

**HANDBOOK**  
**CONCERNING PROTECTION OF PERSONAL**  
**DATA**

**February 1998**

**Ministry of International Trade and Industry**  
**(MITI)**

## I. Background and History of the Handbook

1. The extraordinary development of information processing technology in recent years has made it possible for computers to process large amount of information rapidly, which has in turn made it easier to develop business activities that efficiently respond to diversifying needs and individualization in areas like consumer credit (loans to individuals) and direct marketing. However, personal information is also collected and accumulated without the knowledge of the person concerned and used for purposes unexpected by him. In light of this, there has been interest throughout society concerning appropriate protection of personal data, and many efforts to this end have been initiated.

In April 1989, the Ministry of International Trade and Industry finalized a document entitled "Concerning the Protection of Computer Processed Personal Data in the Private Sector (Guidelines)" as a report from the Personal Data Protection Subcommittee of the Computerization Countermeasures Committee, an advisory group of the Director General of the Machinery and Information Industries Bureau. The Subcommittee also authorized the "Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector," which were formulated in 1988 by the Japan Information Processing Development Center, and published them to a wide spectrum of interested organizations. In conjunction with this, on June 28, 1989 the Ministry issued a notification to interested organizations instructing them to formulate their own guidelines based on the Subcommittee's guidelines.

On July 7, 1989, the Minister of International Trade and industry issued a notification on "The Rule on the Registration concerning the Measures, etc. for the Protection of Computer Processed Personal Data" under which a "The institution of registration list for protection of personal data" was established to register outlines of measures for the protection of personal data implemented by enterprises and business organizations. Twelve organizations registered.

2. However, between the extraordinary progress in information processing technology and trends such as "downsizing" and "end user computing," personal data is being accumulated and used in a more decentralized fashion. No longer is personal data handled only in high-volume, formalized processing by large main-frame computers, it may also be handled by the computer systems of a much wider range of enterprises, including small and medium-sized enterprises. This has produced a growing risk that data will be improperly used, altered, and processed by those lacking proper authorization. There have been scattered cases of personal data being leaked, and these incidents have helped to increase anxiety over personal data protection, which has in turn caused consumers to seek stronger measures for the protection of personal data.

In addition, open computing networks are developing around the world, as the explosive expansion of the Internet demonstrates. Once on the networks, personal data can instantaneously be distributed to a wide range of parties, often beyond national borders, which raises the potential for much larger cases of personal data infringement to be seen and a need for international harmonization of personal data protection measures.

3. Other developed countries have long had personal data protection laws on their books, many of which were revised to conform with the "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" issued by the Organization for Economic Co-operation and Development (OECD) in 1980 (often referred to

as the "OECD Privacy Guidelines"). As information technology is developed, individual countries have also initiated new efforts to strengthen personal data protection.

The EU in particular issued "Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (which we will refer to as the "EU Directive"). Under the EU Directive, countries in the region are asked to enact legislation within three years that will bring their

national laws and ordinances into conformance with the standards set in the Directive. Among the measures in the Directive are a ban on the transfer of personal data to third countries if third countries do not offer an adequate level of protection, and provisions for negotiations with third countries deemed not to offer the adequate level of protection by the EU Committee. Therefore, in Japan, it is requested to ensure the "adequate level of protection"

4. In light of these developments, the Ministry of International Trade and Industry organized in 1995 a "Working Group on Privacy Issues" (Chairman: Masao Horibe, then-Professor at Hitotsubashi University) as a research committee for the Director General of the Machinery and Information Industries Bureau. The Working Group was charged with revising the abstract 1989 Guidelines so that they were more specific, detailed, and concrete, studying ways to supplement the voluntary efforts of private enterprises, and considering measures to enhance liaison functions in dealing with complaints from consumers (data subjects). In April 1996, the Working Group completed its first draft of the Revised Guidelines. These guidelines were revised so as to better reflect the actual business activities engaged in by Japanese enterprises and international trend like the adoption of EU Directive.

In May 1996, explanatory meetings and hearings on the first draft began to be held for interested organizations, including the twelve business organizations that had registered with the Ministry of International Trade and Industry, industries providing personal services (for example, marriage introduction services and private "cram schools"), and local governments. In December 1996, the Ministry of International Trade and Industry solicited the opinions of the general public through the Official Gazetteer and its Internet web site.

This process led to the publication of "Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector" (Ministry of International Trade and Industry Notification No. 98 of March 4, 1997).

5. As was the case with the 1989 guidelines, the Ministry of International Trade and Industry expects that the Revised Guidelines will be used by interested business organizations and their member enterprises to create voluntary rules for personal data protection, and has engaged in publicity and educational activities to that end. Unfortunately, cases of personal data leakage have occurred since the publication of the guidelines.

The primary factor in this is probably that, compared to 1989, there has been extraordinary progress in information technology that has greatly expanded the range of enterprises handling personal data and increased their processing volumes. The Ministry of International Trade and Industry has therefore created and distributed to a wide range of interested parties a "Personal Data Protection Handbook" that explains the Revised Guidelines, using concrete examples to illustrate points of importance in personal data protection policies and providing greater detail on the policies and programs that should be put in place by enterprises handling personal data. The Ministry of International Trade and Industry expects this Handbook to be used not only by enterprises but by consumers, researchers, and a wide range of the general public. It is hoped

- that in doing so we will deepen awareness of the importance of personal data protection.
6. Furthermore, in the future, it is feared to occur the friction and trouble between enterprises and consumers. MITI thinks that it is possible to utilize the Revised Guidelines and this Handbook as one of the criterion so as to resolve such friction and trouble. It is hoped that friction and trouble will be resolved smoothly, when they are utilized in the judicial organizations, consultation services, and other organizations.
  7. The adequate protection of personal data would not be realized without endeavors of enterprises, consumers, administrative organs, and other organizations. MITI wishes this Handbook helpful for the endeavors of persons concerned which intend to improve the level of protection.

## II. Personal Data Protection Handbook

This Handbook provides more detailed explanations of the "Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector" (Ministry of International Trade and Industry Notification No. 98 of March 4, 1997).

### Table of Contents

#### Chapter 1 Purpose of the Guidelines

##### Article 1 Purpose

#### Chapter 2 Definitions

##### Article 2 Definitions

#### Chapter 3 Scope of Application of Guidelines

##### Article 3 Personal Data to which Guidelines Apply

##### Article 4 Extension of Guidelines

#### Chapter 4 Measures Concerning Collection of Personal Data

##### Article 5 Limitation on Collection of Personal Data

##### Article 6 Limitation on Methods of Collection

##### Article 7 Prohibition against Collection of Specific Personal Data of a Delicate Nature

##### Article 8 Measures for Collection of Personal Data Directly from Data Subject

##### Article 9 Measures for Indirect Collection of Personal Data Other than from Data Subject

#### Chapter 5 Measures Concerning Use of Personal Data

##### Article 10 Limitation on Use of Personal Data

##### Article 11 Measures for Use of Personal Data within the Scope of the Purpose

##### Article 12 Measures for Use of Personal Data beyond the Scope of the Purpose

#### Chapter 6 Measures Concerning Disclosure of Personal Data

##### Article 13 Limitation on Disclosure of Personal Data

##### Article 14 Measures for Disclosure of Personal Data within the Scope of the Purpose

##### Article 15 Measures for Disclosure of Personal Data beyond the Scope of the Purpose

#### Chapter 7 Obligation to Manage Personal Data Properly

##### Article 16 Ensuring the Accuracy of Personal Data

##### Article 17 Ensuring Security in Use of Personal Data

##### Article 18 Obligation of Employees to Maintain Confidentiality of Personal Data

##### Article 19 Measures Concerning Entrustment of Personal Data

#### Chapter 8 Rights of Data Subject Concerning Data Regarding Self

##### Article 20 Rights Concerning Own Personal Data

Article 21 Right to Refuse Use or Disclosure of Own Personal Data  
Chapter 9 Organization and Implementation Accountability  
Article 22 Designation of Manager by the Representative  
Article 23 Duties of Manager  
Chapter 10 Other Provisions  
Article 24 Notification when Magnetically-Stored Records are Transmitted and Received  
Using Communication Networks

## **Chapter 1 Purpose of the Guidelines**

### Article 1. Purpose

The purpose of these guidelines is to protect adequately personal data handled by enterprises in the private sector. These guidelines help business organizations to establish guidelines for each industry sector according to the status of the operations of member enterprises, with a view to supporting and promoting the enterprises' establishment of a compliance program aimed at protecting personal data according to the activities of enterprises.

#### < Explanation >

1. "Concerning the Protection of Computer Processed Personal Data in the Private Sector (Guidelines)" (April 1989 report of the Personal Data Protection Subcommittee of the Computerization Countermeasures Committee, Ministry of International Trade and Industry; "the Old Guidelines" hereinafter) did not articulate a purpose.  
However, the Ministry of International Trade and Industry found in its reviews of personal data protection policies that there is a growing awareness of personal data protection among private enterprises as well as business organizations, and in as much as one of the purposes of the guidelines is to promote appropriate personal data protection, this Article was added as clarification.
2. This Article articulates two stages of appropriate personal data protection: the formulation of guidelines for specific industry sectors by business organizations based on the "Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector" (Ministry of International Trade and Industry Notification No. 98 of March 4, 1997; "these Guidelines" hereinafter) and reflecting conditions within their sectors ("Industry Guidelines" hereinafter), and the formulation of Compliance Programs for the protection of personal data by individual enterprises based on Industry Guidelines and reflecting their own business activities.
3. Should a single enterprise do business in more than one sector, it should consult all relevant Industry Guidelines and formulate a Compliance Program that articulates personal data protection policies that adequately take into account all relevant Industry Guidelines and are appropriate for the enterprise's activities.  
Enterprises that are not members of business organizations should refer to these Guidelines in formulating appropriate personal data protection policies.
4. Compliance Programs need not be written in the same legalistic style as these Guidelines. They should describe policies in the way that is easiest for those involved to understand and best reflects the nature of the enterprise.  
Compliance Programs also do not need to be formulated separately. For example, they could be part of work manuals or rules of employment. Likewise, a single enterprise may create multiple Compliance Programs (for example, one for each business division).  
Note that there may be cases where there is the regulation by law and ordinances concerning personal

data protection, or cases where relevant ministries and agencies supervising business done by the enterprise concerned may have already published guidelines on personal data protection. In such cases, these regulations and guidelines should be consulted in the formulation of Compliance Programs.

## **Chapter 2 Definitions**

### Article 2. Definitions

For the purposes of these guidelines, the meaning of the terms set forth in the following subparagraphs shall be provided for in the said subparagraphs.

(1) The term "personal data" means data which relate to an individual, and ones that the individual can be identified from name, date of birth or other descriptions or from number, symbol, other mark, image or sound assigned to the individual contained in the data (including data that the individual can not be identified only from the data, but be identified by easily collating with other data). They exclude, however, such data concerning directors of a corporation or other organization as contained in the data recorded with regard to the corporation or other organization.

(2) The term "manager" means a person designated by the representative of enterprises who has authority to determine the purpose, method, etc. of collection, use and disclosure of personal data.

(3) The term "recipient" means a person or an enterprise that personal data are disclosed to.

(4) The term "consent of data subject" means the declaration of intent, by the data subject, to give consent to the handling of personal data concerning him through an explicit response given through a signed and sealed statement or oral agreement. However, in the case of actions including transactions, applications, subscriptions, etc. not associated with contract procedures through the issue of documents, etc. this shall include the tacit declaration of intent, in which opposition is not expressed, given in the procedures associated with the actions.

### < Explanation >

1. The Old Guidelines only define the term "personal data," but these Guidelines, reflecting the points made in the EU Directive, have been revised for greater specification and detail and therefore define other necessary terminology.
2. Subparagraph (1), "Personal data": The definition is more detailed than in the Old Guidelines and corresponds almost exactly to the definition of personal data found in the "Act for the Protection of Computer-Processed Personal Data Held By Administrative Organs" (Law No. 95 of December 1988; the "Personal Data Protection Act" hereinafter) and "The Rule on the Register concerning the Measures, etc. for the Protection of Computer Processed Personal Data" (Ministry of International Trade and Industry Notification No. 348 of July 7, 1989; abolished on March 3, 1997 with the formulation of these Guidelines). However, we have added the concept

of "ones that the individual can be identified from image or sound" to reflect recent technological advances.

"Number assigned to the individual" refers to telephone numbers, bank account numbers, insurance policy numbers and the like. "Data concerning directors of a corporation or other organization" refers to publicly disclosed information, for example, information on the careers and numbers of shares held by directors printed in business reports distributed at general meetings of shareholders or on documents made available to shareholders and customers.

3. Subparagraph (2), "Manager": This is a concept that was not in the Old Guidelines. The purpose for including it in these Guidelines is to clearly define those within enterprises who are responsible for the appropriate management of personal data and to delineate their responsibilities (see also Chapter 9; and see Article 8, Article 18, and Article 19).
4. Subparagraph (3), "Recipient": In contrast to those providing data, this refers to those that directly or indirectly personal data are disclosed to. "Recipient" is a concept that was not found in the Old Guidelines, but was newly defined in order to ensure transparency in the handling of personal data (see also Article 8, Article 14, Article 15, and Article 20).
5. Subparagraph (4), "Consent of data subject": In principle the consent of the data subject is required for the collection and use of personal data. This definition was added to this Article to clarify the methods by which consent is given (see also Article 7, Article 8, Article 9, Article 11, Article 12, Article 14, and Article 15).  
 "Transactions, applications, subscriptions, etc. not associated with contract procedures" refers to catalog sales, applications for electricity, gas, and other utility services, and applications for drawings, prizes, and the like.
6. Below is a comparison of the terms defined in: "the EU Directive (1)," "the OECD Guidelines (2)," "the Personal Data Protection Act (3)," "the Old Guidelines (4)," and "these Guidelines (5):"

	(1)	(2)	(3)	(4)	(5)
Personal data					
Personal data filing systems (files)					
Processed information					
Subject of processed information					
Manager					
Processor					
Third party					
Recipient					
Consent (of data subject)					
Processing (use) (of personal data)					
International distribution (of personal data)					

< References >

- EU Directive, Article 2
- OECD Guidelines No. 1

- Old Guidelines, Article 1
- Personal Data Protection Act, Article 2

### **Chapter 3 Scope of Application of Guidelines**

#### Article 3. Personal Data to which Guidelines Apply

These guidelines shall apply to personal data processed, either wholly or in part, using electronic computers, optical information processing devices or other automatic processing systems within enterprises, including personal data processed in document form for the purpose of processing by an automatic processing system. This shall not apply, however, to personal data collected by an individual for personal uses.

#### < Explanation >

1. Computers and other automatic processing systems process personal data very quickly and in very large volumes, which gives them vastly more potential to infringe on the interests of the individual than manual processing (hand processing). In light of this, the personal data covered by these Guidelines is basically that processed by computers and other automatic processing systems.
2. However, these Guidelines also cover manually processed personal data when it is associated with automatic processing, for example, data collected and stored for input into automatic processing systems and data output from automatic processing systems for use in addressing. This is done because such data also has a high potential to infringe on personal interests just as data processed entirely by automatic processing systems. The same intention can be found in Article 3:1 of the EU Directive. It was not directly articulated in Article 1 of the Old Guidelines, but was noted in the explanatory materials.
3. However, these Guidelines do not cover personal data collected by individuals for personal use, for example, a personal address book. Note that personal data collected by individuals is covered by these Guidelines when said individuals appear to be employees of specific enterprises.

#### < References >

- EU Directive, Article 3:1
- Old Guidelines, Article 1

#### Article 4. Extension of Guidelines

Provisions to these guidelines may be added or revised according to the activities of the industry sector or enterprises in so far as these additions or revisions are in line with the purpose of adequately protecting personal data.

< Explanation >

1. As stated in Article 1, one of the purposes of this review of personal data protection policies is to encourage business organizations to formulate Industry Guidelines and enterprises to formulate Compliance Programs so as to increase the awareness of personal data protection within enterprises as well as within business organizations.
2. These Guidelines articulate general matters necessary for the adequately protecting personal data regardless of the specific characteristics of individual industrial sectors. To increase the effectiveness with which personal data is protected, Industry Guidelines and Compliance Programs based on these Guidelines should add or revise provisions according to the activities of their specific industries or enterprises, and these Guidelines in no way prevent them from doing so. The same intention can be found in OECD Guidelines No. 6. It should be underscored that revisions must only be for the formulation of highly effective Industry Guidelines and Compliance Programs that are in line with actual business conditions. They shall not allow any reduction in the level of protection afforded personal data.

< References >

- OECD Guidelines No. 6

## **Chapter 4 Measures Concerning Collection of Personal Data**

Article 5. Limitation on Collection of Personal Data

The collection of personal data shall specify clearly the purpose of the collection within the limit of legitimate business of enterprises and shall be conducted to the extent necessary to achieve the purpose.

< Explanation >

1. Chapter 4 formulates principles for the collection of personal data. These Guidelines, like the Old Guidelines, correspond to the "Collection Limitation Principle" and the "Purpose Specification Principle" defined on the "Eight Principles of the OECD Guidelines." [Note] This Article in these Guidelines is the same as the first half of Article 2:1 of the Old Guidelines.
2. "Legitimate" business intends to exclude antisocial business activities.
3. Specification of the purpose of collection shall take the following into account:
  - (1) When data is collected from the subject himself, there must be an assent to the collection in contracts etc. signed by the subject; or there must be an assent in a contract-like relationship of trust with the subject.
  - (2) When data is collected from someone other than the subject, the collector of the information must set the purpose of collection and must clearly state it in contracts etc. with the person from whom data is collected.

- (3) When data is collected from publicly-available documents, the collector of information must still set clear purposes for collection.
- (4) In setting purposes of collection, collectors shall be as specific and clear as possible about the scope of data use and disclosure so that it is possible to anticipate the influence of use and disclosure of collected data on the data subject.

< Note >

The OECD Guidelines delineate eight principles: the "Collection Limitation Principle," the "Data Quality Principle," the "Purpose Specification Principle," the "Use Limitation Principle," the "Security Safeguards Principle," the "Openness Principle," the "Individual Participation Principle," and the "Accountability Principle."

< References >

- EU Directive, Article 6:1(b)
- OECD Guidelines No. 7 and No. 9
- Old Guidelines, Article 2(1)

Article 6. Limitation on Methods of Collection

The collection of personal data shall be conducted by lawful and fair means.

< Explanation >

1. This Article corresponds to Article 2(2) of the Old Guidelines.
2. Personal data is to be collected by "lawful and fair means." Collection by unfair means, for example, falsification of the purpose of collection, will not be tolerated.

< References >

- EU Directive, Article 6:1(a)
- Old Guidelines, Article 2(2)

Article 7. Prohibition against Collection of Specific Personal Data of a Delicate Nature

Personal data which include the following types of data shall not be collected, used or disclosed. This shall not apply, however, in the case where the data subject has given explicit consent to the collection, use or disclosure of the data, or where there are special provisions in laws, or where it is necessary for the judicial procedures to collect, use or disclose the data.

- (1) Race or ethnicity
- (2) Family origin or legal domicile (not including data relating to prefectures of current residence)
- (3) Religion (including ideology and beliefs), political opinions or trade-union membership
- (4) Health, medical treatment or sex life

< Explanation >

1. There are two primary methods of restricting the collection of personal data from the perspective of data subject: restricting the type and nature of the data that can be collected, and specifying the purposes of collection. The Old Guidelines used only the former method of restriction (Article 2), but these Guidelines use both methods. This is done to strengthen protection of the rights of the data subject, respond to domestic problems, and harmonize with Article 8 of the EU Directive. This Article was therefore added to these Guidelines as a means of restricting the type and nature of data collected. (Article 5 contains provisions for the latter method of restriction).
2. Subparagraph (2), "Legal domicile": A prohibition on all collection of data on personal domiciles would risk impairing businesses that need to verify personal identities. The collection of more precise data than the prefectural level is therefore prohibited in these guidelines. However, data on legal domiciles (including nationalities) could at times be used for unfair discrimination in commercial activities and it is therefore desirable that it not be collected except for businesses that require a high level of personal identification.
3. Subparagraph (4), "Health, medical treatment": The classic example would be an individual's medical records. This example should also be considered to include the medical records of the subject's parents, siblings, and relatives etc. given the potential for discovering genetic or potentially-genetic illnesses.

< References >

- EU Directive, Article 8

Article 8. Measures for Collection of Personal Data Directly from Data Subject

When personal data are collected directly from the data subject, the consent of the data subject concerning the collection, use and disclosure of the personal data shall be obtained through written notification of at least the information given below, or of equivalent information. This shall not apply, however, in the case where it is clear that the data subject has been notified in writing of the information given below, or where personal data are collected from data made public by the data subject to a large number of unspecified persons.

- (1) The name or title, department and telephone number or address, etc. of the manager or his agent concerned with personal data within enterprises.
- (2) Purpose of the collection and the use of personal data.
- (3) If there is a plan to disclose personal data, the purpose thereof, the recipient of the personal data or the type and character of the recipient's organization, and whether or not a contract has been concluded concerning the handling of personal data.
- (4) The voluntariness of the data subject concerning provision or non-provision of personal data and the result not to provide personal data.

(5) The existence of the right to request access to personal data and the right to request correction or deletion thereof if the personal data are found to be erroneous following the access, and the specific method by which the right is to be exercised.

< Explanation >

1. The Old Guidelines only discussed the collection of personal data in Article 2(1) and 2(2) (which correspond to Article 5 and Article 6 in these Guidelines). One of the purposes of the revisions, however, was to clarify the rights of the data subject over personal data, and as part of this we have explicitly required that at the time of collection the data subject be notified of the purpose of collection and his right to seek correction and deletion of data, and that the data subject consent to the collection. Clarification of the rights of the data subject is one of the highest-interest issues in the EU and other countries, and EU Directive, Article 10 contains provisions of similar intent to this Article.
2. "Written notification" does not necessarily require that documents separate from applications and the like be used to notify subjects about personal data collection, merely that matters subject to notification be noted in catalogs, applications, contracts and the like.
3. "In the case where it is clear that the data subject has been notified in writing of the information given below" should be interpreted to include cases of in-store displays that are easily verifiable by the data subject (for example, indications provided in posters or in fliers) and renewals of applications for which consent has previously been obtained (for example, data collection by rental video stores when renewing memberships).
4. The collection of "data made public by the data subject to a large number of unspecified persons" does not in principle require the consent of the subject because of the nature of public information, but depending on the purposes for which it is used or the way in which it is processed such data could infringe on interests of the subject that ought to be protected. In cases in which it is difficult to judge if such a risk exists, the consent of the subject should be sought. For example, NTT telephone books could be considered to be included in "public information," but information created for limited purposes and users (for example, a directory of university graduates created and distributed for the purpose of cultivating friendships among classmates) would probably not be considered public information.
5. In notifying consumers of the matters listed in Subparagraphs (1)-(5) of this Article, enterprises need not directly use terminology found in these Guidelines like "the name or title, department and telephone number or address, etc. of the manager or his agent concerned with personal data within enterprises." Any wording that communicates the necessary matters to consumers is acceptable.
6. Subparagraph (1), "The name or title, department and telephone number or address, etc. of the manager or his agent concerned with personal data": This provides a place to inquire about how personal data on oneself is collected and used. In order to clarify the rights to data concerning oneself, we have required an explicit indication of the department and title of the manager (see Article 22) rather than just a company name. The reason for requiring either "the name or title" is because there may be cases in which specifying a manager by name might cause confusion

because of personnel changes within the organization. This description should enable the person responsible to be easily identified.

7. Subparagraph (3), "If there is a plan to disclose personal data": The data subject is usually not directly involved in the disclosure of personal data, so it is necessary to specifically clarify information on the purpose of disclosure and the recipients of data in order to alleviate the anxieties of the data subject.

"The type and character of the recipient's organization" refers to the industry of the organization (enterprise) receiving personal data and its relationship (affiliate, holding company etc.) to the enterprise disclosing data.

8. Subparagraph (4), "The voluntariness of the data subject concerning provision or non-provision of personal data": This refers to information on whether it is mandatory to fill in information on applications and the like or voluntary (for example, for surveys). "Result not to provide personal data" refers to the potential outcome of not responding to questions (for example, if one does not respond to the question on income in a marriage service application, one will be introduced to a partner without considering the condition of his income).

9. In cases in which time and/or space considerations make it difficult to indicate all of the matters listed in this Article, for example "television shopping" or magazine advertisements for catalog sales, the matters listed in this Article should be notified to consumers next time they are contacted (for example, when catalogs or products are sent) and their consent should be obtained at that time.

< References >

· EU Directive, Article 10

Article 9. Measures for Indirect Collection of Personal Data Other than from Data Subject

When personal data are collected indirectly from a source other than the data subject, the consent of the data subject concerning the collection, use and disclosure of the personal data shall be obtained through written notification of at least the information given in (1) through (3) and (5) of the preceding Article. This shall not apply, however, in the case given in (1) through (4) below.

(1) If personal data are collected from enterprises that have obtained the data subject's consent to disclose the personal data in accordance with (3) of the preceding Article when the personal data were collected from the data subject

(2) If personal data are collected and disclosed from enterprises with a guarantee that personal data are handled in a manner equivalent to that of the enterprises through conclusion of a contract stipulating the obligation to maintain confidentiality, the prohibition against re-disclosure and the assignment of responsibility when accidents occur in respect of personal data disclosed.

(3) If it is clear that the data subject has been notified of the information given in (1) through (5) of the preceding Article, and if personal data are collected from data made public by the data subject to a large number of unspecified persons.

(4) If personal data are collected in the case where it is not likely to infringe on the interests of the data subject worthy of protection within the limit of legitimate business of enterprises.

< Explanation >

1. In the Old Guidelines, the only provisions for data collected indirectly from a source other than the data subject was an abstractly worded requirement in Article 2(1) that "the collection of personal data from third party shall be limited to the case where there is no likelihood of infringing on the interests of the data subject worthy of protection." However, the rapid advances recently seen in network technology and the growing importance of business activities that use personal data to respond to diversifying consumer needs have made it more common that personal data is collected indirectly, from sources other than the data subject, rather than directly from the data subject.

This indirect collection, in which the data subject is not directly involved, increases the potential for data to be distributed without the knowledge of the subject himself for data to "take on a life of its own." Such data must be handled with particular caution so as not to infringe on the interests of the data subject.

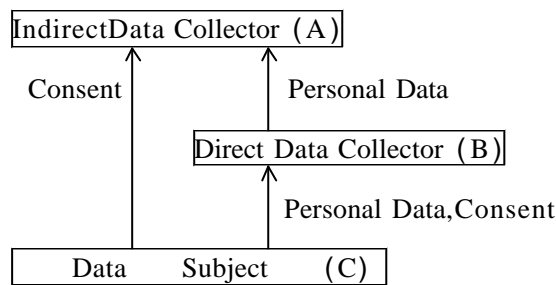
These Guidelines therefore seek to alleviate the worries of data subjects by defining in detail the cases in which it is permissible to collect data indirectly from sources other than the data subject. Basically, this involves providing the same notifications and obtaining the same consent from the data subject as required in Article 8 for directly collected data. Exceptions are provided in Subparagraphs (1)-(4), and notifications and consent are not required in the cases described therein.

2. Subparagraph (4), "If personal data are collected in the case where it is not likely to infringe on the interests of the data subject worthy of protection within the limit of legitimate business of enterprises": As stated in Paragraph 1 above, particular caution must be exerted so that the indirect collection of data from sources other than the data subject does not infringe upon the interests of the data subject. Determination of whether such collection meets the requirements of Subparagraph (4) is not to be made arbitrarily by the parties involved. Rather, this clause should be interpreted as narrowly as possible according to objective standards of reason and social mores.

Therefore, the phrase "within the limit of legitimate business of enterprises" shall be interpreted to mean cases in which collection is absolutely indispensable to legitimate business activities, for example, the collection of personal data by a gas safety service in order to ensure the safety of customers might be construed as meeting this requirement. However, it is anticipated that different industrial sectors will have differing interpretations of the "limits of legitimate business." Industry Guidelines should therefore be as specific and concrete as possible about what constitutes the "limit of legitimate business."

3. The illustration below is provided to clarify the interpretation of this Article. The explanation which follows refers to this illustration. Note that "indirect collection of data from direct data collectors" is defined in exactly the same way as "disclosure of data by direct data collectors." In

light of this relationship, this Article discusses issues from the vantage point of indirect data collection. For restrictions from the vantage point of direct data collectors, see Article 14, which defines rules for the disclosure of personal data.



When Indirect Data Collector (A) collects personal data on Data Subject (C) from Direct Data Collector (B), it must in principle obtain the consent of C to the matters listed in Article 8 Subparagraphs (1)-(3) and (5). This is not necessary, however, in the following cases:

- (1) When A collects personal data on C from B and C has already consented to the anticipated disclosure of data to A in accordance with Article 8(3) at the time B collects data from C.
- (2) A and B have concluded a contract stipulating the obligation to maintain confidentiality, the prohibition against re-disclosure and the assignment of responsibility when accidents occur so that there are guarantees that A will handle personal data in the same manner as B.
- (3) It is clear that C has already been notified of the information given in Article 8 Subparagraphs (1)-(5) and collection is made from data C has disclosed to a large and unspecified number of persons.
- (4) Personal data are collected within the limits of legitimate business of A and is not likely to infringe on interests of C worthy of protection.

< References >

- EU Directive, Article 11

## **Chapter 5 Measures Concerning Use of Personal Data**

Article 10. Limitation on Use of Personal Data

The use of personal data shall, in principle, be limited within the scope of the purpose of the collection.

< Explanation >

Chapter 5 defines principles for the use of personal data. Like the Old Guidelines, these Guidelines correspond to the "Use Limitation Principle" found in the OECD's "Eight Principles." This Article corresponds in content to Article 3(1) of the Old Guidelines.

< References >

- OECD Guidelines No.10
- Old Guidelines, Article 3(1)

Article 11. Measures for Use of Personal Data within the Scope of the Purpose

The use of personal data within the scope of the purpose of the collection shall be done solely in the case given in (1) through (6) below.

- (1) If the data subject has given consent.
- (2) If the use is necessary to permit the data subject to prepare for or to perform a contract to which he is a party.
- (3) If the use is necessary for compliance with legal obligations to which enterprises are subject.
- (4) If the use is necessary in order to protect the vital interests of the data subject including life, health, property, etc.
- (5) If the use is necessary for protecting the public interest or for exercising authority under laws by enterprises or a third party that personal data are disclosed to.
- (6) If the use is necessary for the legitimate interests of enterprises, or a third party or other parties that the personal data are disclosed to, in so far as the interests of the data subject are not infringed.

< Explanation >

1. In the discussion of "scope of purpose of collection" in the Old Guidelines (Article 3(1)), use of personal data was permitted in "cases where it is not likely to infringe on the interests of the data subject worthy of protection" (Article 3(3)). The New Guidelines attempt to strengthen the protection afforded the rights of data subjects over information concerning them by stipulating that personal data can only be used in the cases described in Subparagraphs (1)-(6) even when such data might be used within the scope of the purpose of the collection.
2. Subparagraph (1), "If the data subject has given consent": When personal data are collected after the application of these Guidelines, such data should obviously be used within the scope consented to by the data subject as per Article 8. (Therefore, Subparagraph (1) is verification rule) When personal data are collected prior to the application of the se Guidelines, then Subparagraph (1) would conceivably apply.

< Note >

There is no need to re-obtain consent for data collected with the consent of the data subject prior to the formulation of these Guidelines.

3. Subparagraph (3), "Legal obligations to which enterprises are subject": Rationale for this would probably be found in the Article 218:1 of the Criminal Procedure Act (investigation under warrants) and the Article 72:63 of the Local Tax Code (right to question and investigate

matters concerning business taxes, and similar provisions for other tax codes). These provisions are mandatory and enterprises are obligated to respond.

Other cases where cooperation is voluntary for example, Article 197:2 of the Criminal Procedure Act (investigation and necessary questioning), Article 23:2 of the Lawyers Law (request for reports), and Article 8 of the Family Court Bylaws (request for necessary reports) might be considered to fall under the scope of this provision, but in such cases, use is not unconditional. Requirements for use must carefully weigh the public interest in use with the need to protect personal data. One possibility might be to set a standard that use will only be permitted when requested in writing.

< Note >

Regarding inquiries under Article 23:2 of the Lawyers Law, the Osaka Supreme Court ruled on December 21, 1976 that "this should be interpreted as an obligation to report in response to inquiries unless doing so would impair one's ability to perform one's duties or there are other legal interests that must be protected and these interests outweigh the public interest in obtaining reports in response to inquiries."

4. Subparagraph (5), "If this is necessary for protecting the public interest": This would refer, for example, to a gas service notifying the police, fire-department, and enterprise responding to an accident of information received from the user at the time of an accident.

< References >

- EU Directive, Article 7

Article 12. Measures for Use of Personal Data beyond the Scope of the Purpose

When the use of personal data exceeds the scope of the purpose of the collection, or when the use of personal data is done in the cases other than any of the cases given in (1) through (6) of the preceding Article, it shall be carried out with the prior acknowledgment of the data subject secured by obtaining the prior consent of the data subject or by giving the data subject an opportunity to refuse prior to use, through written notification of at least the information given in (1) through (3) and (5) of Article 8.

< Explanation >

1. When use exceeds the purpose of collection, it departs from the scope of consent given by the data subject. The Old Guidelines therefore stated in Article 3(2), "When the use of personal data exceeds the scope of the purpose of the collection it shall, in principle, be done with the consent of the data subject such as gaining the assent of the data subject or giving the data subject the opportunity to refuse." Likewise, these Guidelines specify that when use goes beyond the scope of the purpose of collection and the requirements of Subparagraphs (1)-(6) of Article 11 are not met, it shall be subject to the prior acknowledgment of the data subject, either by the enterprise obtaining the consent of the data subject or the enterprise providing the data subject with the opportunity to refuse.

2. "Use of personal data beyond the scope of the purpose" when such use is by a different division of the enterprise that collected the data will to some extent depend on what has been given as the "purpose of collection," but in cases in which data is used by a division that the ordinary data subject would not foresee, such use shall require the prior acknowledgment of the data subject even when it is within the same enterprise if it is beyond the scope of the purpose of collection.

< Specific examples >

- (1) A department store collects personal data in the store for the purpose of "sending information about products to you from the department store." In this case, sending product information from the department store's catalog sales division would be permissible.
- (2) A hotel collects personal data for the purpose of "sending information about fairs held by the restaurants and shops in the hotel." In this case, sending product information from a department store in the same corporate group as the hotel would exceed the scope of the purpose of collection.

< References >

- Old Guidelines, Article 3(2)

## **Chapter 6 Measures Concerning Disclosure of Personal Data**

### Article 13. Limitation on Disclosure of Personal Data

The disclosure of personal data shall, in principle, be limited within the scope of the purpose of the collection.

< Explanation >

Chapter 6 defines principles for the disclosure of personal data. Like the Old Guidelines, these Guidelines correspond to the "Collection Limitation Principle" found in the OECD's "Eight Principles." This content of this Article is the same as Article 3(1) of the Old Guidelines.

< References >

- OECD Guidelines No. 10
- Old Guidelines, Article 3(1)

### Article 14. Measures for Disclosure of Personal Data within the Scope of the Purpose

The disclosure of personal data within the scope of the purpose of the collection shall be carried out with the prior acknowledgment of the data subject secured by obtaining the prior consent of the data subject or by giving the data subject an opportunity to refuse prior to disclosure, through written notification of at least the information given in (1) through (3) and (5) of Article

8. This shall not apply, however, in the case given in (1) through (4) below.

(1) If personal data are disclosed to the recipient that the data subject has given consent to disclose the personal data to in accordance with (3) of Article 8 when the personal data were collected from the data subject.

(2) If personal data are disclosed to the recipient with a guarantee that personal data are handled in a manner equivalent to that of enterprises that disclose the personal data through conclusion of a contract stipulating the obligation to maintain confidentiality, the prohibition against re-disclosure and the assignment of responsibility when accidents occur in respect of personal data disclosed.

(3) If it is clear that the recipient is to take measures to obtain the data subject's consent through notification of the information given in (1) through (5) of Article 8 concerning the personal data.

(4) If personal data are disclosed in the case where it is not likely to infringe on the interests of the data subject worthy of protection within the limit of legitimate business of enterprises.

< Explanation >

1. The wording of the Old Guidelines on the disclosure of personal data contained only abstract requirements that it "shall be limited within the scope of the purpose of the collection" (Article 3(1)) and "is not likely to infringe on the interests of the data subject worthy of protection" (Article 3(3)).

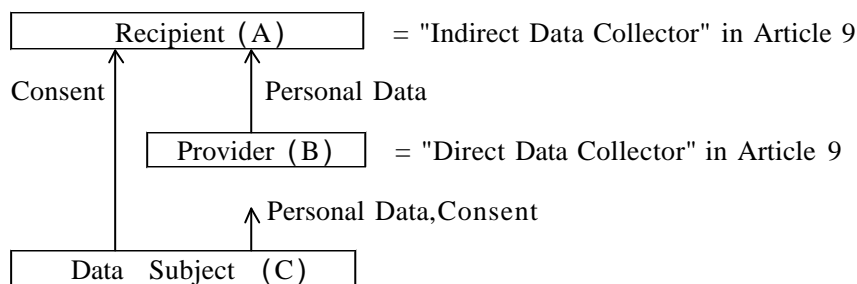
As was noted in Paragraph 1 of the explanation for Article 9, the expansion in business activities making use of personal data has in recent years increased the potential for personal data to frequently be circulated without the knowledge of the data subject. These Guidelines attempt to alleviate the anxieties of data subjects over the disclosure of personal data, which would contribute to efficient business activities, by defining in detail the cases in which disclosure is possible and requiring that prior acknowledgment be received from the data subject except in the cases described in Subparagraphs (1)-(4).

2. Subparagraph (3), "If it is clear that the recipient is to take measures to obtain the data subject's consent": There will be cases in which it is difficult for the provider to confirm that the recipient has obtained the consent of the data subject. Therefore, as long as this is explicitly stated in the contracts and other procedures at the time data is disclosed, the provider does not incur the obligation to confirm that consent has actually been obtained.

3. Subparagraph (4), "If personal data are disclosed in the case where it is not likely to infringe on the interests of the data subject worthy of protection within the limit of legitimate business of enterprises": As was the case in the indirect collection of data discussed in Article 9(4), the data subject is usually not directly involved in the disclosure of personal data, and this provision should therefore be interpreted extremely narrowly as per Paragraph 2 of the explanation for Article 9.

4. As was noted in this Article and the explanation of Article 9, "disclosure of personal data to third parties" is defined in exactly the same way as "indirect collection of data by third parties"

In light of this relationship, Article 14 is essentially a rewrite of Article 9 ("indirect collection of personal data") from the perspective of the direct data collector. As was done for Article 9, we will use the illustration below to explain Article 14 in an more easily understood manner.



When Provider (B) discloses personal data on Data Subject (C) to Recipient (A), it must in principle do so with the prior acknowledgment of C. This is not necessary, however, in the following cases:

- (1) When A collects personal data on C from B and C has already consented to the anticipated disclosure of data to A in accordance with Article 8(3) at the time B collects data from C.
- (2) B and A have concluded a contract stipulating the obligation to maintain confidentiality, the prohibition against re-disclosure and the assignment of responsibility when accidents occur so that there are guarantees that A will handle personal data in the same manner as B.
- (3) A notifies C of the matters listed in Article 8 Subparagraphs (1)-(5) for the data in question and it is clear that B is to take measures to obtain C's consent.
- (4) Personal data are collected within the limits of legitimate business of B and is not likely to infringe on the interests of C worthy of protection.

5. Needless to say, the "disclosure" provided in this article is applied to enterprises outside Japan. It needs to be noted especially, lest the personal data disclosed outside Japan should use inadequately after disclosure.

#### Article 15. Measures for Disclosure of Personal Data beyond the Scope of the Purpose

When the disclosure of personal data exceeds the scope of the purpose of the collection, or when the disclosure of personal data is done in cases other than any of the cases given in (1) through (4) of the preceding Article, the consent of the data subject shall be obtained through written notification of at least the information corresponding to (1) through (3) and (5) of Article 8 concerning the recipient of the personal data. In such cases, "enterprises" given in (1) of Article 8 shall be amended to read "recipient", and "disclose" given in (3) of Article 8 shall be amended to read "re-disclose". This shall not apply, however, in the case where it is clear that the data subject has been notified of the information and has given blanket consent.

#### < Explanation >

1. When disclosure exceeds the purpose of collection, it departs from the scope of consent given by the data subject. The Old Guidelines therefore stated in Article 3(2), "When the disclosure of personal data exceeds the scope of the purpose of the collection, it shall, in principle, be done with the consent of the data subject such as gaining the assent of the data subject giving the data

subject the opportunity to refuse." Likewise, these Guidelines specify that when disclosure goes beyond the scope of the purpose of collection and the requirements of Subparagraphs (1)-(4) of Article 14 are not met, it shall be subject to the consent of the data subject.

2. "Clear that the data subject has given blanket consent": Given the frequency with which personal data is distributed today, it is anticipated that there will be many cases in which it is difficult to obtain the consent of the data subject for each and every disclosure.

However, as noted in Paragraph 1 above, the disclosure of personal data in excess of the purposes of collection departs from the scope of consent given by the data subject, so these provisions must be interpreted strictly. "Blanket consent" from the data subject involves obtaining an explicit written response from the data subject, explicit statements within contractual documents, or other similar procedures.

3. Refer to Explanation 4 in Article 14 concerning the disclosure to enterprises outside Japan.

< References >

· Old Guidelines, Article 3(2)

## **Chapter 7 Obligation to Manage Personal Data Properly**

Article 16. Ensuring the Accuracy of Personal Data

Personal data shall be kept accurate and up-to-date to the extent necessary for the purpose of the use.

< Explanation >

1. Chapter 7 contains principles for the proper management of personal data. Like the Old Guidelines, these Guidelines correspond to the "Data Quality Principle" and the "Security Safeguards Principle" found in the OECD's "Eight Principles."

2. In the Old Guidelines, the principles for "proper management of personal data" were found only in Article 4(1) and (2). In these Guidelines, they are found in Article 16 and Article 17, which correspond to Article 4(1) and (2) of the Old Guidelines respectively, Article 18, which defines the responsibilities of the employees who actually process personal data, not just the managers of personal data, and Article 19, which deals with the increasingly common practice of "outsourcing" (entrusting to outside service providers) the processing of personal data. The last three are new additions.

3. Like Article 4(1) of the Old Guidelines, this Article mandates that personal data be kept accurate and up-to-date to the extent necessary for the purpose of the use, thereby preventing any infringement of the interests of the data subject because of mistaken or outdated data.

4. To keep "for the purpose of the use" include to destroy in the accurate way the data which is

no longer used.

< References >

- EU Directive, Article 6:1(d) and (e)
- OECD Guidelines No. 8
- Old Guidelines, Article 4(1)

Article 17. Ensuring Security in Use of Personal Data

Reasonable security measures shall be taken through both technical and organizational means against such risks as unauthorized access to personal data or as loss, destruction, alteration, leakage, etc. of personal data.

< Explanation >

1. This Article is almost exactly the same as Article 4(2) of the Old Guidelines, but we have added the wording about "technical and organizational means" to reflect the points made in Article 17:1 of the EU Directive.
2. For specific technological measures to ensure security, refer to "Information Systems Security Guidelines" (Ministry of International Trade and Industry Notification No. 518 of August 29, 1995) and the like. Organizational measures to ensure security will require the establishment of in-house standards and accountability systems for the protection of personal data.
3. Therefore, by deleting electronic data and shredding paper including personal data, in face of destruction of data, it needs to be noted lest such data should leak out to third parties.

< References >

- EU Directive, Article 17:1
- OECD Guidelines No. 11
- Old Guidelines, Article 4(2)

Article 18. Obligation of Employees to Maintain Confidentiality of Personal Data

Persons within enterprises engaged in the collection, use and disclosure of personal data shall perform, using sufficient care, the obligation to maintain the confidentiality of personal data in accordance with the provisions of laws, or regulations and instructions specified by the manager of the enterprises.

< Explanation >

1. The Old Guidelines did define the responsibilities of "a person who is competent to decide about the handling of personal data in enterprises" in Article 6 (which is the same as "managers" as defined in Article 2(2) of these Guidelines), but did not define the responsibilities of employees actually processing personal data because this was considered

obvious.

2. However, recent cases of malicious leakage and alteration of personal data indicate that there is a need to increase the awareness of the data processing employees that in practical terms have easiest access to personal data. Therefore, these Guidelines add a new Article that clearly defines the responsibilities of the employees actually processing personal data in addition to those of their managers. The same intentions can be found in Article 16 and Article 17:2 and 3 of the EU Directive.
3. "Persons within enterprises "includes the dispatched worker and part-time workers as well as full-time workers in such enterprises. (Reference to Explanation 2 in Article 3)

< References >

- EU Directive, Article 16, Article 17:2 and 3

Article 19. Measures Concerning Entrustment of Personal Data

In the case where enterprises entrust personal data to an outside enterprise, they shall select one that can handle the personal data at a sufficient level of protection, and shall guarantee, through conclusion of a contract or other legal measure, that the instructions of the manager of the enterprises are observed, that the confidentiality of personal data is maintained, that the re-disclosure of personal data is prohibited, and that responsibility when accidents occur is assigned, and shall maintain the contract, etc. as written documents or magnetically-stored records for the period that the personal data are managed by the outside enterprise.

< Explanation >

1. Recent advances in computer technology have resulted in enterprises engaging in more varied and complex data processing activities, and there are more cases of enterprises entrusting their data processing to outside service providers in order to improve business efficiency and customer services ("outsourcing"). This Article was added in recognition of the need to take measures to prevent mishaps in the processing of personal data outsourced to independent processors.
2. Specifically, the Article notes the need to set standards in the selection of outside processors, to sign contracts with clear confidentiality obligations, explicit bans on re-disclosure, and set time periods for processing, and to require that personal data be returned immediately after processing is finished.
3. Those entrusted with data processing are obviously not allowed to use or disclosure personal data in contravention of the entrustment, and must also manage personal data properly and in accordance with these Guidelines.
4. When the processing of personal data is entrusted to an outside enterprise, the trustor will bear direct responsibility for responding to requests from data subjects to disclose, correct, or delete data, but there may be cases in which serving as a liaison for requests to disclose, correct, or delete data is itself outsourced, or the work of disclosure, correction, or deletion is part of the

outsourcing contract (see also Article 20). However, in this case, the share of responsibilities and roles between the trustor and the trustee should be clear in outsourcing contract.

< References >

· EU Directive, Article 17:4

## **Chapter 8 Rights of Data Subject Concerning Data Regarding Self**

### Article 20. Rights Concerning Own Personal Data

Requests for access to personal data by the data subject shall, in principle, be accepted within a reasonable period of time. If the personal data is found to be erroneous following the access, requests for correction or deletion of the personal data shall, in principle, be accepted within a reasonable period of time. In such cases, recipients of the personal data shall be notified to the extent possible.

< Explanation >

1. Chapter 8 defines principles under which the data subject may request the access, correction and deletion of data regarding the subject himself, or may refuse the use and/or disclosure of said data. Like the Old Guidelines, the discussion of access, correction, and deletion in these Guidelines follows the "Openness Principle" and the "Individual Participation Principle" found in the OECD's "Eight Principles."
2. Making it possible for the data subject to seek the access of data directly related to himself from enterprises collecting, accumulating, and using such data, to seek correction and/or deletion of mistaken data, and in some cases to refuse use and/or disclosure of data plays the role of the final guarantee of the interests of the data subject in today's environment of frequent collection, accumulation, use, and disclosure of personal data.
3. This Article is almost exactly the same as Article 5(1) of the Old Guidelines, but limits requests for correction and/or deletion of the personal data to cases in which data is "found to be erroneous following the access." This is done because it is conceivable that a data subject would request corrections and/or deletions without a valid reason, and that this would impair the efficient business activities of enterprises using personal data, or that it would pose a large impediment to public-interest enterprises such as electricity and gas that are obligated by law to supply their products.
4. One of the purposes of this review of personal data protection policies was to clarify the control of the data subject over his own individual data so that data does not "take on a life of its own" unbeknownst to the data subject in today's environment of frequent distribution of personal data. For this to be achieved, it is desirable that when individuals access personal data they are provided not only with information on the status of the data itself but also, when necessary, on the purposes of collection and the recipients of disclosure.

5. The reason for the "in principle" wording is because there may be some exceptions. For example, it may be necessary to exclude specific personal evaluations or other information which social mores and practices would deem inappropriate for disclosure.
6. A "reasonable period of time" refers to the general period for updates of personal data within the enterprise.
7. The reason for requiring recipients to be notified of corrections and deletions "to the extent possible" is because even though in principle notifications should obviously be given when corrections and deletions are made, it is conceivable that in today's environment of frequent distribution of personal data that it may be difficult to notify all recipients. This clause is not meant to give those correcting or deleting data any large discretionary powers.
8. When data subject request access, it is permissible to charge fees etc. so long as they are not excessive. In such cases, data subjects should be informed of the fees ahead of time. As a reference, Japanese government institutions charge ¥260 as fees for processing disclosure requests (as at December 1997).

< References >

- EU Directive, Article 12
- OECD Guidelines No. 12, No. 13
- Old Guidelines, Article 5(1)

Article 21. Right to Refuse Use or Disclosure of Own Personal Data

Refusals of the use or the disclosure, by the data subject, of personal data managed by enterprises shall be accepted. This shall not apply, however, in the case where the use or the disclosure is necessary for protecting the public interest, or for exercising authority or performing obligations under laws by the enterprises or a third party that the personal data are disclosed to.

< Explanation >

1. The reason for making it a general principle that data subjects may refuse the use or disclosure of their own personal data is because it is conceivable in today's environment of frequent distribution of personal data that the data subject's acknowledgment may not be obtained even in cases in which it is supposed to be obtained before personal data is used or disclosed. Similarly, even when the data subject's acknowledgment has been obtained, there may be cases in which the data subject was not able to accurately foresee the future use and disclosure of data when signing blanket agreements in contracts and similar documents. Therefore, it is necessary to allow the data subject the right to refuse use and disclosure of his own data both in obvious cases where there has been negligence in obtaining the data subject's acknowledgment and in other cases as warranted by subsequent conditions.
2. This Article is almost exactly the same as Article 5(2) in the Old Guidelines, but in additional

exceptions to the principle of refusal of use and disclosure are provided for example, when doing so would pose a large impediment to public-interest enterprises such as electricity and gas that are obligated by law to supply their products, or in the provision of services and goods or the extension of credit when personal data on the individual's use of such services is needed to ensure the recovery of prices and loans.

The wording "for exercising authority under laws" could conceivably include legal purposes not based directly on laws and ordinances themselves.

< References >

- EU Directive, Article 7, Article 14(b)
- Old Guidelines, Article 5(2)

## **Chapter 9 Organization and Implementation Accountability**

### Article 22. Designation of Manager by the Representative

The representative of enterprises shall designate from within the enterprises a person who understands the contents of these guidelines and has the capacity to put them into practice, and shall cause the person to function as the manager of personal data.

< Explanation >

1. Chapter 9 defines the organizations and accountability needed for adherence to the principles espoused in the guidelines. Like the Old Guidelines, these Guidelines correspond to the "Accountability Principle" found in the OECD's "Eight Principles."
2. This Article is almost exactly the same as Article 6 in the Old Guidelines in that it asks enterprises to provide accountability for adherence to the principles espoused in the guidelines by designating a person with practical authority over the collection, accumulation, use, and other handling of personal data. These Guidelines, however, clarify this person's position within the enterprise organization by asking enterprise representatives to designate at least one person from their organizations to serve as a "manager" and be accountable for the matters listed in the following Article. In as much as the manager is the person responsible for the management of personal data by the enterprise, enterprises must avoid needlessly increasing the number of persons designated when doing so would obfuscate accountability. Therefore, enterprises designating more than one manager should clearly delineate the responsibilities of each manager.

< Example >

- (1) Company A is engaged in both the railway and real estate industries. Mr. B is the manager for personal data from the railway business, while Mr. C is responsible for personal data from the real estate business.  
Their responsibilities are clearly defined, so there is no problem having multiple managers.
- (2) Company D has designated Mr. E and Mr. F, both of whom are Assistant General Managers in the Sales Department, as personal data managers.

Their roles and responsibilities are unclear, so multiple managers are undesirable.

Note that in actual practice the manager, together with the "agent" defined in Article 8(1), is responsible for the management of personal data. For example, if Mr. A, the director in charge of sales, is designated as manager, then his agents, the members of the sales department, may respond directly to customer inquiries.

3. No specific qualifications have been defined for "managers," but it is desirable that enterprises nominate someone from their organization that is able to take responsibility for outside dealings (for example, a director).

< References >

- OECD Guidelines No. 14
- Old Guidelines, Article 6

Article 23. Duties of Manager

The manager of personal data within enterprises shall understand and observe the provisions of these guidelines, and shall accept responsibility for causing employees to understand and observe these guidelines by providing training, establishing internal regulations, implementing security measures, establishing a compliance program and taking measures to ensure that the program is made known to everyone.

< Explanation >

1. Article 6 of the Old Guidelines was abstract in its description of implementation duties, so these Guidelines have attempted to define the duties of managers more concretely. In particular, we have included an explicit statement that the manager has the duty of "establishing a compliance program and taking measures to ensure that the program is made known to everyone" so as to improve the awareness of personal data protection within the enterprise.
2. "Employee" includes the dispatched workers and part-time workers as well as full-time workers in such enterprises, and refer to the persons who handle personal data in such enterprises. Education to workers in addition to full-time workers is very important, because there are some case currently that another worker except full-time workers leak personal data.

< References >

- OECD Guidelines No. 14
- Old Guidelines, Article 6

## **Chapter 10 Other Provisions**

Article 24. Notification when Magnetically-Stored Records are Transmitted and Received Using

## Communication Networks

In the case where magnetically-stored records are transmitted and received using a communication network, enterprises that collect personal data concerning the sender or receiver of the records using a communication network cannot notify the data subject, who is the sender or receiver, through transmission of magnetically-stored records rather than through written notification of the data subject, as provided for in Article 8, Article 9, Article 12, Article 14, and Article 15 of these guidelines.

### < Explanation >

1. The rapid expansion of the Internet and other network technologies has made it more frequent that communication networks be used to send and receive needed information, for example, in electronic commerce. This Article was newly added to provide for this.
2. This article defines that the "written notification to the data subject" in Articles 8, 9, 12, 14, and 15 is not limited to paper but may also include notifications through transmission of electronic data.
3. For more information on the protection of personal data in electronic commerce, see "Guidelines Concerning the Protection of Personal Data in Electronic Commerce in Private Sector" formulated by the Electronic Commerce Promotion Council of Japan (ECOM) with reference to the unique business practices associated with electronic commerce (finalized and published in March 1998. URL: <http://www.ecom.or.jp>).