NOVEMBER 2005


# PERSONAL INFORMATION PROTECTION LAW IN JAPAN

The Personal Information Protection Act (Law No. 57 of 2003) (hereinafter referred to as "Act"), which was promulgated on May 23, 2003, became fully effective on April 1, 2005, as to the private sector.[1] The Act aims to "protect the rights and interests of individuals while taking consideration of the usefulness of personal information, in view of a remarkable increase in the use of personal information due to development of the advanced information and communications society" (Article 1).

It is very important to note that the Act constitutes only a part of Japan's privacy regulatory framework. The Act outlines only general requirements and obligations, leaving the details of its regulation and interpretation to the government ministries, which issue administrative guidelines for those business sectors for which they are responsible. The purpose of these ministerial guidelines is twofold:

*1) To clarify the legal interpretation of the Act.* As stated above, the Act outlines only general requirements. Therefore, these ministerial guidelines aim to provide guidance to businesses as to how to comply with the Act, by explaining various terms used in the Act, examples of measures to be taken, and so on.

*2) To set out additional desirable items to promote voluntary efforts.* The guidelines contain both mandatory and desirable provisions. As the nature and manner of using personal information and the scale of risks associated therewith vary from one industry to another, the Act provides only for minimum obligations and leaves each ministerial guideline to set up sector-specific desirable measures to satisfy the specific needs in each business sector.

The provisions of the guidelines may not always be the same, in terms of measures to be taken to meet

1. The provisions relating to obligations of the national government or local governments became effective on May 30, 2003. The official English translation of the Act is available at http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf.

general requirements provided in the Act. Therefore, companies operating in Japan must carefully read the ministerial guidelines that apply to each business. It is also important to note that each business is subject to at least two guidelines and possibly more. This is because employment data is governed by "Guidelines Regarding Measures to Be Taken by Businesses to Ensure Adequate Handling of Personal Information Regarding Employment Management" issued by the Ministry of Health, Labour and Welfare ("MHLW"). All businesses are subject to the above MHLW guidelines ("MHLW Employment Guidelines"), while each individual business should be subject to those ministerial guidelines that specifically govern the business in which it is engaged. Although we refer to guidelines in some points of this memorandum, it does not cover the full analysis and explanation of the various guidelines.

## BASIC CONCEPTS

**Personal Information.** In the Act, "Personal Information" is defined as "information about a living individual which can identify the specific individual by name, date of birth, or other description (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual") (Article 2, Paragraph 1). This definition is very broad and includes even public information, such as information in the phone book, public journals, and personnel lists. "Person" for the purposes of the Act refers to a specific individual who may be identified through the Personal Information (Article 2, Paragraph 6).

**Personal Information Database, Etc.** "Personal Information Database, Etc." is defined in the Act as any collection of information, including Personal Information, systematically created to enable searching of specific Personal Information using electronic computation equipment or any other method that is systematically organized to facilitate the searching of specific Personal Information as designated by government order (Article 2, Paragraph 2) (hereinafter referred to as "Personal Information Database"). As is clear from the definition, a Personal Information Database may include Personal Information not processed by computer. If a database is indexed in such a way that items can be easily retrieved using a table of contents, index, or similar reference (*e.g.,* a business-card holder), such database would fall under the definition of Personal Information Database (Article 1 of the Cabinet's Enforcement Order of the Act).

**Entity Handling Personal Information.** The Act applies to an entity handling Personal Information, which is an entity that uses as part of its operations a Personal Information Database, excluding (i) national institutions, (ii) local public entities, (iii) independent administrative agencies subject to another statute regulating their collection and use of Personal Information, and (iv) any entity designated by government order as presenting *de minimis* risk of impinging on individual rights and interests based on the method with which it uses Personal Information and the volume of Personal Information at issue (hereinafter referred to as the "Entity") (Article 2, Paragraph 3). According to the Cabinet's Enforcement Order of the Act, entities handling the Personal Information of not more than 5,000 individuals at any time during the period of the last six months shall be exempted (Article 2 of the Cabinet Order).

**Personal Data.** "Personal Data" is defined as Personal Information stored on a Personal Information Database (Article 2, Paragraph 4).

## OBLIGATIONS OF THE ENTITY UNDER THE ACT

**How Do We Acquire Personal Information?** *Purpose of Use*. The Entity must describe, as specifically as possible, the purposes of using Personal Information ("Purpose of Use") (Article 15, Paragraph 1). Merely expressing the Purpose of Use in abstract terms does not meet this requirement. For instance, according to "Guidelines Targeting the Economic Industrial Sector Regarding the Personal Information Protection Law" issued by the Ministry of Economy, Trade and Industry ("METI Guidelines"), a statement that the Personal Information is intended "for use in business activities" "to improve the quality of services" or "for use in marketing activities" is not sufficient.

*Notice or Public Announcement of Purpose of Use*. In the event that the Entity obtains Personal Information, it shall immediately notify the Person of the Purpose of Use or make a public announcement, unless the Entity has made a public announcement of the Purpose of Use in advance (Article 18, Paragraph 1). Further, if Personal Information is directly

acquired from the Person in writing (contract, other document, web page, etc.), the Entity must clearly indicate the Purpose of Use in advance (Article 18, Paragraph 2).

*No Unjust Method of Collecting Personal Information.* The Entity shall not collect and gather Personal Information through deceit or other unfair or fraudulent means (Article 17).

**How Do You Use Personal Information?** The Entity shall not exceed the scope of the Purpose of Use unless it obtains the prior consent of the Person (Article 16, Paragraph 1).

**How Can You Share Personal Data With Third Parties?** The Entity shall not transfer Personal Data to any third party without the prior consent of the Person, except in the following instances: (i) such transfer is required by law; (ii) such transfer is required to protect a person's life, bodily safety, or property, and obtaining prior consent of the Person presents undue hardship; (iii) such transfer is required to promote public health or positive child development, and obtaining prior consent of the Person presents undue hardship; or (iv) such transfer is required for agents of national institutions and local public entities to perform their duties, and obtaining prior consent of the Person presents undue hardship (Article 23, Paragraph 1).

In this connection, it is very important to note that a "third party" includes an affiliated company, and therefore, in principle, the Entity cannot share the Personal Data with its affiliated companies without obtaining consent of the Person concerned.

As an exception to the above general prohibition, the Entity can share the Personal Data with third parties in the following cases:

*Opt-Out Exception (Article 23, Paragraph 2).* The Entity must, prior to provision of Personal Data, provide the Person with notice or place the Person in circumstances whereby the Person can easily learn of the following information and suspend the provision to the third party at the Person's request:

- That the provision to the third party is established as the Purpose of Use.
- The specific contents of the Personal Data provided to the third party.
- The means or methods of providing the Personal Data to the third party.
- That the provision to the third party will cease at the request of the Person.

*Delegation (Article 23, Paragraph 4, Item 1).* In cases where Personal Data is entrusted to another person/entity (*e.g.,* a data-processing company) to the extent necessary to achieve the Purpose of Use of that Personal Data, the Entity may transfer the data without obtaining the consent of the Person. It should be noted, however, that the Entity is responsible for the supervision of such delegates for proper handling of Personal Data (Article 22). The METI Guidelines and other guidelines require that the Entity must enter into an agreement setting out the responsibilities of such delegates to protect the Personal Data.

*Merger, etc. (Article 23, Paragraph 4, Item 2).* When the Personal Data is provided to another company in accordance with succession to business operations for reasons such as a merger, the Entity need not obtain consent of the Person. It should be noted that the METI Guidelines clearly state that providing the Personal Data to a third party in the process of pre-contractual negotiations (such as due diligence) does not fall within this exception. According to the METI, to comply with the Act, the target company needs to make the Personal Data anonymous before providing the information for the purpose of due diligence, unless it obtains the Person's consent or uses the opt-out exception.

*Joint Use (Article 23, Paragraph 4, Item 3).* The purpose of this joint use exception is to allow the Entity to share the Personal Data with, typically, affiliated companies. To avail itself of this joint use exception, the Entity, prior to information sharing, must provide the Person with notice or place the Person in circumstances whereby the Person can easily learn of the following information:

- The fact that the Personal Data is to be jointly used.
- The items of the Personal Data to be jointly used.
- The parties that are to jointly use the Personal Data.
- The purpose of the joint use of the Personal Data.
- The name or title of the entity or person responsible for the management of the joint use of the Personal Data.

**How Do You Need to Manage Security of the Personal Data?**
*Data Integrity.* The Entity shall use its best efforts to ensure that the collection and use of Personal Data by the Entity falls within the limits of the Purpose of Use and that the Personal Data is accurate and updated (Article 19).

*Security Control Measures.* The Entity shall take necessary and appropriate measures to prevent the loss, destruction, damage, or unauthorized disclosure of the Personal Data and shall take other measures to ensure the secure management of Personal Data (Article 20). Such security control measures include organizational, personnel, physical, and technical security control measures. The METI Guidelines set forth general requirements for such security control measures, by providing detailed examples of how to meet these requirements.

In addition, the Entity shall appropriately supervise its employees who collect and use Personal Information and cause them to implement and abide by the security measures described above (Article 21). As already discussed in connection with the transfer of the Personal Data, the Entity, when delegating the task of collecting and processing Personal Data to a contractor or other outside consultant, in whole or in part, shall appropriately supervise such contractor or consultant and cause it to implement and abide by the security measures described above (Article 22).

**Access and Correction.** Upon request by the Person, the Entity shall disclose and deliver to the Person making the request, without delay and through the means prescribed by government order, the Personal Data held by such Entity. No such disclosure and delivery, in whole or in part, shall be required under any of the following instances: (i) the risk of injury to the life or bodily safety of the Person or a third party or the risk of impinging on the rights and interests of the Person or a third party or their property exists as a result of such disclosure and delivery; (ii) such disclosure and delivery would result in a material interference with the Entity's operations; or (iii) such disclosure and delivery would result in a violation of other laws (Article 25, Paragraph 1).

Further, the Entity shall provide the Person with an opportunity to revise, correct, supplement, or delete Personal Data in the event that such Personal Data is inaccurate (Article 26). The Act also requires the Entity to provide the Person with an opportunity to request cessation of use or deletion of the Personal Data in the event that the Entity is in violation of the requirements enunciated in the Purpose of Use provision above or the Personal Data has been obtained by unjust means (Article 27).

## ENFORCEMENT

Failure to comply with the Act may result in administrative penalties. The competent minister may issue recommendation for corrective measures to the Entity in breach, and if the Entity does not follow such recommendation, the competent minister may issue an order (Article 34). If the Entity does not comply with the order issued by the competent minister, the person in breach of such order shall be liable to imprisonment for up to six months or a fine of not more than 300,000 Japanese yen (Article 56). A company shall also be liable for a fine of not more than 300,000 Japanese yen when its representative, agent, employee, or any other person engaged has breached such order in the course of its business (Article 58).

## REPORTING/PUBLICATION IN CASE OF LEAKAGE OR DATA LOSS

Some ministerial guidelines[2] provide that in the event the Personal Data is leaked or lost, it is mandatory to report this to the Person affected and the competent ministry. Further, these guidelines require the Entity to publicly announce such data leakage or data loss incident to the extent possible. Though most guidelines state that such reporting or publication is only desirable, or are silent on this issue, as a matter of practice, once such an incident happens, most Japanese companies report the incidents to the Persons affected and the competent ministries on a voluntary basis.

2. "Practical Guidance on Security Control Measures, etc., in the Guidelines Regarding Personal Information Protection in the Financial Business" issued by the Financial Services Agency, "Guidelines on Personal Information Protection in the Credit Industry in the Economic and Industrial Sector" issued by METI, and "Guidelines on Protection of Personal Information in the Telecommunication Business" issued by the Ministry of Internal Affairs and Communication.

## BASIC ACTION CHECKLIST

For your convenience, below is a basic action checklist, although this is not a comprehensive list.

**Review of Your Business Model and Process.**

- Identify and list the Personal Information that you already hold and the Personal Information that you collect and use (including both employment data and customer data).
- Specify the Purpose of Use of the Personal Information already held by your company, as well as of the Personal Information that will be collected.
- Ensure that the Personal Information is being and will be used only for such specified Purpose of Use.
- Review the documents and web pages through which you collect the Personal Information, and ensure that such documents and web pages include clear indications of the Purpose of Use.
- Determine whether you provide Personal Data to any third parties, including your affiliate companies.
- If the answer to the question above is yes, obtain the consent of the Person concerned before providing the Personal Data to such third parties except for the following cases:

    - Provision to delegates
    - Joint use
    - Opt-out
    - Merger, etc.

**Publication of Information Required Under the Act.** You need to place the Person in circumstances whereby he or she can easily find out (such as by reading on a web site or in a pamphlet) the following information. The first five points are mandatory, while the final point is only voluntary and desirable:

- The name of your company.
- The purpose of Use of all the Personal Data held by your company.
- Contact information for making a complaint.
- Matters regarding opt-out, if applicable.
- Matters regarding joint use, if applicable.
- Procedures for making a request for disclosure, correction, or cessation of use of the Personal Data held by your company.

You may meet this requirement by including all this information in the privacy statement to be placed on the web site.

**Security Control Measures.**

- Train employees on these new privacy rules and security measures.
- Have employees sign confidentiality agreements or covenants, if necessary.
- Review and revise work rules, if necessary.
- Review contracts with third-party delegates to ensure that they contain provisions regarding the protection of the Personal Information.
- Establish the section/person in charge of handling inquiries, complaints, and requests.
- Review current data security practices and internal policies/rules and make sure necessary security control measures are taken.

## LAWYER CONTACT

For further information, please contact your principal Firm representative or the lawyer listed below. General e-mail messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

**Michiru Takahashi**
81.3.6800.1821
mtakahashi@jonesday.com