

# **Summary of Opinions on the Protection of Personal Information**

June 29, 2007  
Quality-of-Life Policy Council

## Table of Contents

### Introduction

#### **I. Conditions Following the Enforcement of the Personal Information Protection Act**

#### **II. General Matters**

1. So-called “overreactions”
2. Publicity and education

#### **III. Objects to be Protected and Business entities Handling Personal Information Required to Perform Certain Duties**

1. About the system under which all personal information is treated in a similar way under the Personal Information Protection Act
  - 1) Objects to be protected
  - 2) Special measures
2. Scope of business entities handling personal information required to perform certain duties

#### **IV. Efforts of Entities, etc.**

1. General efforts of entities, etc.
  - 1) Appropriate guidelines, etc.
  - 2) Assistance to entities
  - 3) Enhancement of supervision over entities
2. Acquisition, utilization, discontinuance of utilization and erasure
3. Proper safety control
  - 1) Level of safety control measures
  - 2) Supervision over employees
  - 3) Supervision over contractors
  - 4) Management of commercial name lists held by entities
4. Restrictions on provision of information to third parties
5. Relationship with consumers, etc. (including the owners of personal information)
  - 1) Purpose of utilization determined by entities
  - 2) Disclosure of the name of the party from whom information has been obtained

#### **V. Function of Authorized Personal Information Protection Organizations**

#### **VI. Processing Complaints**

#### **VII. Compliance with International Rules**

**VIII. Significance of Independent Organizations**

**IX. Protection of Personal Information of the Deceased**

**X. Others**

1. Handling of personal information held by state administrative organs
2. Efforts of local governments

**Concluding Remarks**

## Introduction

The Act on the Protection of Personal Information (Act No.57 of 2003; hereinafter, “Personal Information Protection Act”) was promulgated in May 2003, and fully enacted in April 2005. The Personal Information Protection Act intends to protect the rights and interests of individuals while taking consideration of the usefulness of personal information, to function as an institutional base on which every person may enjoy the benefits of the advanced information age with a sense of security.

The “Basic Policy on the Protection of Personal Information” (the Cabinet decision of April 2, 2004; hereinafter, the “Basic Policy”), which has been established in accordance with the provisions of paragraph 1, Article 7 of the Personal Information Protection Act, requires that the Cabinet Office examine the conditions of how the Act is applied around three years after its full enactment and take necessary measures based on the results of this examination, and that the Quality-of-Life Policy Council follow up the conditions that regulate how the Act is applied.

The Panel on the Protection of Personal Information under the Quality-of-Life Policy Council therefore began to examine the conditions surrounding how the Act is implemented in November 2005, and conducted interviews with related entities, private organizations, relevant ministries, etc. Subsequently, the Panel compiled and publicized the “Main Problems for Further Examination in the Field of the Protection of Personal Information” in July 2006. Following this, the Cabinet Office collected related opinions from a wide public spectrum. The Panel continued discussions based on the main problems, further examining the issue along with the collected public opinions, etc., and summed up its opinions concerning future legislation for the protection of personal information as mentioned in this report.

The Quality-of-Life Policy Council hereby recommends that the Government take the necessary measures based on the Council’s opinions.

## **I. Conditions Following the Enforcement of the Personal Information Protection Act**

### **(1) Citizens' understanding and efforts of the entities**

According to the "Public Opinion Poll on the Protection of Personal Information" (conducted by the Cabinet Office in September 2006; hereinafter, "Public Opinion Poll,"), approximately 80% of respondents knew of the existence of the Personal Information Protection Act. Of these persons, about 75% felt that their friends, etc. had enhanced their understanding of, or interest in, the protection of personal information, and approximately 70% felt that measures taken by private entities and administrative organs for the protection of personal information had improved. According to the "Survey on Efforts of Entities for the Protection of Personal Information" (conducted by the Cabinet Office in March 2007; hereinafter, "Survey on Efforts of Entities,") 50% to 60% of the corporate respondents have a central department responsible for the company's efforts to protect personal information, or prepare and publicize a privacy policy (a declaration of its approach to or company policy for the protection of personal information) or other statements.

As is clear from the results of these surveys, it can be safely said that the public has an increased awareness of the necessity to protect personal information and efforts of entities have been bolstered as a result of the full enactment of the Personal Information Protection Act, etc.

On the other hand, according to the Public Opinion Poll, approximately 70% of the respondents felt uneasy that their personal information could be used for unfair purposes unbeknown to them, or that their personal information has been provided to third parties without their consent. This indicates that the public at large is still ill at ease regarding the treatment of personal information.

The Basic Policy requires that if any leakage of personal information takes place, the business entity concerned must publicize the relevant facts to the greatest extent possible. In fiscal 2005, entities that suffered such leakages disclosed facts on 1,556 cases of leakage, etc. of personal information. The fact that these cases continued to take place even after the enactment of the Personal Information Protection Act may be reflected in the results of the Public Opinion Poll. Since employees are often involved in these cases, entities are required to enhance supervision over, and education of, their employees in order to avoid such leakages of personal information.

According to the Survey on Efforts of Entities, 1% to 2% of respondents replied that they were asked to provide personal information but refused to do so even in cases in which they were permitted to do so without obtaining the consent of the owner under the Personal Information Protection Act. According to the Public Opinion Poll, approximately 50% of respondents who knew of the existence of the Act felt some inconvenience in their daily lives due to the Act, citing such reasons as the suspension of emergency phone or name lists, etc. within school or local communities. As seen from these survey results, and as pointed out by some entities in interviews conducted by the Quality-of-Life Policy Council, there have been a number of cases of "overreaction," in which even necessary personal information has not provided, or necessary emergency phone or name lists are no longer being prepared due to misunderstanding of the Act or other reasons.

### **(2) Efforts of the state, etc.**

The Personal Information Protection Act requires the State, local governments, authorized

personal information protection organizations, etc. to take measures for the protection of personal information based on the Basic Policy.

At the State level, ministries with jurisdiction over various types of business activities, etc. have established a total of 35 guidelines for 22 business sectors (as of May 31 of 2007), guide and supervise the concerned and have designated 34 organizations in total as authorized personal information protection organizations. In addition, the Cabinet Office and related ministries have been engaging in activities for publicity of, and education on, the personal information protection system among entities and the public through various media.

Local governments and the National Consumer Affairs Center of Japan, meanwhile, have created a personal information grievance system to process complaints smoothly. In fiscal 2005, they received 14,028 cases of complaint, and gave instructions or advice accordingly.

Each authorized personal information protection organization has established its own guidelines for the protection of personal information, and makes efforts to process complaints against the treatment of personal information by entities concerned, asking these entities to make an explanation, and giving instructions to them.

## **II. General Matters**

### 1. So-called “overreactions”

#### (1) Current conditions

- a. Paragraph 1, Article 23 of the Personal Information Protection Act stipulates, “A business entity handling personal information shall not provide, in principle, personal data to a third party without obtaining the prior consent of the person.”

However, in any of the following cases when priority should be placed on the social or public interest or other rights or interests, it is specified in the Act that such personal data may be provided without gaining the consent of the person: i) cases in which the provision of personal data is based on laws and regulations; ii) cases in which the provision of personal data is necessary for the protection of the life, body or property of an individual and in which it is difficult to obtain the consent of the person; iii) cases in which the provision of personal data is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person; or iv) cases in which the provision of personal data is necessary for cooperating with a state organ, a local government, or an individual or a business entity entrusted by one in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person are likely to impede the execution of affairs.

The term “case in which it is difficult to obtain the consent of the person” specifically refers to cases in which it is physically impossible to obtain the consent of the owner of the personal data, or that the characteristic or use of the personal data concerned may be hampered if the fact is known to the owner. It is generally understood that this term does not necessarily imply that the consent of the owner of such personal data must be obtained in all cases.

- b. Paragraph 2, Article 23 of the Personal Information Protection Act stipulates, “With respect to personal data intended to be provided to a third party, where a business entity handling personal information agrees to discontinue, at the request of a person, and where the business entity, in advance, notifies the person of the certain matters, the business entity may provide such personal data to a third party without the consent of the person.” (This is referred to as an “opt-out” case.)
- c. The Ministry of Internal Affairs and Communications has notified each local government to the effect that all municipalities should begin preparations to establish an Ordinance for the Protection of Personal Information as soon as possible, if one does not already exist, in view of the purposes of the provisions of the Personal Information Protection Act and of the Act on the Protection of Personal Information Retained by Administrative Organs (Act No.58 of 2003; hereinafter, the “Administrative Organs’ Personal Information Protection Act,”) and that any municipality that has already established the Ordinance should review it in consideration of the contents of the Administrative Organs’ Personal Information Protection Act (Notice from Director-General for Policy Planning, the Ministry of Internal Affairs and Communications dated June 16, 2003.)
- d. The current conditions of name lists, etc. that are often mentioned in connection with so-called “overreactions” are as follows:
- i) List of persons in need of assistance in times of disaster
- In March 2006, the Cabinet Office (the section in charge of disaster prevention) established the “Guidelines for the Evacuation of Persons in Need of Assistance at a Time of Disaster,” which include a provision on preparing a list of persons in need of assistance in times of disaster, and submitted the Guidelines to each local government. In April 2007, the Cabinet Office prepared concrete procedures as a guide to take measures for persons in need of assistance, and submitted these to all local governments.
- Since no voluntary disaster relief organization exists in which the number of such individuals who may be identified by their personal information included in the list of persons in need of assistance in times of disaster, exceeds 5,000, a direct and related infringement of the Personal Information Protection Act will likely not take place.
- ii) List of persons that require support from welfare commissioners or childcare commissioners
- Under the Welfare Commissioners Act (Act No.198 of 1948) and the Child Welfare Act (Act No.164 of 1947), welfare commissioners and childcare commissioners are required to properly observe living conditions of persons falling under specific criteria, if necessary, provide consulting services for their daily lives and give advice, etc. In particular, the commissioners’ activities include watching over the aged, confirming the safety of persons needing assistance in times of disaster, prevention of the aged from falling victim to immoral business practices, and supervision of abused children.
- To facilitate the activities of welfare and childcare commissioners, the Ministry of Health, Labour and Welfare has asked each local government to provide these commissioners with personal information in an appropriate manner.
- Welfare and childcare commissioners, as local public personnel involved in special services, perform their duties by sharing information with the relevant authorities,

etc. on local residents who need assistance in resolving their daily problems. The cases in which welfare or childcare commissioners must receive personal information to perform their duties from business entities handling personal information can be considered to fall under the category that decrees it a necessity to cooperate with the State, etc. In such cases, therefore, business entities handling personal information are allowed to provide such personal information to welfare or childcare commissioners without the consent of the owner of such personal information.

iii) Name lists of neighborhood associations

As the number of neighborhood associations consisting of more than 5,000 residents is relatively small there seems to be a limited number of neighborhood associations that are considered to be an “entity handling personal information” required to perform specific information protection duties under the Personal Information Protection Act.

iv) Emergency phone lists, etc. at schools

As for emergency phone lists, address books, etc. at schools, the Ministry of Education, Culture, Sports, Science and Technology revised the explanation of the “Guideline for Measures Taken by Entities to Ensure Proper Treatment of Personal Information of Students, etc. at Schools” (prepared by the Ministry on November 11, 2004) in February 2006. The explanation states that the consent of students, etc. should be obtained in advance.

(2) Problems

a. After the full enactment of the Personal Information Protection Act, etc., some cases of “overreaction” occurred in which necessary personal information was not provided or the preparation of name lists, etc. was suspended due to misunderstanding of the Act, etc.

b. Some members pointed out that the heightened awareness of privacy has led to the occurrence of problems such as those following: information sharing between welfare and disaster prevention departments at the same local government has been disturbed; sharing of information on persons needing assistance between welfare commissioners or voluntary disaster relief organizations has been prevented; and welfare commissioners are finding it difficult to perform their activities in an efficient manner.

(3) Discussions on the expansion of scenarios in which personal data may be provided without the consent of the owner

Concerning the scenarios in which personal data may be provided without the consent of the owner of such data, members made following comments.

a. General matters

· Most cases of “overreaction” can be resolved if the right principles are correctly disseminated through guidelines. If some problems cannot be resolved with the current legislation, it will be necessary to revise the relevant laws or regulations.

- Overall, the number of cases of “overreaction” has started to slow. “Overreactions” have occurred as Japanese society as a whole had in the past been generally indifferent to personal information. However, personal information can no longer be handled as easily as before. We must wait and see what measures to take until the real intention of the Personal Information Protection Act is fully understood by Japanese nationals.
- In reality, most of the cases of “overreaction” reported to the Quality-of-Life Policy Council fall under the category in which personal data may be provided without the consent of the owner as specified under the Personal Information Protection Act.
- Emergency phone lists at schools will be useless if some persons are not included for the simple reason that they have refused to provide their personal information.
- The preparation and distribution of name lists of alumni associations should be judged by these associations considering compliance matters.

b. Clarification of the intention of the Act

- To help reduce the occurrence of cases of “overreaction,” it is necessary to consider the usefulness of personal information in a clearer and more concrete manner in the Personal Information Protection Act.

c. Principle of interest balancing

- It is recommended to introduce a clause in which a general principle of interest balancing is used as a basis in cases in which that personal data may be provided without the consent of the owner.
- If a general principle of interest balancing is introduced, the protection and use of personal information may be unbalanced.
- If a general principle of interest balancing is introduced, it will be necessary to enhance the rights of owners of personal information by obligating the disclosure of the name of the party providing such personal information.

d. Cases in which the provision of personal data is based on laws and regulations

- It is recommended to include cases in which “personal information is made public conventionally” in the category under which personal data may be provided without the consent of the owner.
- The concept that “personal information is made public conventionally” concerns the accountability of the Government, and therefore it is inappropriate to include this concept in the code of behavior for private entities.

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

- It is recommended to include cases in which the provision of personal data is needed for the protection of “safety” or “existence” of a person in the category of “the provision of personal data is necessary for the protection of the life, body or property of an individual” (Item 2, paragraph 1, Article 23 of the Personal Information Protection Act).

f. Cases in which the provision of personal data is necessary to cooperate with a state organ, a local

government or an individual entrusted by such an organ

- In cases in which the provision of personal data is necessary to cooperate with the State, etc., it is recommended to clearly note that personal data may be provided without the consent of the owner of such personal data, if a certain activity is in the public interest or needed for the performance of government services, or if there is no possibility of infringement of rights or interests and there is a reasonable reason.

- It is recommended to include cases of cooperation with incorporated administrative agencies, etc. in the category that it is necessary to cooperate with the State, etc.

- The scope of the term “an individual entrusted by such organ” is unclear.

- It is possible to clarify the scope of the term “an individual entrusted by such organ” through interpretation or actual application.

g. Relationship with ordinances

- Some ordinances of local governments lack a clause similar to the provision of the Administrative Organs’ Personal Information Protection Act, which deems that personal data may be provided for unintended purposes. This may be one of the reasons why so-called “overreactions” have taken place. To assist local governments in responding to the protection of personal data in a more flexible manner, or help them revise their ordinances, it is urgent that fundamental portions of the Personal Information Protection Act be revised.

- It should be noted that local governments established an ordinance for the protection of personal information before the State enacted the Personal Information Protection Act. It should also be noted that local governments have promoted related efforts in the general trend towards decentralization.

(4) Direction of future studies

At the Government level, common consent was gained at the Inter-Ministerial Liaison Meeting on the Protection of Personal Information in February 2006 (hereinafter, “Common Consent of Related Ministries.”) The Government as a whole should enhance its efforts, including in regard to raising awareness of the personal information protection system among citizens and entities and clarifying concrete cases involving the provision of personal data to third parties.

a. Non-provision of personal information due to misunderstanding of the Personal Information Protection Act

Even in cases provided for under the Act in which personal information may be provided to third parties without the consent of the owner, there exist some cases in which personal information is not provided due to misunderstanding of the Act.

Based on the Common Consent of Related Ministries, etc., therefore, the Cabinet Office now makes efforts to clarify the interpretation and the application standard of the Personal Information Protection Act, while related ministries make efforts to revise guidelines, explanations, etc. by sector, when necessary. From now on, the Government will be required to make these efforts in order to have the public and entities fully understand the intention of the Act.

b. Objects that can be prepared with the consent of the owner of personal information

Personal information may be provided with the consent of the owner of personal information under the Personal Information Protection Act.

On the back of heightened awareness of privacy and other factors, however, there are some cases in which various name lists cannot be prepared as before largely because owners of personal information have refused to cooperate, or spare their time, in the preparation of such documents.

i) In view of these problems, it is important first of all to publicize the concrete contents of the Act concerning the procedures for preparing and distributing such tools as name lists and educate the public in regard to this point.

ii) Paragraph 1, Article 23 of the Personal Information Protection Act stipulates, “A business entity handling personal information shall not provide, in principle, personal data to a third party without obtaining the prior consent of the person.” However, in certain cases specified by laws or regulations, or in cases in which personal data is necessary for the protection of life, body or property of an individual but it is difficult to obtain the consent of the owner, or in other specific cases, it is specified in the Act that such personal data may be provided without the consent of the owner. In consideration of the intention of the Act, namely that the usefulness of personal information is properly exploited and at the same time the rights and interests of individuals are protected, it will be necessary to properly apply the current provision (Paragraph 1, Article 23 of the Personal Information Protection Act) that personal data may be provided without the consent of the owner of such personal data.

If cases occur that do not fall under the said provision but have a reason similar to that mentioned in the current provision, it will be necessary to fully understand the actual situation and study whether or not personal data may be provided without the consent of the owner or not on an individual basis. In relation, it should be noted that according to the Public Opinion Poll, approximately 70% of respondents feel uneasy in regard to the protection of personal information due to a suspicion that their personal information could be used for unfair purposes unbeknown to them, or that their personal information could be provided to third parties without their consent.

iii) Article 11 of the Personal Information Protection Act stipulates that “Local governments shall endeavor to take the necessary measures in order to ensure the proper handling of the personal information they hold.” At present, all prefectures and municipalities have established related ordinances. Since there have been some cases in which information sharing between related departments at the same local government has been disturbed, all local governments are required to properly interpret and apply their ordinances with reference to the Administrative Organs’ Personal Information Protection Act, and to publicize and educate the public on the intention of the Personal Information Protection Act.

According to the Public Opinion Poll, approximately 10% of respondents have refused to provide their details for a list; 8% of this figure simply didn’t want to be involved in community activities (there reasoning had nothing to do with the Personal Information Protection Act). Approximately 90% of them feared that such name lists could be used for unintended purposes or illegally disclosed to unknown persons. In some cases, the Personal Information Protection Act has been used to excuse their refusal to cooperate in community

activities.

On the contrary, however, there have been cases in which the Act has played a role in helping residents deepen understanding of community activities, including disaster prevention activities as well as those to prevent crime and boost general welfare.

In consideration of these conditions, it will be important for each local government to make concerted efforts to obtain local residents' understanding of the purpose or intention of community activities that require the preparation of name lists or information sharing, and to also ensure that personal data they hold is maintained in a secure manner.

## 2. Publicity and education

### (1) Current conditions

- a. To facilitate the protection of personal information, the Basic Policy deems it extremely important to fully publicize the personal information protection system on the details of the system through various media, including the Internet, posters, pamphlets and explanatory meetings among the public and entities, and requires that the Cabinet Office and each ministry publicize and educate the public and entities.

The Common Consent of Related Ministries emphasizes the importance of government-wide efforts to publicize the personal information protection system among the public and entities, and to clarify concrete examples of cases in which personal data may be provided to third parties.

- b. Based on the Basic Policy and the Common Consent of Related Ministries, the Cabinet Office and each ministry are now making efforts to publicize and raise public awareness of the personal information protection system among the general public and entities through various media, including websites, individual publicity materials and explanatory meetings.

### (2) Problems

The public and entities are evidently becoming more and more aware of the existence of the Personal Information Protection Act. However, the specific contents of the Act and the existence of related grievance desks are less well known. The points, for example, are little known.

- 1) There are cases in which personal data may be provided to a third party without the consent of the owner.
- 2) Any personal data contained in a name list may be provided to a third party with the consent of the owner.
- 3) Any person may ask a private entity or an administrative organ to disclose any retained personal data on him/her being held.

### (3) Direction of future studies

To help mitigate so-called "overreaction" and promote public-based activities to protect and

utilize personal information, it will be essential to publicize the objectives and contents of the Personal Information Protection Act among the public and entities in a more concrete way through various media, including the Internet, the preparation and distribution of pamphlets or posters, and explanatory meetings.

### **III. Objects to be Protected and Business entities Handling Personal Information Required to Perform Certain Duties**

1. About the system under which all personal information is treated in a similar way under the Personal Information Protection Act

1) Objects to be protected

(1) Current conditions

a. Paragraph 1, Article 2 of the Personal Information Protection Act stipulates, “The term ‘personal information’ shall mean information about a living individual which can identify the specific individual.”

b. Paragraph 2, Article 2 of the Act stipulates, “The term ‘a personal information database, etc.’ shall mean an assembly of information including personal information, and an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer, or a similar assembly.”

Paragraph 4, Article 2 of the Act stipulates, “The term ‘personal data’ shall mean personal information constituting a personal information database, etc.”

c. Paragraph 5, Article 2 of the Act and Article 4 of the Cabinet Order for the Enforcement of the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003; hereinafter, “Personal Information Protection Act Enforcement Cabinet Order”) stipulate, “The term ‘retained personal data’ shall mean such personal data over which an entity handling personal information has the authority to disclose, or other authorities, excluding data which will harm public or other interests if its presence or absence is known and data that will be erased within six months.”

d. Under the Personal Information Protection Act, “personal information” is protected when it is acquired or utilized, “personal data” is protected when it is managed or provided, and “retained personal data” is protected when the owner of the personal data is involved.

e. The Organization for Economic Co-operation and Development (OECD) defines the “objects to be protected” as “all kinds of information related to individuals (owners of the data) that is or can be identified.” The international practice is that the “objects to be protected” are defined in a broad sense, as in Japan.

(2) Problems

Some members suggested that the definition of the “objects to be protected” should be revised.

(3) Direction of future studies

Under the Personal Information Protection Act, the “objects to be protected” are categorized into three groups—personal information, personal data and retained personal data—according to the necessity of protection and the possibility of performance of duties. In some countries overseas, mainly data that is automatically processed or can be managed in files is protected, although there are differences from country to country. In consideration of these conditions, it can be safely said that the definition, etc. of “personal information” in Japan is almost in harmony with that being used in countries overseas.

\* For the proper protection of personal information of the deceased, please refer to IX.

2) Special measures

(1) Current conditions

With respect to “personal information for which strict implementation of its proper handling especially needs to be ensured for the further protection of the rights and interests of individuals in view of the nature and the method of utilization of the personal information” (Article 6 of the Personal Information Protection Act,) acts on businesses, including those in the medical care, finance/credit, telecommunications, etc., sectors have established confidentiality provisions, and various rules and guidelines have defined strict safety control measures. With respect to personal credit information, in particular, the Money Lending Business Act, revised and promulgated in December 2006 (Act No.32 of 1983), adopts a provision that the use of this information by a money lender for purposes other than predetermined ones shall be penalized.

(2) Problems

In some sectors, high-level protection of personal information is demanded by the public, and this information is handled in a fairly rigid manner. Some members commented that these cases should be utilized as good examples.

(3) Direction of future studies

For individual sectors in which personal information needs to be handled in a fairly rigid manner, respective acts on businesses have established confidentiality provisions, and various rules and guidelines have defined strict safety control measures. Therefore, it is essential to pay close attention to the development of the protection of personal information under the current framework.

2. Scope of business entities handling personal information required to perform certain duties

(1) Current conditions

a. Article 3 (Basic Principle) of the Personal Information Protection Act stipulates, “In view of

the fact that personal information should be handled cautiously under the philosophy of respecting the personalities of individuals, proper handling of personal information should be promoted.”

A business entity using a personal information database, etc. for its business is defined as a business entity handling personal information (Paragraph 3, Article 2 of the Act.) The Act imposes certain duties on business entities handling personal information with the aim of preventing the infringement of rights or interests of individuals.

b. Article 2 of the Cabinet Order for the Enforcement of the Act on the Protection of Personal Information stipulates that if, in the case of an entity, the total number of specific individuals identified by the personal information constituting a personal information database, etc. used for its business does not exceed 5,000 on any day during the past six months, the entity shall be excluded from the definition of a business entity handling personal information by reason that the entity can be considered an entity having little likelihood to harm the rights and interests of individuals considering the volume and manner of utilization of the personal information they handle.

c. Of 35 guidelines for the protection of personal information covering 22 business sectors in total, 14 guidelines obligate small entities to perform certain duties, 17 require that they make an effort to perform certain duties, and four exclude them from the definition of a business entity handling personal information (as of May 31, 2007).

(2) Problems

Some members pointed out that all entities, whether they are considered a business entity handling personal information under the Personal Information Protection Act or not, should be obligated to perform certain duties by reason that personal information should be properly handled for the protection of the rights and interests of individuals, and that many foreign countries impose certain duties on such entities despite the volume of personal information they handle.

(3) Direction of future studies

In Japan, if, in the case of an entity, the total number of subjects for which they hold personal information does not exceed 5,000, the entity is excluded from the definition of a business entity handling personal information under the Personal Information Protection Act by reason that the entity can be considered as an entity having little likelihood to harm the rights and interests of individuals considering the volume and the manner of utilization of the personal information they handle. This exclusion was formulated in due consideration of the burdens on entities and the relatively small risk of infringement of the rights and interests of individuals as well as the actual condition of the personal information held by such entities.

In view of the possible performance of certain duties under the Personal Information Protection Act, it can be safely said that the current practice of determining a business entity handling personal information depending on the volume of personal information held by an entity is appropriate at present.

#### **IV. Efforts of Entities, etc.**

1. General efforts of entities, etc.

1) Appropriate guidelines, etc.

(1) Current conditions

a. Article 8 of the Personal Information Protection Act stipulates, In order to support the activities performed by entities and others to ensure the proper handling of personal information, the State shall provide information, formulate guidelines to ensure the appropriate and effective implementation of measures to be taken by entities and others, and take any other necessary measures.

b. Considering that the rules established by the Personal Information Protection Act set minimum requirements only, the Basic Policy requires that each ministry establish or revise guidelines depending on actual conditions of each business sector as soon as possible and provide business associations, etc. with information, advice, etc. when they voluntarily prepare guidelines.

c. As of May 31, 2007, related ministries with jurisdiction over business, etc. have established 35 guidelines for 22 business sectors in total.

d. In some cases, two or more guidelines apply to a single entity.

(2) Problems

Some members made comment on the guidelines as follows:

a. Concrete cases of interpretation and flexible application of the Personal Information Protection Act should be clearly indicated.

b. The existence of some differences among various guidelines is unavoidable because under the relevant minister, each ministry establishes guidelines, etc. depending on the actual conditions of business sectors.

c. Certain portions of guidelines, etc. may be standardized and shared by all business sectors.

(3) Direction of future studies

As for the indication of concrete cases of interpretation and flexible application of the Act, the Cabinet Office and related ministries have so far revised guidelines or related explanations as the case may be in collaboration with one another. In the future, too, the Cabinet Office and related ministries should continue such efforts.

Under the competent minister, each ministry establishes guidelines, etc. depending on the actual conditions of business sectors. Therefore, it is natural that there exist some differences among

various guidelines. Since there are some cases that two or more guidelines apply to a single entity, however, the Government should study the standardization of various guidelines. In doing so, the Government needs to assess the actual conditions of business sectors, and examine the diffusion and compliance of current guidelines.

2) Assistance, etc. to entities

(1) Current conditions

a. Article 8 of the Personal Information Protection Act stipulates, in order to support the measures for the protection of personal information formulated or implemented by local governments and the activities performed by citizens, entities and others to ensure the proper handling of personal information, the State shall provide information, formulate guidelines to ensure the appropriate and effective implementation of measures to be taken by entities and others and take any other necessary measures.

b. The Basic Policy entails the following requirements: Each ministry needs to place a priority on “the transparency of measures taken by entities through the establishment and publicity of their privacy policy, etc.” in its guidelines, etc., and each entity must take these measures on a priority basis.

c. Certain local governments and private organizations implement certification systems for entities that conduct activities at a certain level or higher for the protection of personal information, or a registration system that summarizes customers’ personal information.

d. Related ministries conduct activities to publicize and educate on effective measures as assistance to small and medium-sized enterprises (SMEs.) The “tax measures for enhancement of information infrastructure” are taken for SMEs. Low interest loans under the policy finance system are also available to SMEs.

e. Some members pointed out that certification and registration systems implemented by certain local governments and private organizations are effective in promoting activities for the protection of personal information because such systems require an particular organizational or technical response when certification or registration is made or renewed.

2) Problems

a. Some entities find it burdensome to earnestly conduct activities for the protection of personal information, while others are less serious in taking the measures required under the Personal Information Protection Act.

b. Some members pointed out that many SMEs and micro enterprises do not fall under the category of a business entity handling personal information and therefore these enterprises’ efforts for the protection of personal information fall short.

- c. Some members pointed out that many SMEs find it costly to manage information, etc. appropriately.
  - d. Some members pointed out that it is necessary for a greater number of entities to voluntarily establish and publicize their privacy policy.
- (3) Direction of future studies
- a. Privacy policy  
It is necessary for a greater number of entities to voluntarily establish and publicize a privacy policy.
  - b. Information management costs, etc.  
It is necessary to take various measures, including organizing seminars, so that SMEs, micro enterprises, etc. may be well informed of the content of the Personal Information Protection Act and concrete examples of safety control measures may be disseminated. At the same time, it is advisable that all available support measures be utilized to improve safety control measures of SMEs, micro enterprises, etc.
- 3) Enhancement of supervision over entities
- (1) Current conditions
- a. The Personal Information Protection Act establishes common minimum rules for general entities, and expects that each entity will autonomously make an every effort to protect personal information in consideration of its actual business conditions. With the aim of securing effective compliance, therefore, the Act establishes provisions concerning “the collection of reports by the competent minister” (Article 32); “advice from the competent minister” (Article 33); “recommendations and orders from the competent minister” (Article 34); and “penalties against violation of orders” (Article 56).
  - b. The Basic Policy establishes the following conditions, and related efforts are carried out.
    - i) If a case of large scale leakage of personal information should occur, each ministry shall make an effort to collect the necessary information and rapidly examine and take appropriate countermeasures in consideration of the extent of damage and social influence.
    - ii) With the cooperation of related ministries, the Cabinet Office shall accumulate and categorize cases of large-scale leakage of personal information and provide each ministry with the necessary information.
    - iii) The Cabinet Office and related ministries shall receive or collect from grievance organs, etc. information on crooked entities, and provide these organs, etc. with the responses, etc. of related ministries, if necessary.
  - c. There have been cases of criminal acts through the misuse of name lists. In one particular case, the

personal information of several millions of individuals was leaked.

Among the cases where a person with access authority duplicates personal information using a medium held by the person and removes the said information from the premises cannot be punished as no adequate laws or regulations applicable to such cases exists. Considering the possibility of the occurrence of similar cases, some members pointed out that merely enhancing supervision over entities will not be enough.

- d. With respect to large-scale cases or malicious leakage of personal information, each relevant minister submits a recommendation to, or collects a report from, the entity concerned as the entity is obliged to take safety control measures and supervise its employees and contractors.
- e. As for which portions of personal information can be categorized as a “trade secret,” entities are required to properly manage such trade secrets through access control, etc. in accordance with the provisions of the Unfair Competition Prevention Act (Act No.47 of 1993) and the Guidelines for Trade Secret Management (prepared by the Ministry of Economy, Trade and Industry on January 30, 2003 [revised on October 12, 2005]).
- f. Some entities utilize working regulations, etc. to prevent their employees from handling personal information in an inappropriate manner.

(2) Problems

Some members pointed out that supervision over crooked entities should be strengthened. Other members pointed out that with respect to cases of large-scale or malicious leakage of personal information, each relevant minister should more strictly exercise his/her authority under the Personal Information Protection Act.

(3) Direction of future studies

- a. With the aim of securing appropriate handling of personal information, the Personal Information Protection Act grants each relevant minister supervisory authority by which each minister can make recommendations or issue orders. As the case may be, penalties, etc. under related laws and regulations, including the Penal Code (Act No.45 of 1907) may be applied to cases of infringement of the rights or interests of individuals. In view of preceding sentences, it is essential to continue to apply the Personal Information Protection Act, etc. in a more rigorous manner, including the proper exercise of each relevant Minister’s authority against entities.
- b. Name lists, etc. could potentially be used to commit vicious crimes. Therefore, as before, entities are required to take the necessary and proper measures to ensure safe management of personal data, including adequate management of personal data as a trade secret and utilizing working regulations, etc. to prevent employees from conducting illegal acts. At the same time, it is advisable that an investigation agency and related organs respond to these cases in collaboration to the extent that criminal investigations may not be hampered.

It is also advisable that further studies be made to prevent employees from leaking personal information held by entities.

2. Acquisition, utilization, discontinuance of utilization and erasure

(1) Current conditions

a. In the Personal Information Protection Act there exist the following provisions concerning the acquisition, utilization, discontinuance of the utilization and erasure by a business entity handling personal information.

i) When handling personal information, a business entity handling personal information shall specify the purpose of utilization of personal information (hereinafter, the “Purpose of Utilization”) as much as possible. (Article 15)

ii) In principle, a business entity handling personal information shall not handle personal information without obtaining the prior consent of the person concerned, beyond the scope necessary for the achievement of the Purpose of Utilization. (Article 16)

iii) A business entity handling personal information shall not acquire personal information by deception or other wrongful means. (Article 17)

iv) In principle, when having acquired personal information, a business entity handling personal information shall, except in cases in which the Purpose of Utilization has already been publicly announced, promptly notify the person of the Purpose of Utilization or publicly announce the Purpose of Utilization. (Paragraph 1, Article 18)

v) When a business entity handling personal information acquires such personal information on a person as is written in a document directly from the person, the business entity shall expressly show the Purpose of Utilization in advance. (Paragraph 2, Article 18)

vi) Where a business entity handling personal information is requested by a person to discontinue using or to erase retained personal data on the grounds that the retained personal data is being handled in violation of the restriction by the Purpose of Utilization or obligations of proper acquisition, and where it is found that the request has a reason, the business entity shall discontinue using or erase the retained personal data concerned without delay to the extent necessary to redress the violation. (Article 27)

b. Paragraph 1, Article 31 of the Personal Information Protection Act stipulates, “A business entity handling personal information shall endeavor to appropriately and promptly process complaints about the handling of personal information.”

(2) Problems

a. Some members pointed out that business activities can be adversely affected since it is rather difficult to acquire personal information or utilize their means, including through the use of direct mails. Other members pointed out that certain measures should be taken to prevent the improper use of personal information for unintended purposes (the Personal Information Protection Act has provisions concerning the discontinuance of utilization and erasure of personal information in the case of its use

for unintended purposes).

- b. Under the Act, a person may request a business entity handling personal information to discontinue use or erasure of retained personal data only if the personal information was acquired in an unfair manner or is being handled in violation of legal provisions. However, some members doubted the appropriateness of this single measure.
- c. Even after the enactment of the Act, the number of spam e-mails, random telephone sales calls, direct mails, etc. has not decreased in the slightest. Some members pointed out that this is one of the reasons for so-called “overreactions.” Other members pointed out that random telephone sales calls should be banned because they can cause stress, or damage, to consumers.

(3) Direction of future studies

- a. Although some members pointed out that it is rather difficult to acquire personal information or utilize unsolicited communication tools such as direct mails, other members feared that name lists could be used for unintended purposes.

In the cases of the United Kingdom and Germany, the conditions of a request for the discontinuance of utilization or erasure of personal data are broadly defined. In the United Kingdom, in particular, the owner of personal data holds the right to demand the discontinuance of utilization of such data for the purpose of direct marketing.

Certain entities make it clear in their privacy policy or direct mails that if requested by owners of personal information, they will discontinue the delivery of direct mails to them.

If requested to discontinue the utilization of personal information, etc., an entity must immediately take the proper measure as part of processing of complaints under Article 31 of the Personal Information Protection Act. On the other hand, certain entities make it clear in their privacy policy, etc. that if requested, they will be ready to discontinue utilizing personal information, etc. Therefore, it is necessary to pay attention to these efforts for the protection of the rights and interests of individuals, and to take the necessary measures to promote these efforts, including reviewing the Basic Policy, etc.

- b. Spam e-mails and random telephone sales calls are regulated by the Act on Regulation of Transmission of Specified Electronic Mail (Act No.26 of 2002) and the Act on Specified Transactions (Act No.57 of 2003), respectively. Grievance desks of Consumer Affairs Centers, etc. give advice for individual cases of direct mail-related problem.

It is necessary to regulate cases of utilization of personal information for unintended purposes through the exploitation or coordinated use of such tools/systems.

3. Proper safety control

- 1) Level of safety control measures

- (1) Current conditions

- a. Article 20 of the Personal Information Protection Act stipulates, a business entity handling personal information shall take the necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.
- b. The risk of occurrence of IT-related accidents is not certain, and therefore it is difficult to make a decision on proper investment in information security. In March 2005, therefore, the “Study Group on Enterprises’ Information Security Governance” of the Ministry of Economy, Trade and Industry developed the Benchmark for Information Security Measures as an indicator for investment decisions with the aim of establishing a basis for information security governance (the establishment and implementation of a system of corporate governance that also places priority on social responsibilities and a system of internal control supporting corporate governance from the viewpoint of information security).
- c. The “Guideline for the Business and Industry Sector with Respect to the Act on the Protection of Personal Information” (established jointly by the Ministry of Health, Labour and Welfare and the Ministry of Economy, Trade and Industry on October 22, 2004 [revised on March 20, 2007]; hereinafter, “Guideline for the Business and Industry Sector”) requires that a business entity handling personal information take necessary and proper measures depending on the risks involved in consideration of the extent of infringement of rights and interests of persons if their personal data is leaked, for example.
- d. In February 2006, the Information Security Policy Council finalized a three-year medium and long-term plan titled “Toward the Realization of the First Information Security Basic Plan (Secure Japan.)” Based on this Basic Plan, an annual plan is prepared every year. Secure Japan 2007, finalized in June 2007, mentions the need to establish an information sharing system, the need to study a method to quantify information security risks for enterprises and the development of human resources concerned in addition to the need for measures to educate individuals.
- e. To promote organized information security measures, the Ministry of Economy, Trade and Industry implements the following three policies:
  - i) Diffusion and promotion of the Information Security Management System (ISMS), a certification scheme based on international standards and implemented by an independent organization.
  - ii) Promotion of information security audit systems such as the above based on national standards implemented by an independent organization.
  - iii) Formulation of information security governance concepts in which information security measures are considered to affect management risks.
- f. In the private sector, a system is being implemented that objectively evaluates whether an organization’s security measures satisfy certain standards or not.

(2) Problems

The required conditions of safety control measures vary depending on changes in the social environment. The main issue is to what extent safety control measures should be taken.

(3) Direction of future studies

- a. Safety control measures that can meet the conditions required and depending on the technological progress or changes in social environment need to be taken.
- b. The risks involved in information leakage differ from business sector to business sector. Therefore, entities need to take proper safety control measures in view of more defined possible risks characteristic of the business environment they operate in.
- c. It is important for entities to improve their information security measures based on the Government's information security policy. Therefore, it is essential for the Government to implement measures to promote efforts of entities and the development of human resources, and disseminate the necessary information/knowledge.
- d. The information security certification system, etc. can be considered to be effective and informative in improving safety control measures for the protection of personal information.

2) Supervision over employees

(1) Current conditions

- a. Article 21 of the Personal Information Protection Act stipulates, when a business entity handling personal information has an employee handle personal data, it shall exercise necessary and appropriate supervision over the employee to ensure the security control of the personal data.
- b. The Basic Policy states that in order to ensure appropriate protection of personal information handled by an entity, including the prevention of leakage, etc. of personal information, it is important for the entity to educate or train employees who handle personal information in daily business activities so they well understand the significance of protecting personal information.
- c. The "Guideline for Measures to Be Taken by Entities to Ensure the Proper Treatment of Personal Information for Employment Management" (established by the Ministry of Health, Labour and Welfare on July 1, 2004; hereinafter, "Employment Management Guideline") and the Guideline for the Business and Industry Sector allow for the following:
  - i) It is advisable that when important matters on handling of personal information for employment management are established, prior notice be given to trade union(s), etc. and a consultation be held as needed.
  - ii) It is advisable that when above-mentioned important matters are established, employees be notified, etc.
- d. The Guideline for the Business and Industry Sector states that matters related to monitoring (the term

“monitoring” means supervision of employees at work utilizing cameras, etc.) represent a priority issue concerning the treatment of personal information for employment management (refer to the above “c. i)”) contained in the Guideline for the Business and Industry Sector and the Employment Management Guideline, and that attention should be paid to the following points:

- i) The purpose of monitoring should be clarified in advance, included in the internal regulations, and made known to the employees.
- ii) A person responsible for monitoring and his authority should be determined.
- iii) Before monitoring is implemented, a draft of the internal regulations containing a provision concerning the monitoring should be established and made fully known to employees.
- iv) An audit should be carried out to verify whether monitoring is being implemented in a fair manner.

(2) Problems

Some members made comments on the supervision of employees as follows:

- a. In certain business sectors in which advanced safety control measures are required, employees are excessively burdened with efforts geared toward the protection of personal information.
- b. The precondition for supervision over employees for the purpose of protection of personal information is the correction of entities’ insufficient understanding of the Personal Information Protection Act, etc. and the rectification of inadequate training of employees.
- c. Before monitoring is implemented, it is important to follow proper procedures, including consultation between management and employees.
- d. Written pledges signed by employees sometimes contain a clause that trade secrets should be protected and an infringing employee would be obligated to pay damages. However, it is necessary to treat employees in a proper manner.

(3) Direction of future studies

It is natural for entities to conduct proper supervision over their employees under labor-related laws and regulations. However, entities are required to treat their employees in a fair manner in consideration of the comments indicated in (2) above.

Furthermore, it is advisable that guidelines, etc. be reviewed with reference to descriptions in the above (1) c and d and promoted in a proper manner depending on the actual conditions of each business sector.

3) Supervision over contractors

(1) Current conditions

- a. Article 22 of the Personal Information Protection Act stipulates, when a business entity handling personal information commissions an individual or a business entity to handle personal data in whole or in part, it shall exercise necessary and appropriate supervision over the contractor to ensure the security control of the personal data.
- b. Item 1, paragraph 4, Article 23 of the Act stipulates, the contractor shall not be deemed a third party

in cases in which a business entity handling personal information commissions the handling of a personal data in whole or in part within the scope necessary for the achievement of the Purpose of Utilization. Therefore, the acquisition of consent of the owner of the personal data before providing the contractor with the personal data is unnecessary.

- c. The Basic Policy states as follows: when a business entity handling personal information commissions an external contractor to handle personal information, it is important for the business entity handling the personal information and the contractor to sign a service agreement in which the responsibilities, etc. of both parties are clarified and the contractor is required to take measures to prevent leakages of personal information. This is so that the business entity handling the personal information can ensure an effective system of supervision over the contractor. This should include supervision over a sub-contractor.

(2) Problems

- a. When a business entity handling personal information commissions an external contractor to handle personal information, or when the business entity handling personal information allows the contractor to re-commission a sub-contractor to handle the personal information, the business entity handling the personal information more often than not requires the contractor and/or the sub-contractor to take safety control measures in an even more stringent manner.
- b. Consumers (including owners of personal information), etc. are generally not aware of how their personal information is handled, especially in cases where a business entity handling personal information commissions an external contractor to handle the said personal information. Therefore, the fact of whether the handling of personal information is outsourced or not should be made known to consumers, etc.

(3) Direction of future studies

a. Supervision over contractor

To ensure the credibility of its business, a business entity handling personal information needs to require a contractor and/or a sub-contractor handling personal information to take safety control measures in a proper manner.

b. Disclosure of the outsourcing process

As for the disclosure of the process of outsourcing the handling of personal information, some members require that a business entity handling personal information be obligated to disclose the names of contractors, while others comment that this matter should be examined carefully in consideration of the feasibility of disclosure of the names of all contractors, confidentiality obligations imposed on business entities, etc.

Since the outsourcing relationship often changes in business activities from time to time, it may be difficult for a business entity handling personal information to disclose the names of contractors.

On the other hand, certain business entities handling personal information mention matters

related to outsourcing (whether outsourcing is happening or not, the contents of the outsourced activities, etc.) in their privacy policy, etc. It is therefore necessary to pay attention to these efforts in order to protect the rights and interests of individuals, and to take necessary measures to promote these efforts, including reviewing the Basic Policy, etc.

4) Management of commercial name lists held by entities

(1) Current conditions

a. Article 20 of the Personal Information Protection Act stipulates, a business entity handling personal information shall take necessary and proper measures for the prevention of leakage, loss or damage, and for other security control of the personal data.

b. As for telephone directories and car navigation systems, it is generally understood that whole or a part of the personal information database, etc. contained therein is prepared by third parties, and that they only contain names, addresses or whereabouts, or telephone numbers. Therefore, if these directories, etc. are used for business without being edited or processed, the information contained therein is excluded from the cases to which the condition concerning “the number of specific individuals identified by personal information constituting a personal information database, etc. used for the business” applies in connection with the requirements of a business entity handling personal information. (Article 2 of the Personal Information Protection Act Enforcement Cabinet Order)

c. The Guideline for the Business and Industry Sector states as follows: Even if a business entity handling personal information disposes a commercial name list, which can be easily purchased by any person at a book store, (on the condition that the commercial name list is in no way processed by the business entity) without using shredder, etc., or causes the commercial name list to be collected by a junk dealer, the business entity will not be deemed to be in breach of duties of safety control measures (or of duties related to the supervision of employees or contractors).

d. The Guideline for the Business and Industry Sector further states as follows: As for telephone directories and car navigation systems, etc., the possibility cannot be denied that personal information constituting such directories, etc. may be regarded as persona data. However, it can be safely said that it is not necessary to impose certain duties on business entities handling personal information because the business entity will likely least infringe the rights and interests of individuals in view of how such directories, etc. are used.

(2) Problems

It is necessary that widely distributed name lists, including commercial ones, be managed in the same way as other personal data. However, it can be said that these widely distributed name lists should be treated differently from other personal data in due consideration of the necessity of protection of the rights and interests of individuals and realistic management by entities.

(3) Direction of future studies

Even if widely distributed name lists, etc., including commercial ones, are maintained by a business entity handling personal information, the business entity is least likely to infringe the rights and interests of individuals. In addition, it is necessary to request these business entities to take realistic control measures. Accordingly, any of the following responses will be considered reasonable:

- i) Under the Personal Information Protection Act, a business entity handling personal information is required to take “necessary and proper” measures for the security control of the personal data. Therefore, the Basic Policy should be reviewed so that such security control measures will be taken for widely distributed name lists, etc.
- ii) In the case of widely distributed name lists, etc. as well, a study will be conducted with a view to revising the Personal Information Protection Act Enforcement Cabinet Order to exclude cases involving widely distributed name lists, etc., as for the case of telephone directories, etc., from the cases to which the condition concerning “the number of specific individuals identified by personal information constituting a personal information database, etc. used for the business” applies.

In the case of widely distributed name lists, etc., it is necessary to further examine their scope. It can be safely said that these name lists may include those of qualified experts, career information, addresses, etc. of distinguished persons, publications containing information concerning corporate officers, other commercial name lists, and name lists disclosed on the websites.

#### 4. Restrictions on provision of data to third parties

##### (1) Current conditions

- a. Article 23 of the Personal Information Protection Act stipulates, a business entity handling personal information shall not, except for cases specified in laws and regulations and other specified cases, provide personal data to a third party without obtaining the prior consent of the person.
- b. Paragraph 4, Article 23 of the Act stipulates that the individual or business entity receiving such personal data shall not be deemed a third party in any of the following cases: i) such personal data is provided to a contractor; ii) such personal data is provided pursuant to a merger, etc.; or iii) such personal data is jointly used within a group. This is because the owner of such personal data may reasonably deem that the business entity handling personal information and the individual or business entity receiving such personal data constitute the same party.
- c. Concerning the Purpose of Utilization and the scope of joint users, the Act stipulates as follows.
  - i) Cases that such personal data is provided to a contractor: The individual or business entity receiving such personal data shall not be deemed a third party if they are merely engaged in the service “within the scope necessary for the achievement of the Purpose of Utilization.” (Item 1, paragraph 4 of Article 23)
  - ii) Cases that such personal data is provided pursuant to a merger, etc.: The individual or business entity receiving such personal data must obtain the prior consent of the person if they wish to handle the personal information “beyond the scope necessary for the

achievement of the Purpose of Utilization of the personal information concerned before the succession.” (Paragraph 2 of Article 16)

- iii) Case that such personal data is jointly used in a group: “The scope of the joint users, the purpose for which the personal data is used” is, in advance, notified to the person (Item 3, paragraph 4 of Article 23), and “the purpose for which the personal data is used” shall be revised only after having obtained the prior consent of the person. (Paragraph 5 of Article 23)

(2) Problems

Some members doubted if the current conditions—the Purpose of Utilization or the scope of the joint users—are appropriate for cases of outsourcing handling of personal data, mergers, etc. and the joint use of personal data.

(3) Direction of future studies

Considering that some members asked for the imposition of restrictions on the Purpose of Utilization or the scope of the joint users in the cases of outsourcing of handling of personal data, merger, etc. and the joint use of personal data, it is necessary for a business entity handling personal information to determine the appropriate scope of use of personal data for the benefit of consumers, etc. (including the owner of personal data). For example, clarification of the Purpose of Utilization or the scope of the joint users in the cases of outsourcing of handling of personal data, merger, etc. and the joint use of personal data.

Other members asked for the relaxation of conditions for the joint use of personal data. Under the current framework, however, it is possible to request business entities handling personal information to clarify their Purpose of Utilization or the scope of the joint users in cases pertaining to outsourcing of personal data, mergers, etc and the joint use of personal data. Therefore, it will be sufficient for business entities handling personal information to determine a proper privacy policy, etc. depending on the particulars of their business operations.

5. Relationship with consumers, etc. (including the owners of personal information)

1) Purpose of utilization determined by entities

(1) Current conditions

- a. Article 15 of the Personal Information Protection Act stipulates, when handling personal information, a business entity handling personal information shall specify the purpose of utilization of personal information (hereinafter, “Purpose of Utilization”) as much as possible.

The term “shall specify ... as much as possible” means that business operations and the purposes for which personal information is to be used must be clarified in a concrete form as far as possible. In other words, the above provision asks for detailed specification of the Purpose of Utilization as far as possible instead of abstract or general specification thereof.

b. The Guideline for the Business and Industry Sector mentions “the delivery of products, information on new products, and related after-sales services in the field of XX business” as an example of specification of the Purpose of Utilization. It is desirable that the term “XX business” be specified pursuant to socially accepted ideas so that the owner of personal information may easily understand it. For example, it is widely accepted that “XX business” be specified using the term of middle or smaller grouping in the Standard Industrial Classification for Japan.

(2) Problems

Some members pointed out that there are cases in which the scope of the Purpose of Utilization specified by business entities handling personal information is too wide. For example, business operations for which personal information is used include all of those specified in their articles of incorporation or contribution. These members asked for improvements thereof.

(3) Direction of future studies

If a business entity handling personal information conducts diversified business operations, it may include all of those specified in its articles of incorporation or contribution in the scope of the Purpose of Utilization specified by the business entity.

Even under these conditions, however, certain business entities handling personal information establish the limited scope of the Purpose of Utilization for each type of customer in their privacy policy, etc. with the aim of informing the owner of the personal information of its business activities and the purposes for which personal information is used. These efforts should be taken into consideration in order to protect the rights and interests of individuals. It will be necessary to take appropriate measures, including a review of the Basic Policy, to promote these efforts.

One potential measure may be to allow the owner of personal information to select from among the Purposes of Utilization.

2) Disclosure of the name of party from whom information has been obtained

(1) Current conditions

Paragraph 1, Article 25 of the Personal Information Protection Act stipulates, when a business entity handling personal information is requested by a person to disclose such retained personal data as may lead to the identification of the person, the business entity shall, in principle, disclose the retained personal data without delay. This provision implies that a business entity handling personal information is not required to inform consumers, etc. (including owners of personal information) of the name of the party from whom the personal data has been obtained, unless the retained personal data contains the name of the party.

(2) Problems

Members made the following comments on the disclosure of the name of the party from whom personal information has been obtained.

a. Under the Personal Information Protection Act, a business entity handling personal information is not

required to inform consumers, etc. (including owners of personal information) of the name of the party from whom the personal data has been obtained. However, some members asked for the disclosure of the name of the party. What responses may be reasonable?

- b. Many consumers, etc. (including owners of personal information) tend to hold misgivings since the name of the party from whom personal data has been obtained is not given. Therefore, it seems to be important to obligate a business entity handling personal information to mention the names of the main parties from whom personal data is obtained in their privacy policy, etc. to help erase fears of consumers, etc. (including owners of personal information).

(3) Direction of future studies

Some members pointed out that the name of the party from whom personal data has been obtained should be disclosed for the benefit of owners of personal information. Other members, however, stated that information on the name of the party from whom personal data has been obtained should not be disclosed in a uniform manner as this kind of individual management will hamper the business activities of business entities, and that this matter should be examined more carefully.

In the EU, consumers have a right to ask for the disclosure of the name of a party from whom personal data has been obtained.

Even in Japan, certain business entities handling personal information clarify, as concretely as possible, the manner of procurement of personal information—the name of a party from whom personal data is obtained, the types of sources from which personal data is procured, and other related matters—in their privacy policy in advance. These efforts should be taken into consideration for the protection of the rights and interests of individuals. It will be necessary to take appropriate measures, including reviewing the Basic Policy, to promote these efforts.

## V. **Function of Authorized Personal Information Protection Organizations**

(1) Current conditions

- a. The Personal Information Protection Act establishes a system that authorizes a private organization to act as an authorized personal information protection organization. The purpose of this system is to help maintain the credibility of private organizations that conduct activities to ensure proper handling of personal information, and to facilitate and promote such activities by private organizations.
- b. Paragraph 1, Article 37 of the Act stipulates that an authorized personal information protection organization shall conduct the following activities:
  - i) The processing of complaints about the handling of personal information of such business operations handling personal information as the targets of the business (hereinafter, “target entities”) (Item 1)
  - ii) The provision of information for target entities,” including the preparation and publicity of the personal information protection guidelines (Item 2)
  - iii) Any business necessary for ensuring the proper handling of personal information by target entities (Item 3)

- c. The Basic Policy states as follows: It is expected that authorized personal information protection organizations as private organizations will be able to play an extremely important role in voluntarily processing complaints. For example, these organizations may assist business entities handling personal information in making their own efforts to process complaints so that such problems may be resolved voluntarily and practically. They may also assist business entities through the establishment of guidelines, etc. Therefore, it is important to fully utilize this system.

Each ministry is expected to contribute to the promotion of designating authorized personal information protection organizations, through the provision of information or advice to business associations, etc.

- d. As of May 31, 2007, a total of 34 such organizations had been approved by a total number of five relevant ministers as authorized personal information protection organizations in accordance with the provisions of Article 37 of the Personal Information Protection Act.

(2) Problems

In the case of leakages, etc. of personal information, it is important not only for target entities and competent ministries to take measures but also for authorized personal information protection organizations to provide target entities with instructions and advice. Therefore, it is expected authorized personal information protection organizations will work to enhance their functions.

(3) Direction of future studies

Under Articles 42 and 43 of the Personal Information Protection Act, authorized personal information protection organizations process complaints regarding the manner of handling of personal information by target entities, request target entities to make explanations and submit materials, and provide target entities with instructions and advice to ensure compliance with personal information protection guidelines.

However, some members pointed out that there are differences in the activities and actual work carried out by authorized personal information protection organizations. Therefore, less active authorized personal information protection organizations are expected to proactively process complaints and provide information to target entities in the future.

In some business sectors, the number of authorized personal information protection organizations is insufficient. Therefore, it is advisable that ministries with jurisdiction over these business sectors activate authorization activities.

From now on, it will be important to fully publicize the roles of authorized personal information protection organizations to the public and entities and to make efforts to help improve confidence in these organizations. In addition, it will be necessary for these organizations to proactively engage in personal information leakage cases in order to further enhance their functions.

It may be advisable for these organizations to exchange opinions among themselves in order to share knowledge.

## **VI. Processing Complaints**

### (1) Current conditions

- a. Article 31 of the Personal Information Protection Act stipulates, a business entity handling personal information shall endeavor to appropriately and promptly process complaints.
- b. Article 42 of the Act stipulates, when an authorized personal information protection organization is requested by a person, etc. to solve a complaint about a target business entity, the organization shall offer the person, etc. the necessary advice, investigate the circumstances pertinent to the complaint and request the target business entity to outline the content of the complaint.
- c. Article 13 of the Act stipulates, in order to ensure that complaints are handled appropriately and promptly, a local government shall endeavor to mediate the processing of complaints and take other necessary measures. Article 9 of the Act stipulates, the State shall take necessary measures to ensure the appropriate, prompt processing of complaints.
- d. The Basic Policy states that many of the grievances or complaints related to personal information may be appropriately resolved through complaint processing, not by way of lawsuit, etc., from the viewpoint of promptness and economy. In addition, the Basic Policy states that the multilayered structure for processing complaints can function smoothly only if related organizations properly perform their roles and maintain close coordination.
- e. The Basic Policy states that the National Consumer Affairs Center of Japan (NCACJ) shall engage in offering advice on personal information and contribute to the enhancement of various grievance desks through activities such as the development of consulting staff with expertise by way of training, etc. and the preparation and distribution of manuals on complaint processing in collaboration with various grievance organs, including Consumer Affairs Centers, etc. In addition, the Basic Policy states that the NCACJ shall carry out the above activities with the cooperation of authorized personal information protection organizations, etc., if necessary, and distribute manuals to these organizations and participate in training programs for staff of these organizations.

In addition, the Basic Policy states that the NCACJ shall collect from various grievance organs, and analyze, cases of complaints relating to personal information and prepare reference materials such as a “summary of individual complaints and responses” so that knowledge obtainable from the “summary of individual complaints and responses” may be accumulated and shared among the concerned parties.

Thus, the NCACJ prepares and distributes copies of the “Manual on Complaint Processing for Personal Information” and the “Summary of Personal Information Protection-related Complaints and Responses,” collects examples of complaints and responses, and conducts training programs for consulting staff engaged in personal information protection.

- f. Both the Cabinet Office and the NCACJ has established and operates its own system for collecting cases of personal information-related complaints and responses for the purpose of information sharing. In June 2006, these two organizations began to exchange data accumulated in respective systems with one another.
  - g. Each ministry exchanges opinions on complaints and responses with authorized personal information protection organizations.
- (2) Problems
- Some members pointed out that grievance desks should be networked so that they may share information on actual complaints and responses and thereby process complaints in a more efficient manner.
- (3) Direction of future studies
- A complaint about the handling of personal information may be filed with: 1) the business entity concerned; 2) an authorized personal information protection organization; 3) a local government department such as a Consumer Affairs Center; or 4) the NCACJ.
- The system for authorized personal information protection organizations should be enhanced through the promotion of designation of authorized personal information protection organizations and the provision of information on complaints raised with concerned business so that complaints raised by consumers, etc. may be processed more smoothly.
- To process complaints more smoothly, various organizations need to effectively cooperate with the NCACJ, Consumer Affairs Centers, authorized personal information protection organizations, etc. through the sharing of information on actual cases of complaints and responses.

## **VII. Compliance with International Rules**

- (1) Current conditions
- a. An example of international efforts for the protection of personal information is the “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” (hereinafter, the “OECD Guidelines”). The eight principles indicated in the OECD Guidelines work as the basis of international and national efforts thereafter. Japan’s personal information protection system is based on the OECD Guidelines.
  - b. The United Nations adopted the “United Nations Guidelines on Computerized Personal Data Files” in 1990.
  - c. The OECD promotes efforts in line with the OECD Guidelines. Recently, it has been studying the enforcement of each member country’s privacy law to cross-border problems.
  - d. The EU has adopted the “Directive 95/46/EC of the European Parliament and of the Council of 24

October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.” This Directive obligates member countries to establish legislation that allows for the movement of personal data to a third country, in principle, only if the third country has established adequate level protective measures.

- e. The Asia Pacific Economic Cooperation (APEC) established the APEC Privacy Framework in November 2005. APEC is currently looking into the establishment of cross-border privacy rules, etc. although in a manner different from that of the EU.

(2) Problems

The protection of personal information requires common infrastructures throughout the world. Therefore, global viewpoints, such as international frameworks, are important.

Some members pointed out that it is a problem that Japan’s laws have no explicit provisions concerning the international movement of information.

(3) Direction of future studies

- a. The OECD is studying the enforcement of each member country’s privacy law to cross-border problems. The APEC is studying the establishment of cross-border privacy rules, and problems related to information sharing and cross-border cooperation in investigations and law enforcement.
- b. It is essential to promote international cooperation based on efforts made by the OECD, APEC, the EU, etc. At the same time, it is important to make an effort to ask the international community to better understand Japan’s personal information protection system.
- c. When it becomes necessary to examine Japan’s personal information protection system in the future, it will be essential to pay due attention to the actual conditions of the system as well as international moves concerning the protection of personal information.

## **VIII. Significance of Independent Organizations**

(1) Current conditions

- a. The duties of entities handling personal information specified in Chapter 4 of the Personal Information Protection Act are imposed for personal information used for business. Therefore, a relevant minister with jurisdiction over each business sector is given administrative responsibility and authority to ensure proper handling of personal information in the business sector.
- b. As of May 31 of 2007, ministries with jurisdiction over business, etc. have established 35 guidelines for 22 business sectors in total. Each relevant minister guides and supervises entities, etc.
- c. As of May 31 of 2007, 34 organizations had been designated as authorized personal information protection organization by relevant ministers in accordance with the provisions of Article 37 of the Act.

(2) Problems

In many countries overseas, independent organizations enforce a personal information protection act.

(3) Direction of future studies

In Japan, personal information is handled by private entities as part of their business operations, and therefore is indispensable to their business. In addition, the methods of handling personal information are varied in their characteristics, largely depending on the type and condition of each business. To ensure proper handling of personal information, therefore, it is extremely important to take a specific approach for each type of business, and it is reasonable and effective to simultaneously supervise business operations and handling of personal information by these entities.

Considering the above, it is reasonable to maintain the system in which the relevant minister holds sway. It is also necessary to study the establishment of independent organizations as a medium or long-term task in view of compatibility with international practices.

Reference: As an international example, an independent organization is required to meet the following conditions (please refer to the below-mentioned note.) In consideration of the conditions concerning autonomy, independence, proper scope of functions and enforcement authority under laws or regulations, it seems take steps for Japanese organizations to meet these conditions.

- i) Must be a public body established on an appropriate legal grounds.
- ii) Must be guaranteed an appropriate degree of autonomy and independence to perform its duties.

As for autonomy, it must be given legal authority to take proper measures without obtaining the approval of a third party. It must have independence to enable it to operate free from political and governmental interference and to withstand the influence of vested interests.

- iii) The law under which the authority operates must be compatible with the principal international instruments dealing with data protection and privacy.
- iv) Must have an appropriate range of functions with the legal powers necessary to perform those functions. An independent organization for data protection must have certain functions in areas such as compliance, supervision, investigation, redress, guidance, public education, etc. The independent organization must merely be advisory but must have supervisory powers with legal and administrative consequences.

Note: The “Criteria and Rules for Credentials Committee and the Accreditation Principles” (adopted by the International Conference of Data Protection Commissioners on September 25, 2001 [revised by the International Conference of Data Protection and Privacy Commissioners on September 9, 2002.]

## **IX. Protection of Personal Information for the Dead**

### (1) Current conditions

- a. The purpose of the Personal Information Protection Act is to prevent the occurrence of the infringement of rights and interests of the owners of personal information. The Act has no intention to protect personal information concerning deceased persons and thereby protect the rights and interests of their surviving families. Under the Act, “personal information” is limited to that of living individuals. Under the Act, therefore, only if certain information on a dead person constitutes personal information of any of the surviving family members, the information of the deceased person is protected as the personal information of the living person(s).
- b. The “Guidelines for the Proper Handling of Personal Information by Medical or Nursing Care Entities” (established by the Ministry of Health, Labour and Welfare on December 24, 2004 (revised on April 21, 2006); hereinafter, “Medical and Nursing Care Guidelines”) state as follows: If a medical or nursing care entity retains certain information of a certain patient or user even after the patient or user has passed away, the medical or nursing care entity shall take the same safety control measures as those taken for living individuals in order to prevent the information from being leaked, lost or damaged.
- c. The “Guidelines for Provision, etc. of Medical Treatment Information” (established by the Ministry of Health, Labour and Welfare on September 12, 2003; hereinafter, “Medical Treatment Information Guidelines”) state as follows:
  - i) If a patient passes away, a medical worker shall immediately provide the surviving family with information concerning the patient’s medical care up to the time/cause of death, etc.
  - ii) If requested by the surviving family (spouse, child, father, mother or equivalent) a medical worker shall provide the surviving family with information concerning the medical treatment record.
  - iii) When providing the surviving family with medical care information, a medical worker shall fully respect the patient’s wishes before death, honor, etc.
- d. Some countries overseas have enacted special laws pertaining to the handling of personal information of dead persons. In Japan, certain medical institutions belonging to local governments have established their own guidelines containing the handling of personal information of dead persons.

### (2) Problems

Some members pointed out that it is rather a problem that the Current Act only protects the personal information of living persons.

### (3) Direction of future studies

At present, the Medical and Nursing Care Guidelines and the Medical Treatment Information Guidelines specify necessary measures to be taken for the protection of personal information of the dead. Therefore, it will be appropriate to pay close attention to related developments.

## **X. Others**

1. Handling of personal information held by state administrative organs
  - (1) Current conditions
    - a. Paragraphs 1 and 2, Article 8 of the Administrative Organs' Personal Information Protection Act stipulate, In any of the cases i) there exist relevant laws or regulations; ii) the consent of the owner of personal information is obtained; and iii) there is a special reason for the provision of retained personal information, a state administrative organ may, in principle, use for itself, or provide to a third party, retained personal information for purposes other than the Purpose of Utilization.
    - b. The "Treatment of Names of Public Employees by Each Administrative Organ" (August 3, 2005; the Common Consent of the Liaison Conference on Information Disclosure) states that each administrative organ shall disclose the names of public employees belonging to the administrative organ contained in the information concerning the performance of duties by the employee, unless there is a possibility that a particular problem will take place.
    - c. Under Article 5 of the "Act on Access to Information Held by Administrative Organs" (Act No.42 of 1999; hereinafter, "Act on Access to Information,") personal information is deemed to be inaccessible information. Of: i) information that is disclosed, or scheduled to be disclosed, pursuant to provisions of laws and regulations or customary practice; and ii) information concerning the performance of duties of public employees, personal information concerning the position and performance of duties of a public employee is excluded from the inaccessible information. Therefore, if a request for disclosure is made under the Act on Access to Information, any information that is not deemed as inaccessible information must be disclosed. (The name of a public employee belonging to an administrative organ that is contained in the information concerning the performance of duties by the employee, which can be disclosed under Common Consent, falls under the category, "information that is disclosed, or scheduled to be disclosed, pursuant to customary practice." Therefore, the name will be disclosed.)
    - d. Cases in which personal information is disclosed upon request for disclosure under the Act on Access to Information falls under "cases in which there exist relevant laws or regulations," for which the provision of such information is permitted under the Administrative Organs' Personal Information Protection Act. Therefore, the Administrative Organs' Personal Information Protection Act does not prevent disclosure under the Act on Access to Information.
    - e. Despite the fact that disclosure should be carried out under the Act on Access to Information and has been happened in the past, some administrative organs discontinued publicizing brief personal records

of senior public employees on the grounds that the Administrative Organs' Personal Information Protection Act had been enacted.

(2) Problems

Some members pointed out that some state administrative organs discontinued disclosing such information, or that there exist gaps between the contents of disclosed information of senior public employees. Other members pointed out that these problems should be resolved in connection with information disclosure principles.

(3) Direction of future studies

The "Manner of Disclosure of Brief Personal Data of Senior Public Employees by State Administrative Organ" (Notice from Director-General, Administrative Management Bureau, the Ministry of Internal Affairs and Communications dated May 22, 2007) was prepared with the aim of providing information as far as possible required for ensuring citizens' confidence in administrative activities, and with the purpose of applying the Administrative Organs' Personal Information Protection Act in a uniform manner.

As mentioned above, state administrative organs are allowed to disclose personal information if disclosure is justified under the Administrative Organs' Personal Information Protection Act. Therefore, it is important to apply the Act in a proper manner in consideration of the significance of the provision of information.

For this purpose, it will be necessary to improve administrative management as the case may be under the framework of the current laws.

2. Efforts of local governments

(1) Current conditions

a. Contents and operation of ordinances

i) Articles 5 and 11 of the Personal Information Protection Act stipulate, "Local governments shall be responsible for formulating and implementing the measures necessary for ensuring the proper handling of personal information according to the characteristics of their area in conformity of the purport of this Act" and "Local governments shall endeavor to take necessary measures in order to ensure the proper handling of the personal information they hold," respectively.

ii) The Ministry of Internal Affairs and Communications has notified each local government that municipalities should begin preparations to establish an ordinance for the protection of personal information as soon as possible, if one does not already exist, in view of the purposes of the provisions of the Personal Information Protection Act and of the Administrative Organs' Personal Information Protection Act, and that any municipality that has already established an ordinance should now review it in consideration of the content of the Administrative Organs' Personal Information Protection Act (Notice from Director-General for Policy Planning, the Ministry of Internal Affairs and Communications

dated June 16, 2003).

- iii) As of April 2006, all local governments (prefectures, cities, wards, towns and villages) have their own ordinance for the protection of personal information.
- iv) The Ministry of Internal Affairs and Communications requires each local government to include a provision concerning manually processed information, and establish provisions concerning disclosure of cases of inappropriate handling of personal information and amendments, regulations for outsourcing, complaint processing and grievance procedures, and punishment of violations, with reference to the Administrative Organs' Personal Information Protection Act. All local governments are required to review these provisions on an annual basis.

b. Cooperation with local communities

- i) In March 2006, the Cabinet Office (the section in charge of disaster prevention) established the "Guidelines for the Evacuation of Persons in Need of Assistance at a Time of Disaster," and submitted the Guidelines to each local government. The Guidelines lay down the correct method of handling personal information in the case that local governments and communities cooperate with each other in preparing an evacuation plan for persons in need of assistance during times of disaster. The Guidelines recommend that each local government adopt a provision for its ordinance for the protection of personal information—the use of retained personal information for purposes other than the Purpose of Utilization and permission to hand such information to third parties are allowed under the provision—and share, from time to time, such information on persons in need of assistance held by welfare departments, etc. with related organizations, including disaster prevention departments, voluntary disaster relief organizations and welfare commissioners, without obtaining the consent of the persons in need of assistance. In April 2007, the Cabinet Office prepared a handbook to the Guidelines concerning concrete procedures to take measures for persons in need of assistance as well as related examples, and submitted this to all local governments.
- ii) Welfare commissioners play the role of institution representatives cooperating with administrative authorities and the role of employees in charge of local welfare. As they are required to perform confidentiality obligations under the Welfare Commissioners Act, the Ministry of Health, Labour and Welfare requires each local government to provide these commissioners with personal information in a proper and appropriate manner.

(2) Problems

Some members raised questions or made comments as follows:

- a. Is the intention of the Personal Information Protection Act reflected in the ordinance of each local government or its application?
- b. Isn't it a problem that the contents or application of an ordinance differs from local government to local government?

- c. It would surely be useful to establish certain criteria for handling personal information in cases in which local governments and community organizations cooperate with one another in the fields of disaster, crime prevention, community welfare, etc.
- d. It is important to improve the level of such efforts for the protection of personal information conducted by organizations related to local governments.

(3) Direction of future studies

a. Contents and operation of ordinances

In view of the general trend towards decentralization, Article 5 of the Personal Information Protection Act stipulates, local governments shall be responsible for formulating and implementing the measures necessary for ensuring the proper handling of personal information according to the characteristics of their area in conformity of the purport of this Act. Therefore, the Government should request local governments to ensure personal information is handled properly in view of the intention of the Act, and provide them with necessary information on related efforts, etc. taken by the Government.

As for the provision of personal information to third parties, there have been overreactions within certain elements of the public. Therefore, it is recommended that local governments make efforts to interpret and implement their ordinances in a proper manner with reference to the Administrative Organs' Personal Information Protection Act, and actively carry out related activities to educate the public on the real intention of the Personal Information Protection Act.

b. Cooperation with local communities

For the case that local governments and community organizations cooperate with each other in the fields of disaster prevention, local welfare, etc., each ministry in charge of related measures needs to examine how to handle personal information, and urge local governments to share examples of their efforts with other local governments.

To help improve the level of such efforts for the protection of personal information conducted by organizations related to local governments, it is desirable to ensure these organizations are entirely familiar with the personal information protection system.

## Concluding Remarks

This "Summary of Opinions on the Protection of Personal Information" was prepared at the 20th session of the Quality of Life Policy Council after a wide-scale examination of the conditions surrounding the protection of personal information in view of the development of affairs following the full enactment of the Personal Information Protection Act. This Summary of Recommendations on the Protection of Personal Information contains such recommendations for problems that are at this stage starting to appear.

At the meetings of the Quality of Life Policy Council, many points of arguments concerning the ideals of personal information protection, including those concerning the optimum balance between protection and utilization of personal information, were raised. In particular, a consensus was formed that if

“overreactions” were found inappropriate, the problem should be resolved as soon as possible, since the diversified use of personal information is becoming increasingly indispensable not only to business activities but also to public life.

Even now, the intention of the Personal Information Protection Act seems to be rather widely misunderstood. This is one of the main reasons for the overreactions. It is strongly recommended, therefore, that the Government make every effort to implement the measures explained in this Summary of Opinions including, for example, the review of the Basic Policy, the review of Guidelines and their explanations as the case may be, and publicity and education on the detailed contents of the Act. Considering the fact that cases of overreaction are being found within certain elements of the public, it is also recommended that local governments make efforts to interpret and implement their ordinances and actively carry out related activities to educate local residents.

Various discussions took place not only on cases of “overreaction” but also on the enhanced protection of the rights and interests of individuals and the ideal state of independent organizations, etc. and these matters should be examined on a continual basis. Since the protection of personal information requires responses or measures that can reflect changes in economic and social conditions, it will be also necessary to examine this matter from this viewpoint. When studying related systems, due attention should be paid to the trend of international studies carried out by the OECD, APEC and similar.

The Quality-of-Life Policy Council believes that in the annual follow-up of how the Personal Information Protection Act is being applied, the effects of the above-mentioned measures against “overreactions” should be assessed and the circumstances surrounding various problems related to the protection of personal information closely observed. In addition, further measures should be studied, including the necessity of revising of related laws and regulations.

Last but not the least, it is recommended that the Government share the information on these problems, conduct the necessary deliberations from now on, and make further efforts to promote correct understanding of the Personal Information Protection Act among entities and citizens.