure that the information is easily accessible to the data subject beforehand, it is able to provide the concerned personal data regardless of the preceding paragraph.

1. Provision to third party should be set as the purpose of use
2. Items of personal data provided to third parties
3. Methods of providing to third parties
4. Suspension of provision to third parties personal data which identifies the concerned data subject as requested by the data subject.

If the following i. to iv. items are all notified to the data subject beforehand or information is easily accessible to the data subject, the entity is able to provide the concerned personal data regardless of the preceding paragraph.

i. Setting provision to third parties as purpose of use

ii. Items of personal data provided to the third parties

Example 1) Name, address, telephone number

Example 2) Name, product purchase history

iii. Means or methods of providing to third parties

Example 1) Publication of books

Example 2) Placement on the Internet

Example 3) Printout and issue, etc.

iv. Suspend provision to third parties according to the request of data subject.

(c) Non-applicability as third party (Paragraph 4, Article 23)

As the following i. to iii. do not correspond to third parties, information can be provided without the consent of the data subject or the opt-out in third party provision.

i. Consignment (Item 1, Paragraph 4, Article 23)

Item 1, Paragraph 4, Article 23

In the following cases, the persons receiving the corresponding personal data does not correspond to third parties in the application of the provisions of the preceding Paragraph 3

1. When the entity handling personal information consigns the whole or part of the handling of personal data in the scope required for achieving the purpose of use.

When consigning the whole or part of operations related to the handling of personal data, does not corresponding to third party.

The entity handling personal information has the responsibility to supervise consignees (Article 22).

Example 1) When handing personal data for consigning information processing such as data input, etc.

Example 2) When handing personal data for express courier service personal to department stores want to deliver the ordered product

ii. Succession of business (Item 2, Paragraph 4, Article 23)

Item 2, Paragraph 4, Article 23

In the following case, the person receiving the concerned personal data is not considered a third party in the application of the preceding paragraph 3.

2. When personal data is provided with the succession of business due to other reasons such as merger

The person receiving the concerned personal data is not considered a third party in the

transfer of personal data due to succession of business by merger, division of company, sales transfer, etc.

Even after the succession of business, personal data must be used in the scope of the purpose of use prior to the transfer.

It should be noted that the person receiving the concerned personal data may be considered a third party if in the negotiation stage prior to the entering of the contract for business succession, the company is investigated by the other company and the personal data of the company is provided to the other company.

Example 1) Transfer of personal data to new company after merger, division of company

Example 2) Transfer of personal data to the company to which sales is transferred

iii. Shared use (Item 3, Paragraph 4, Article 23)

Item 3, Paragraph 4, Article 23

In the following case, the person receiving the concerned personal data is not considered a third party in the application of the preceding paragraph 3.

3. When the personal data is jointly used with a specific party, the data subject is notified beforehand or is in a state in which the data subject can learn easily of this fact. Items of the personal data used jointly, scope of parties using the personal data jointly, purpose of use of users, name of the person supervising the management of the said personal data.

The person receiving the concerned personal data is not considered a third party when using the personal data jointly with a specific party, the following a) to d) information must be notified (#2) to the data subject beforehand (#1), or the data subject must have easy access to the information (#3), and at the same time, if shared use is disclosed.

#1 “Beforehand” means “prior to the shared use of personal data”.

#2 Regarding “notification to data subject”, see 1. (7).

#3 Regarding “data subject must have easy access to this information”, see 1. (11).

<Examples of shared use>

Example 1) Shared use of information within the scope of the purpose of use for providing general services at group companies

Example 2) Shared use of personal data within the scope of the purpose of use between parent-child and affiliated companies

Example 3) Shared use of personal data within the scope of the purpose of use with foreign companies

a) Items on personal data used jointly

Example 1) Name, address, telephone number

Example 2) Name, product purchase history

b) Scope of shared users (the scope must be clear to the data subject, and as long as the scope is clear, separate listing may not necessarily be required)

c) Purpose of use of users (all purposes of use of jointly used personal data)

d) Name of person committed to handling requests related to disclosure, etc. and receiving grievances, as well as has responsibility over the management of personal data such as safety management, etc. and authority over disclosure, correction, and cessation, etc. of the contents of the personal data. (Amongst shared users, the entity with the authority to primarily receive and process grievances, disclose, correct, etc. is called “person with responsibility”. It does not refer to an internal supervisor of shared users.)

Paragraph 5, Article 23

When changing the purpose of use of users prescribed in the preceding item 3 or the name of the person with responsibility over the management of personal data , the entity handling personal information must notify the data subject of the changes beforehand or the data subject must have easy access to this information.

a) and b) above cannot be changed, but c) and d) can be changed within the scope deemed not difficult for the data subject to conceive (#1) from common sense. Prior to the change, changes must be notified (#2) to the data subject or the data subject must have easy access to this information (#3).

#1 Regarding “scope deemed not difficult for the data subject to conceive”, see (1).

#2 Regarding “notification to data subject”, see 1. (7).

#3 Regarding “data subject must have easy access to this information”, see 1. (11)

(d) Personal data related to employment management

In the provision of personal data to a third party (except when corresponding to Paragraphs 1 through 4 of Article 23), the following items should ideally be noted for personal data on employment management. The required and appropriate measures shall also be devised in accordance with the nature of the business operation involved, and conditions in which personal data is handled on employment management.

Here, provision of personal data on employment management to a third party means provision of personal data on employment management such as personnel ability rating information, etc. of concerned employees to leased company when leasing employees, and provision of personal data on employment management of information on the ability of engineers when assigning workers.

Consequently, this does not apply to cases where personal data such as name and title of employees are received from the company, this information is made into a database, and providing it to parties aiming to disclose or sell the information.

- * Parties receiving personal information must not leak nor plagiarize personal information obtained through the handling the personal data on the concerned employees.
- * Approval of re-provision of the concerned personal data must be obtained from the entity in writing beforehand.
- * Clarification of storage period at parties receiving information.
- * Verification with entities that after the purpose of use has been achieved, the personal data is returned, destroyed, or deleted, and these processes are implemented appropriately and definitely.
- * Prohibition of copy of personal data at parties receiving information (except when the aim is backup required for safety management).

(5) Disclosure of items on handled personal information, disclosure, correction, cessation, etc. of handled personal information (Articles 24 to 30)

1) Disclosure of items on handled personal information (Article 24)

(a) Notification of items on handled personal information to data subject (Paragraph 1, Article 24)

Paragraph 1, Article 24

The entity handling personal information must ensure that the data subject is accessible to the following items on handled personal information (including instances in which response is made to demand by the data subject without delay).

1. Name of concerned entity handling personal information
2. Purpose of use of all handled personal information (except when corresponding to Items 1 to 3, Paragraph 4, Article 18)
3. Procedures based on the requirements of the provisions of the following paragraph, Paragraph 1 of the following Article, Paragraph 1 of Article 26 or Paragraph 1 or 2 of Article 27 (including the handling charge if prescribed in the provisions in Paragraph 2 of Article 30)
4. In addition to the above item, items prescribed by ordinance as items required to ensure

appropriate handling of handled personal information

Ordinance Article 5

The items prescribed by ordinance of Item 4, Paragraph 1, Article 24 are as follows.

1. Party accepting grievances regarding handling of personal information by entity handling personal information
2. If the entity handling personal information is an applicable provider of an authorized personal information protection organization, name of the said personal information protection organization and party accepting grievances

The entity handling personal information shall ensure that the following i. to iv. handled personal information is easily accessible to the data subject (including instances in which response is made to demand by the data subject without delay)(#1) (excluding 1.(4) #Handling of telephone directory, car navigation systems, etc.).

Regarding personal information owned form prior the enforcement of this Act, as there are no acts of acquiring personal information at the time of enforcement, and the provisions of Article 18 do not apply, there is a need to devise measures indicated in Paragraph 1, Article 24 at the time this Act is enforced.

#1 Regarding “accessible by data subject (including instances in which response is made to demand by the data subject without delay), see 1. (12).

i . Name of entity handling personal information

ii. Purpose of use of all handled personal information (However, except for certain cases (#2). Same as ”purpose of use” related to personal information used in Article 15 onwards.)

#2 “certain cases” mean the following.

- a) When the notification or disclosure of the purpose of use to the data subject may cause life-threatening, physical and asset damage to the data subject or a third party (Same as example (2)(e) i.)
- b) When the notification or disclosure of the purpose of use to the data subject may violate the rights or interests of the concerned entity handling personal information (Same as example (2)(e) ii.)
- c) When a national organization, etc. requires the support of private companies, etc. to implement paperwork designated by ordinance, and the notification or disclosure of the purpose of use of the personal information obtained by the cooperating private company from the national organization to the data subject may interfere with the implementation of the said paperwork (Same as example (2)(e) iii.)

iii. Handling charge related to the notification of the purpose of use of handled personal information and disclosure of handled personal information (restricted to when this is prescribed) (#3) and procedures for seeking disclosure (#4).

#3 The handling charge for demand for disclosure based on the Law on the Disclosure of Information Owned by Administrative Organizations (1999 Law No. 42) Article 16 and Enforcement Order of the said Law (2000 Cabinet Order No. 41) Paragraph 1, Article 13 is 300 yen (disclosure implementation handling charge is changed separately).

#4 "Demand for disclosure, etc." is defined as demand for notification of the purpose of use of handled personal data, for disclosure of handled personal data, for revision, addition or deletion of items in handled personal data, for cessation or cancellation of use of handled personal data or for cessation of availability of handled personal data to third parties.

iv. Party submitting grievances and enquiries on the handling of the handled personal information are submitted (if the entity handling personal information belongs to an authorized personal information protection organization (#5), includes the name of the organization and party submitting)

#5 "Authorized personal information protection organization" system

System certified by the competent minister on private organization conducting activities with the aim of securing appropriate handling of personal information such as processing of grievances, etc. The set up of this system aims to secure reliability of the concerned activities and promote protection of personal information by private organizations (refer to Article 37 and onwards).

(Reference)

Paragraph 1, Article 37

Incorporated entities attempting to implement services outlined below for the purpose of ensuring appropriate handling of personal information of entity handling personal information (including organizations which are not incorporated entities for which the representative or manager is prescribed, sales in Item 3 in the following article) can be authorized by the competent minister.

1. Processing of grievances prescribed by Article 42 on the handling of personal information by entity handling personal information applicable for the services (hereafter referred to as "applicable entities").
2. Provision of information for applicable entities for items contributing to ensuring the

appropriate handling of personal information

3. In addition to the above item 2, activities required for ensuring the appropriate handling of personal information of applicable entities

Paragraph 2, Article 37

Parties receiving the authorization in the preceding paragraph must apply to the competent minister in accordance with the provisions of ordinance.

Paragraph 3, Article 37

If the competent minister implements the authorization of Paragraph 1, it must disclose this.

Paragraph 1, Article 42

When the data subject requests resolution of grievances on the handling of personal information of applicable entities to the authorized personal information protection organization, the organization must provide the required counseling and advice, investigate the situation of the grievances, notify the applicable entity of the details of the grievances, and seek prompt resolution.

Paragraph 2, Article 42

When the authorized personal information protection organization deems it necessary to resolve the grievances related to the submission in the preceding paragraph, it can seek an explanation in writing or orally from the concerned applicable entity, or seek the submission of documents.

Paragraph 3 of Article 42

In the event the applicable entity is sought by the authorized personal information protection organization as prescribed in the preceding paragraph, it cannot refuse without a legitimate reason.

(b) Notification of purpose of use of handled personal information (Paragraph 2 and 3 of Article 24)

Paragraph 2, Article 24

When the entity handling personal information is sought by the data subject for notification of the purpose of use of handled personal information identified by the said data subject, it must notify this to the data subject without delay. However, this does not apply to the following cases.

1. When the purpose of use of the handled personal information that can identify the data subject is clear from the provisions of the preceding paragraph
2. When corresponding to Items 1 to 3, Paragraph 4, Article 18

Paragraph 3, Article 24

When the entity handling personal information decides not to notify the data subject of the purpose of use of the handled personal information in compliance with provisions of the

preceding paragraph, it must notify the data subject of this without delay.

When the entity handling personal information is sought by the data subject to notify the purpose of use of handled personal information that can identify the data subject, it must do so without delay except for the following i. to iv. (#) If the entity decides not to notify the data subject, it must notify the data subject of this without delay (excluding 1 . (4) #Handling of telephone directory, car navigation systems, etc.).

Regarding “notification to data subject”, see 1. (7).

i. When the purpose of use of handled personal information that can identify the individual based on the above (a) measures are clear

ii. When the notification or disclosure of the purpose of use to the data subject may cause life-threatening or physical or asset damages to the data subject or third party

(Example same as (2)(e) i.)

iii . When the notification or disclosure of the purpose of use to the data subject may violate the rights or interests of the concerned entity handling personal information

(Example same as (2)(e) ii.)

iv . When a national organization, etc. requires the support of private companies, etc. to implement paperwork designated by ordinance, and the notification or disclosure of the purpose of use of the personal information obtained by the cooperating private company from the national organization to the data subject and the acquisition of consent from the data subject may interfere with the implementation of the said paperwork

(Example same as (2)(e) iii.)

2) Disclosure of handled personal information (Article 25)

Paragraph 1, Article 25

When the entity handling personal information is sought the disclosure of handled personal information that can identify the said data subject (including the notification that no handled personal information that can identify the said data subject exists, same applies below) by the data subject, it must disclose the said handled personal information to the data subject without

delay by a method designated by ordinance. However, if disclosure corresponds to one of the following items, the entity is allowed not to disclose all or part of the information.

1. When there are risks of life-threatening, physical or asset damages, and other violations of the rights and interests of the data subject or third party
2. When there are risks of marked interference of the appropriate implementation of activities related to the concerned entity handling personal information
3. When other ordinances are violated

Ordinance Article 6

The method prescribed by the Paragraph 1, Article 25 ordinance is based on the delivery of documents (when a method consented by the party seeking disclosure is available, this shall be used).

When the entity handling personal information is sought by the data subject to disclose handled personal information that can identify the data subject (when such information does not exist, notification of this), it must disclose the said information to the data subject by a method based on the delivery of documents (when a method consented by the party seeking disclosure is available, this shall be used (#1)) without delay (excluding 1 . (4) #Handling of telephone directory, car navigation systems, etc.).

If other procedures for disclosure are designated by the provisions of other ordinances, these shall have priority.

Regarding the procedures to be implemented in response to the request for disclosure of employment management information, the entity handling personal information shall discuss with the labor union, etc. beforehand. If the disclosure of the handled personal information sought by the data subject in part or in whole has the risk of incurring marked interference in the appropriate implementation of activities, the entity must make the efforts to set down items related to the disclosure of handled personal information taking into account nondisclosure, and devise measures to inform workers, etc.

#1 “when a method consented by the party seeking disclosure is available, this shall be used”

Various disclosure methods are available including e-mail, telephone, etc. if these are consented by the party seeking disclosure. It means that methods based on the delivery of documents are possible without consent.

If the party seeking disclosure does not specify the disclosure method and does not object to the method indicated by the entity handling personal information (including when disclosure by telephone is sought, and after the required confirmation of the data subject, enquiries are replied in the same call), it can be taken that the said method has been consented. Methods of obtaining consent from the party seeking disclosure include the entity handling personal information indicating the disclosure method, and the entity selecting from the several methods desired by the party seeking disclosure.

However, disclosure corresponds to any one of the following i. to iii., the entity need not disclose all or part of the information. In this case, it must notify (#2) the data subject of this.

#2 Regarding “notification to data subject”, refer to 1. (7).

i. When there are risks of life-threatening, physical, or asset damages to the data subject or a third party, or violations of other rights and interests

Example) When the disclosure of the name of the illness at medical institutions, etc. may aggravate the mental and physical conditions of the data subject

ii. When there are risks of marked interference of the appropriate implementation of personal information handling activities

Example 1) When the disclosure of all grading information at test centers may cause marked interference in the maintenance of the test system

Example 2) When repeated disclosure is sought for the same contents requiring complicated handling from the same data subject and incurs marked in, and this may incur marked disruption of activities by monopolizing the enquiry desk and thus disabling other enquiry activities.

iii. When other ordinances are violated

Case) When the disclosure of handled personal information recording the fact that a financial institution registered a transaction with the competent minister based on the “Law on Punishment of Organized Crimes and Restrictions on Crime Interests” Paragraph 1, Article 54 violates Paragraph 2 of the article.

3) Correction of handled personal information, etc. (Article 26)

Paragraph 1, Article 26

When the entity handling personal information is sought by the data subject to correct, add, or delete (hereafter referred to as “correction, etc.”) the contents of the handled personal information that can identify the said data subject for reason that the contents are false, except when special procedures are designated by the provisions of other ordinances in relation to the correction of the contents, the entity must conduct the required investigation without delay within the scope required for achieving the purpose of use, and based on the results, implemented corrections of the said handled personal information contents.

Paragraph 2, Article 26

When the entity handling personal information corrects, etc, all or part of the handled personal information in compliance with provisions of the preceding paragraph, or decides not to implement the corrections, it must notify the data subject of this (if it has implemented

corrections, etc., the details as well) without delay.

When the entity handling personal information is sought by the data subject to implement corrections, etc. for reason that the handled personal information contains errors and are false, as a general rule (#1), it shall implement the corrections, etc. (#2), and notify the data subject of the details of corrections, etc. without delay (excluding 1. (4) #Handling of telephone directory, car navigation systems, etc.).

If special procedures are designated by the provisions of other ordinances, these shall have priority.

#1 "General rule"...Corrections, etc. need not be implemented if deemed unnecessary in view of the purpose of use, or when the error pointed out is incorrect. However, the data subject must be notified³ in such a case, without delay, that correction, etc. will not be implemented.

#2 "Correction, etc." means the correction, addition, or deletion of the handled personal information contents.

#3 Regarding "notification to the data subject", see 1. (7).

<Examples of not requiring correction>

Case) When the subject of correction, etc. is not a fact but information related to evaluation

4) Cessation of handled personal information (Article 27)

Paragraph 1, Article 27

An entity handling personal information must cease or delete (hereinafter called "cease, etc.") without delay the use of handled personal information that can identify the data subject, when demand to cease, etc., is made on grounds that the said personal information is being handled in violation of the provisions of Article 16 or obtained in violation of the provisions of Article 17, provided that action is within the scope necessary to rectify the violation. However, this shall not apply if huge expenses are necessary for cessation, etc., of the use of the information in question or if there are other reasons that make cessation, etc., difficult to implement and if alternative measure is to be implemented for the protection of the rights and interests of the data subject.

Paragraph 2, Article 27

An entity handling personal information must cease without delay availability to a third party of handled personal information that can identify the data subject, if the data subject seeks cessation of availability of the said handled data to a third party on grounds that the said data is being made available to the third party in violation of provisions of Paragraph 1, Article 23, and if the claim is substantiated. However, this shall not apply if huge expenses are necessary for

cessation of availability or if there are other reasons that make cessation difficult to implement and if alternative measure is to be implemented for the protection of the rights and interests of the data subject.

Paragraph 3, Article 27

An entity handling personal information must notify the data subject of handled personal information without delay of the decision to cease, etc., or not to cease, etc., the use of all or part of handled personal data, implemented in compliance with provisions of Paragraph 1, or of the decision to cease, etc., or not to cease, etc., availability of all or part of handled personal information to a third party, implemented in compliance with provisions of the preceding paragraph.

If the subject of the handled personal information seeks cessation, etc., (#2) of data use on grounds of procedural violation (#1), the entity handling personal information must implement appropriate measure as a general rule (#3). In case of cessation, etc., of data use, the said enterprise must notify the data subject (#4) to this effect. (excluding 1.(4) #Handling of telephone directory, car navigation systems, etc.)

#1 "Procedural violation" is defined as data use other than the designated purpose without consent, illegal access to data or availability of data to third party without consent.

#2 "Cessation, etc., of use" is defined as cessation of use, deletion or cessation of availability of handled personal information to third parties.

#3 "General rule": Data use need not be ceased, etc., if demand exceeds the limits of action necessary for rectifying the violation or when claim of procedural violation is inaccurate. However, the data subject must be notified in such a case, without delay, that use will not be ceased, etc.

#4 Regarding "notification to data subject," see 1.(7).

5) Explanation of reason (Article 28)

Article 28

In the case of an entity handling personal information notifying the data subject of handled personal information of full or partial non-implementation of measure required by the said data subject or of measure different from the one specified, in compliance with Paragraph 3 of Article 24, Paragraph 2 of Article 25, Paragraph 2 of Article 26 or Paragraph 3 of the preceding article, the said enterprise must explain the reason to the data subject.

An entity handling personal information must explain to the data subject the reason for non-implementation of disclosure, public announcement, revision, cessation of use, etc., of handled personal information or of the reason for implementing a different measure, when notifying the data subject of such action (#).

Regarding "notification to data subject," see 1. (7).

6) Procedure implemented in response to demand for disclosure, etc. (Article 29)

Paragraph 1, Article 29

An entity handling personal information shall be able to establish the method for accepting demand in compliance with provisions of Paragraph 2 of Article 24, Paragraph 1 of Article 25, Paragraph 1 or Paragraph 2 of Article 26 or Paragraph 1 or Paragraph 2 of Article 27 (hereinafter referred to in this article as "demand for disclosure, etc.") as designated by ordinance. In such a case, the data subject must demand disclosure, etc., in compliance with the established method.

Paragraph 2, Article 29

An entity handling personal information shall be able to demand the data subject of the handled personal information to present information items necessary to identify the handled personal information in question. In such a case, the said entity must implement appropriate measure with attention to convenience of the data subject, including presentation of information contributing to identification of the handled personal information and question, in order to enable the data subject to demand disclosure, etc., easily and precisely.

Paragraph 3, Article 29

Demand for disclosure, etc., may be submitted by proxy, in compliance with provisions of the ordinance.

Paragraph 4, Article 29

An entity handling personal information must pay due attention to avoid imposing excessive load on the data subject, when defining the procedure for accepting demand for disclosure, etc., based on provisions of the three preceding paragraphs.

Ordinance Article 7

The items that an entity handling personal information may be able to define when accepting demand for disclosure, etc., in compliance with Paragraph 1, Article 29 of the Law shall be the

following.

1. The party requesting disclosure, etc.
2. Format for documents to be submitted in writing (including records produced electronically, magnetically, or with any other method in which data cannot be recognized by the human senses) in demand for disclosure, etc.
3. Method of authenticating the party demanding disclosure, etc., or proxy specified by the following article.
4. Method of collecting handling charge described in Paragraph 1, Article 30 of the Law.

Ordinance Article 8

Proxy able to demand disclosure, etc., under provision of Paragraph 3, Article 29 of the Law shall be either of the following.

1. Legal proxy of underage or incompetent person
2. Proxy designated by the data subject to demand disclosure, etc.

(a) An entity handling personal information is able to define items i-iv below in the method of accepting demand for disclosure, etc. (#1) Moreover, the method established requires information to be made accessible by the data subject (including instances in which response is made to demand by the data subject without delay). (#2) (See (5)1.) Also, the entity handling personal information shall be able to deny disclosure, etc., if the said entity has established a method of accepting demand for disclosure, etc., in a rational framework and the party making the demand does not comply with the method.

#1 "Demand for disclosure, etc." is defined as demand for notification of the purpose of use of handled personal data, for disclosure of handled personal data, for revision, addition or deletion of items in handled personal data, for cessation or cancellation of use of handled personal data or for cessation of availability of handled personal data to third parties.

#2 See 1.(12) for state in which "information [is] to be made accessible by the data subject (including instances in which response is made to demand by the data subject without delay).

i. Body to accept demand for disclosure, etc.

ii. Format of documents to be submitted in making demand for disclosure, etc. (including records produced electronically, magnetically, or with any other method in which data cannot be recognized by the human senses) and other methods of accepting demand for disclosure, etc. (such as acceptance by mail, fax, etc.).

iii. Method of authenticating identity of the party demanding disclosure, etc., as the data

subject or the subject's proxy ((a) legal proxy for under age or incompetent person or (b) proxy appointed by the data subject in submitting demand for disclosure, etc.). (However, the method of authentication must be appropriate in accordance with the nature of the business operation involved, conditions in which personal information is handled, and method of accepting demand for disclosure, etc.)

Example 1: Authentication in case of demand by data subject in person (personal visit) -- driver's license, health insurance beneficiary certificate, resident registry card with photo, passport, alien registration certificate, pension passbook, certificate of seal and official seal

Example 2: Authentication in case of demand by data subject (online) -- ID and password

Example 3: Authentication in case of demand by data subject (telephone) -- designated registered data (such as birth date) and callback

Example 4: Authentication in case of demand by data subject (by mail, fax, etc.) -- copy of driver's license or resident registry

Example 5: Authentication in case of demand by data subject (by mail, fax, etc.) -- copy of official certificate such as driver's license, health insurance beneficiary certificate, etc., to be sent from the customer, etc., and mailing of document by registered mail to the address of the customer, etc., shown on the official certificate receipt.

Example 6: Authentication in case of demand by proxy (personal visit) -- driver's license, health insurance beneficiary certificate, passport, alien registration certificate or pension passbook for data subject and proxy, as well as attorney license number in case of attorney and letter of proxy certifying designation as proxy by the data subject.

iv. Method of collecting charges for issuing notice on purpose of use of handled personal information and for disclosure of handled personal information

If method of accepting demand for disclosure, etc., is not specified, applications must be accepted freely.

(b) In order to facilitate the procedure for disclosure, etc., an entity handling personal information shall be able to request the data subject to make available information items necessary in specifying personal data (such as address, ID, password, membership number, etc.). In order to specify the data subject's own data easily, the said subject must provide information that facilitates identification of the subject's own personal information for the subject's own convenience.

(c) In establishing the procedure for accepting demand for disclosure, etc., an entity handling personal information must pay due attention to avoid imposing excessive load on the data subject when making such a demand, such as requiring presentation of troublesome documentation beyond what is necessary, specifying location that is unnecessarily inconvenient, separate from

the location of business operation, as the site for accepting such demands, etc.

7) Handling Charges (Article 30)

Paragraph 1, Article 30

An entity handling personal information shall be able to collect charges for execution of action in response to demand for notice on the purpose of use of personal data under provisions of Paragraph 2, Article 24, or to demand for disclosure under provisions of Paragraph 1, Article 25.

Paragraph 2, Article 30

An entity handling personal information must establish fixed charges within the range recognized as rational vis-à-vis real expenses, when collecting charges under the provisions in the preceding paragraph.

An entity handling personal information shall be able to establish fixed charges for measures taken in response to demand for notice on the purpose of use of handled personal data or to demand for disclosure of handled personal data. When handling charges are established, the information must be made accessible by the data subject (including cases in which response is made to the demand of the data subject without delay) (#). (See (5) 1)).

When collecting charges, the charges must be fixed within the range recognized as rational vis-à-vis real expenses. (See (5) 1)(a)iii.)

See 1. (12) for state in which "information [is] to be made accessible by the data subject (including cases in which response is made to demand by the data subject without delay).

(6) Handling of grievances (Article 31)

Paragraph 1, Article 31

An entity handling personal information must exert effort for swift and appropriate handling of grievances related to handling of personal information.

Paragraph 2, Article 31

An entity handling personal information must develop an organization necessary to realize the objective described in the preceding paragraph.

An entity handling personal information must exert effort into swift and appropriate handling of grievances related to personal information handling. Also, in executing swift and appropriate handling of grievances, the entity must work on development of an organization in charge of grievances handling, establishment of procedure for grievance handling, etc. However, the entity need not cater to irrational demands.

In development in grievance handling organization, JIS Z9920 "Guidelines on Grievance Handling Management System" may be used as reference.

(7) Transitory Action (Articles 2-5 of Miscellaneous Rules in the Law)

(Transitory action related to consent of the data subject)

Article 2

If a data subject has given consent to handling of the subject's personal information prior to enforcement of the Law and if the said consent is equivalent to consent to handling said personal information for purposes other than the specified purpose of use under provisions of Paragraph 1, Article 15, this shall be interpreted as consent as described in Paragraph 1 or 2, Article 16.

Article 3

If a data subject has given consent to handling of the subject's personal information prior to enforcement of the Law and if the said consent is equivalent to consent to granting availability of the said personal information to third parties under Paragraph 1, Article 23, this shall be interpreted as consent as described in the said paragraph.

(Transitory action related to notice)

Article 4

If notice is issued to a data subject regarding items comparable to items that must be made easily accessible for the data subject under provisions of Paragraph 2, Article 23, prior to enforcement of the Law, the said notice shall be deemed issued under provisions of the said paragraph.

Article 5

If notice is issued to a data subject regarding items comparable to items that must be made easily accessible to the data subject under Item 3, Paragraph 4, Article 23, prior to enforcement of the Law, the said notice shall be deemed issued under provisions of the said item.

"Consent of a data subject" in (1)(c), (1)(d) and (4)(a) is defined as consent in compliance with the Law, even when issued prior to enforcement of the Law.

Also, "notice to a data subject" in (4)(b) and (4)(c)iii is defined as notice issued to the data subject in compliance with the Law, even when issued prior to enforcement of the Law.

Also, provisions of Article 18 (Notice, etc., on objective of use at acquisition of information) shall not apply to personal information handled prior to enforcement of the Law, since personal information acquisition did not take place at enforcement. (See (2)(b).) However, action described in Paragraph 1, Article 24, must be executed at enforcement for notification of the data subject on items regarding handled personal data. (See (5) 1)(a).)

3. Handling of Personal Information at Research Institutes, Etc., of Private Organizations

Item 3, Paragraph 1, Article 50

The provisions of the forgoing chapter shall not apply to any one of the following entities belonging in the category of entities handling personal information, if all or part of the purpose of handling personal information is described in the corresponding item.

3. Organization or entity belonging to a university or any other institution aimed at academic research – Purpose contributing to academic research

Although there are situations in research activities at research institutes, etc., of private organizations in which personal information is handled, the Law shall not apply under Item 3, Paragraph 1, Article 50, if this is done for the purpose of academic research by the said organization and if such activity contributes to academic research. For this reason, the principles under Item 3, Paragraph 1, Article 50, of the Law are organized here regarding research institutes, etc., of private organizations in the economic and industrial sectors, engaged in research activities involving personal information handling.

Organizations that bear the name of "research Institute" or "laboratory," such as research Institutes of private business enterprises, that are engaged in product development cannot be regarded and operation aimed at academic research. For this reason, they do not fall in the category of "organization or institutions aimed at academic research" under the Law.

Principles under Item 3, Paragraph 1, Article 50

"University or any other institution aimed at academic research" defined in Item 3, Paragraph 1, Article 50, is defined as an institution whose principal objective is academic research (discovery, analysis or establishment of methodology of new laws and principles, systematization of new knowledge or its method of application, exploration of cutting-edge academic disciplines, etc.).

At such an institution, if academic research accounts for all or part of the objective of handling personal information, such an institution shall not be obliged to fulfill the obligations of an entity handling personal information.

<Exemption from the Law>

Example: Research institute of an organization engaged primarily in academic research, in which academic research accounts for all or part of the objective for handling personal information.

<Non-exemption from the Law>

Example 1: Research institute of an organization engaged primarily in academic research, in

which personal information is used exclusively for the purpose of analyzing product development data (excluding academic research purposes).

Example 2: Research institute of an organization whose principal objective is not academic research.

C. Principles of "recommendation," "order" and "emergency order"

Paragraph 1, Article 34

If the competent Minister recognizes the need to protect the rights and interests of a private individual in case of violation of provisions of Articles 16 through 18, Articles 20 through 27 or Paragraph 2, Article 30, by an entity handling personal information, the said Minister shall be able to issue recommendation to the said entity to terminate said violation or to take other necessary action to rectify the violation.

Paragraph 2, Article 34

If the competent Minister recognizes serious infringement of the rights and interests of a private individual due to failure of the entity handling personal information, which had been issued recommendation in compliance with provisions of the foregoing Item, to take appropriate action and without justifiable reason, the said Minister shall be able to order execution of measure pertaining to the recommendation against the said entity.

Paragraph 3, Article 34

If the competent Minister recognizes the need to take urgent action in face of evidence of serious infringement of the rights and interests of a private individual by an entity handling personal information, in violation of Article 16, Article 17, Articles 20 through 22 or Paragraph 1, Article 23, notwithstanding provisions of the two foregoing paragraphs, the said Minister shall be able to order execution of action to terminate the said violation or other action to rectify the violation.

Article 56

Entities committing violation of order under provisions of Paragraph 2 or Paragraph 3 of Article 34 shall be sentenced to imprisonment of six months or less or punitive payment of 300,000 yen or less.

Paragraph 1, Article 58

In case of violation of the provisions of the two foregoing articles by a representative of an incorporated entity (including unincorporated entities which have provisions for representatives or managers; hereinafter the same for the Paragraph), a proxy of an individual or incorporated entity, or an employee or worker at such an entity against the business operation of the said individual or entity, penalty or fine based on the said articles will be imposed on the violator, as well as the incorporated entity or individual.

Paragraph 2, Article 58

In case of application of provisions of the foregoing paragraph on an entity that is not incorporated, the representative or manager of the said entity shall represent the unincorporated entity in litigation, and provisions of laws related to criminal litigation shall apply if the incorporated entity is a suspect or defendant.

"Recommendation (Paragraph 1)," "order (Paragraph 2)" and "emergency order (Paragraph 3)" by the Minister of Economy, Trade and Industry under Article 34 are based on decision on whether or not the entity handling personal information has implemented necessary measures, etc., along the Guidelines.

In other words, failure to comply with provisions that are defined as compulsory in the Guidelines can be judged as violation of provisions from Articles 16 through 18, Articles 20 through 27 or Paragraph 2, Article 30. If judged as violation, a "recommendation" is issued when deemed necessary to protect the rights and interests of an individual. In case of failure to comply with provisions that are defined as "preferable" in the Guidelines, on the other hand, it may not be judged violation of provisions from Articles 16 through 18, Articles 20 through 27 or Paragraph 2, Article 30. However, action by entities handling personal information is preferred from the standpoint of promoting protection of personal information.

An "order" is issued not simply with failure to comply with a "recommendation" but only when serious infringement of rights and interests of an individual is likely in case of failure to take action pertaining to the recommendation and without justifiable reason. In order to establish whether or not the party in question has complied with the "recommendation," the Minister of Economy, Trade and Industry is to issue "recommendation" establishing the period of time during which action should be taken.

An "emergency order" is issued without a "recommendation" in case of violation of Article 16, Article 17, Articles 20 through 22 or Paragraph 1, Article 23, by an entity handling personal information and when action must be taken urgently due to evidence of serious infringement of rights and interests of an individual.

In order to establish whether or not the party in question has complied with an "order" or "emergency order," the Ministry of Economy, Trade and Industry is to issue an "order" or "emergency order" defining a period of time during which action should be taken. If action is not taken during the said period, penalty (Articles 56 & 28) shall apply.

D. Review of Guidelines

The principles of personal information protection evolve with changes in social conditions,

public awareness, technological advances, etc. Effort will be directed to annual review of the Guidelines after enforcement, in face of changes in the social environment and other conditions.

E. Reference Items and Standards in Appropriate and Effective Execution of Obligations, etc., by Entities Handling Personal Information

An entity handling personal information should preferably develop, implement, maintain and update a compliance program for personal information protection, corresponding to the scale of its business operation and activity.

In developing such a scheme, JIS Q 15001 "Requirements of a Compliance Program on Personal Data Protection" may be used as reference. In executing security management measures for personal data, JIS X 5070 "Security Technologies: Evaluation Standards for Information Technology Security" and JIS X 5080 "Model for Information Security Management Implementation" may be used as reference.

An entity handling personal information may publish "a declaration on policy and principles in personal information protection (such as privacy policy, policy statement, etc.) employing the following items as reference and announce it publicly by means of publication on the Web, etc.

(a) Items related to appropriate handling of personal information with attention to content and scale of business operation

i. Objective of use of personal information acquired (Article 18)

ii. <In case of making personal information available to third parties without consent of the data subject> (Paragraphs 2 & 3, Article 23)

* Availability to third party to be included in objective of use

* Personal data items to be made available to third parties

* Means and methods of making information available to third parties

* Cessation of availability to third parties, in response to requests from data subject

iii. <In case of shared use> (Paragraphs 4 & 5, Article 23)

* Evidence of shared use with designated parties

* Personal data items to be shared

* Range of parties designated for shared use

* Objective of shared use by designated parties

* Name or title of person responsible for personal data management among parties designated for shared use

iv. Items related to handled personal data (Article 24)

* Name and title of individual

* Objective of use of all handled personal data

* Procedure in responding to "demand for disclosure, etc." (when so designated)

* Fixed handling charges pertaining to disclosure or notice of objective of use of handled personal data (when so designated)

* Body to accept grievances (including name of body for resolving disputes and name of relevant designated personal information production organization, if the entity in question belongs to a

designated personal information protection organization)

v. Items related to procedure for responding to demand for disclosure, etc. (Article 29)

* Application form format (when so designated)

* Method of acceptance (when so designated)

* Presentation of information useful in identifying handled personal data

vi. Items related to body accepting inquiries and grievances (Paragraph 5, Article 23; Paragraph 1, Article 24; Paragraph 1, Article 29; and Article 31)

(b) Compliance with laws and regulations related to protection of personal information

(c) Items related to personal information security management measures

(d) Items related to continuous update and improvement of compliance program

"Entity belonging to a designated personal information protection organization" is an entity handling personal information which is member of a designated personal information protection organization or entity with contractual relations with such an organization under which the organization is to handle grievances, etc.