Guidelines Relating to Measures to be taken by Businesses in Order to Ensure the Proper Handling of Personal Information Relating to Employment Management
(Commentary)

March, 2005

Counselor’s Office for Labor Policy
Director-General for Policy Planning, Ministry of Health, Labor and Welfare
Guidelines Relating to Measures to be taken by Businesses in Order to Ensure the Proper Handling of Personal Information Relating to Employment Management
(Commentary)

Table of Contents

Introduction........................................................................................................................................... 1

I. Purpose........................................................................................................................................... 2

II. Definitions ..................................................................................................................................... 5
  ○ Businesses.................................................................................................................................... 6
  ○ Worker, etc.................................................................................................................................... 9

III. Matters Serving As Guidelines for Appropriate and Effective Implementation of Measures Taken By Businesses............................................................................................................................................. 11
  1. Matters relating to specification of the purpose of use provided in Article 15 of the Law 11
  2. Matters relating to employee’s consent provided in Article 16 of the Law and Article 23 Paragraph 1 of the Law.................................................................................................................................................. 13
  3. Matters relating to security control measures provided by Article 20 of the Law and supervision of employees provided by Article 21 of the Law................................................................. 16
  4. Matters relating to supervision of delegates provided in Article 22 of the Law ............. 20
  5. Items related to provision to a third party which is stipulated by Article 23 of the Law 24
  6. Items related to disclosure of Held Personal Data that is stipulated by Article 25 Paragraph 1 of the Law.................................................................................................................................................. 27
  7. Items related to suitable measures in light of the convenience to the Principal, which is stipulated in Article 29 Paragraph 2 of the Law ................................................................. 29
  8. Items regarding handling grievances which is stipulated in Article 31 of the Law ..... 30
  9. Items that shall be taken into account when the Business Handling Personal Information must take measures to secure appropriate handling of Personal Information regarding employment management ............................................................................................................................................. 31

IV. Handling of Personal Information regarding employment management by a business other than the Business Handling Personal Information................................................................. 32

<Reference 1> Delegation, provision to a third party and joint use........................................... 33
<Reference 2> Provision of Personal Information regarding Employment Management . 34
<Reference 3> Issues to consider when handling employment management information concerning health information ............................................................................................................................................. 35
<Reference 4> Issues to consider in order to secure appropriate handling of personal information at the time of application for a job, temporary transfer to another company, change in employment and termination of employment ................................................................. 37
Introduction

- This Commentary was compiled as a concrete guide to support activities carried out by Businesses relating to ensuring proper handling of Personal Information with respect to employment management, in order to achieve appropriate and smooth application of the Guidelines Relating to Measures to be taken by Businesses in Order to Ensure the Proper Handling of Personal Information Relating to Employment Management (Ministry of Health, Labor and Welfare Notification 259, July 1, 2004; hereafter the “Guidelines”).

- This Commentary consists of a clause-by-clause commentary and the “Reference” section at the end. The “Reference” section at the end takes up, as topics, several points among those points considered to be important with regard to protection of Personal Information relating to employment management throughout the Law Concerning Protection of Personal Information (Law of 2003, No. 57), the Enforcement Order for the Law Concerning Protection of Personal Information (2003, Cabinet Order 507) and the Guidelines.

- If the portions of the Commentary stating [that they] “must” be done are not complied with, this shall be deemed by the Minister of Health, Labor and Welfare as a regulatory violation, and the Minister of Health, Labor and Welfare and other governing Minister of the business will together take procedures with respect to issuing an advisory, order or emergency order pursuant to Article 34 of the Law. Meanwhile, although it is not judged a regulatory violation if the portions stating [that they are] “asked” to be done are not complied with, from the perspective of promoting the protection of Personal Information relating to employment management, it is strongly hoped that they will be tackled.

- The examples given in the Commentary are typical examples, but even for those examples that can be interpreted as complying with the law, in fact each case must be examined individually while giving consideration to each business’s own circumstances, the range, etc. of the subject workers, and other matters.
I. Purpose

These Guidelines set forth the items required for appropriate and effective implementation of the measures to be carried out by businesses in order to ensure the proper handling of Personal Information relating to employment management with regard to the requirements of the Law Concerning Protection of Personal Information (hereafter, “the Law”).

With regard to Personal Information relating to employment management, guidelines and other required measures established by the Ministers or others with jurisdiction over the business carried on by the Personal Information handling Business concerned shall be heeded, in addition to these Guidelines.

[Relevant Clauses]

Law Article 1

In light of the dramatic expansion in the use of Personal Information in conjunction with the development of advanced information-telecommunication society, this Law has the purpose of protecting the rights and interests of individuals while considering the usefulness of Personal Information, through setting forth the basic philosophy and basic governmental policy with respect to the proper handling of Personal Information and the determination of matters which form the basis of measures concerning the protection of Personal Information, making explicit the duties, etc., of the national government and Local Public Entities, as well as setting forth obligations, etc., to be complied with by businesses which handle Personal Information.

Law Article 3

In view of the fact that Personal Information should be treated with care based on the philosophy of respect for personal privacy, Personal Information must be treated appropriately.

Law Article 8

The national government, in order to assist measures adopted and executed by Local Public Entities relating to the protection of Personal Information and activities carried out by citizens, businesses, or like persons with respect to securing the appropriate handling of Personal Information, shall formulate a policy and implement other necessary measures for the providing of information and the appropriate and effective implementation of measures by businesses and other persons.

Law Article 34

The Competent Minister may, upon finding it necessary for the protection of individual rights or interests where a Business Handling Personal Information has violated a provision of Article 16 to and including Article 18; Article 20 to and including Article 27; or Article 30 to and including Article 32, admonish that Business Handling Personal Information to cease such violative conduct or otherwise to take measures necessary to correct such violation.

2. The Competent Minister, upon finding that the violation of an important individual right or interest is imminent, where without a suitable reason measures have not been
taken by a Business Handling Personal Information which has been admonished pursuant to the provisions of the previous Paragraph, may order that Business Handling Personal Information to implement the measures related to that admonishment.

3. The Competent Minister may, upon finding that measures are urgently necessary due to the fact that an important individual right or interest has been violated where a Business Handling Personal Information has violated Article 16, Article 17, Article 20 to and including Article 22, or Article 23 Paragraph 1, notwithstanding the provisions of the previous two Paragraphs, order the Business Handling Personal Information to cease such violative conduct or otherwise take measures necessary to correct such violation.

Law Article 36

The Competent Minister in the provisions of this Subsection shall be as follows. However, if the Prime Minister finds it necessary in order to promote the efficient implementation of the provisions of this Subsection, the Prime Minister may designate a specific minister or the National Public Safety Commission (hereafter, a “Minister, Etc.”) as the Competent Minister with respect to the specific matters in the treatment of Personal Information performed by Business Handling Personal Information.

With respect to the management of employment in the handling of Personal Information performed by Business Handling Personal Information, the Minister of Health, Labor, and Welfare (the Minister of Land, Infrastructure and Transport with respect to management of seamen’s employment), and the Minister, Etc. having jurisdiction over the business activities of that Business Handling Personal Information.

With respect to matters other than those described in the previous Item in the handling of Personal Information performed by Business Handling Personal Information, the Minister, Etc. having jurisdiction over the business activities of that Business Handling Personal Information.

The Prime Minister must publicly disclose when designating a Competent Minister pursuant to the proviso of the previous Paragraph.

3. Competent Ministers must maintain close mutual contact and cooperation in the enforcement of the provisions of this Subsection.

[Commentary]

- With respect to protection of Personal Information, the use of Personal Information in conjunction with the development of advanced information-telecommunication society has been accompanied by a dramatic expansion in the use of Personal Information, and further, incidents involving leaking of information are occurring very frequently these days. Under these circumstances, the Law Concerning Protection of Personal Information (Law of 2003, No. 57; hereafter, the “Law”) was enacted for the purpose of protecting the rights and interests of individuals while considering the usefulness of Personal Information.

- Also, in Article 36 of the Law, with respect to Personal Information in the context of employment management, the Minister of Health, Labor and Welfare and the Minister having jurisdiction over the business are the Competent Ministers. These Guidelines,
compiled by the Minister of Health, Labor and Welfare based on the provisions of Article 8 of the Law, summarize the general principles applicable to all businesses and are guidelines for ensuring the appropriate and effective implementation of the measures to be carried out by businesses.

With respect to the admonishment, order and emergency order provided for in Article 34 of the Law, the Minister of Health, Labor and Welfare and the Minister having jurisdiction over the business shall cooperate in carrying out the procedures.

A person who violates an order made pursuant to the provisions of Article 34 Paragraph 2 or Paragraph 3 of the law shall be subject to imprisonment for not more than six months or a fine of not more than 300,000 yen.

In addition to these Guidelines, businesses must also take heed of the necessity of handling [Personal Information] pursuant to any guidelines, etc. established by the Ministries with jurisdiction over the business that take business-specific considerations into account.
II. Definitions

In these Guidelines, the meanings of the terms set forth in the following Items shall be as defined in the relevant Item, in addition to those specified in Article 2 of the Law.

i. Business: Among those Businesses Handling Personal Information as provided in Article 2 Paragraph 3 of the Law, an entity that handles Personal Information concerning employment management (except as provided in IV).

ii. Worker, etc.: Workers employed by a business as defined in the previous Item, persons attempting to become workers and persons who attempted to become workers employed by a business as defined in the previous Item, and persons who have been employed by a business in the past.

[Relevant Clauses]

Law Article 2 Paragraph 3

In this Law, the phrase a “Business Handling Personal Information” refers to a person that provides Personal Information Databases, Etc., for use in business operations, but exclude the following:

i. Organs of the national government;
ii. Local Public Entities;
iii. Independent administrative corporations (referring to independent administrative corporations as provided in the Law on Protection of Personal Information Held by Independent Administrative Corporations (2003 Law No. 59), Article 2, Paragraph 1; likewise hereafter);
iv. Persons as prescribed in the Cabinet Order as being little threat to the rights or interests of individuals from the standpoint of the quantity of Personal Information handled and the method of use.

Cabinet Order Article 2

For those persons as prescribed in the Cabinet Order for Law Article 2, Paragraph 3, Item 4, when the total number of specific individuals that can be identified by the Personal Information that comprises the Personal Information Database, Etc. used for that business (except for the number of specific individuals who can be identified through Personal Information comprising all or part of the relevant Personal Information Databases, Etc., when only the name, or address or location (including map or computer image displays indicating address or place of residence), or telephone number is included as Personal Information for all or part of the relevant Personal Information Databases, Etc. created by another person, and this is collected and used by the business without being processed) does not exceed five thousand (5000) on any day within the past six months.

[Commentary]

- In addition to the definitions set forth in Law Article 2 (Personal Information, Personal Information Databases, Etc., Businesses Handling Personal Information, Personal Data, Held
Personal Data and Principal), these Guidelines set forth the definitions of “Businesses” and “Workers, Etc.”

- **Businesses**
  “Businesses” are persons, among those Businesses Handling Personal Information as prescribed by Law Article 2 Paragraph 3, that provide Personal Information relating to employment management. The substance of “Businesses Handling Personal Information” and “Personal Information relating to Employment Management” here are as follows.

(1) “Businesses Handling Personal Information” are persons (*3) that handle Personal Information Databases, Etc. (*2) for use in business operations, except for Independent Administrative Corporations, etc. as prescribed in the Law on Protection of Personal Information Held by organs of the national government, Local Public Entities and Independent Administrative Corporations (2003 Law No. 59) and persons that are little threat to the rights or interests of individuals from the standpoint of the quantity of Personal Information handled and the method of use (*1).

Also, because no distinctions are made with regard to the legal personality of the Business Handling Personal Information, unincorporated associations (voluntary associations) or individuals also may fall under the category of Businesses Handling Personal Information.

(*1) “Persons that are little threat to the rights or interests of individuals from the standpoint of the quantity of Personal Information handled and the method of use” are those for which the total number of specific individuals (*4) who can be identified by the Personal Information comprising the Personal Information Databases, Etc., used for that business does not exceed five thousand (5000) on any day within the past six months, according to Article 2 of the Enforcement Order for the Law Concerning Protection of Personal Information (2003, Cabinet Order 507; hereafter “Cabinet Order”).

The aggregate number of specific individuals who can be identified by the Personal Information comprising all of the Personal Information Databases, Etc., managed by such Business shall be the basis for judging whether or not the number exceeds five thousand people. However, duplicate entries of the same individual shall be excluded. “Personal Information” includes customer information and employee information, etc.

(*2) “Personal Information Databases, Etc.” are collections of information including Personal Information which are structurally constituted so as to be able to search for specific Personal Information by computer, and in the case where a computer is not used, collections of information that can easily be searched by others with a table of contents, index, code, etc. provided so that a certain set of rules (e.g., in the order of the Japanese syllabary, by birth date, etc.) can be used to organize, classify and easily search for specific Personal Information.

[Examples of “Personal Information Databases, Etc.”]
1) Personnel and labor management databases, client management databases
2) E-mail address books stored by e-mail software (when e-mail addresses and names are input together)
3) Information on business cards received by employees which is input and organized using spreadsheet software, etc. on a computer for business use (regardless of the owner) and in a state that is searchable by other employees, etc.

4) Files of employee information with names organized in the order of the Japanese syllabary with an index in the order of the Japanese syllabary

5) Commercially available directories classified and organized by name, address and company, and telephone directories provided by telephone companies

[Cases not corresponding to “Personal Information Databases, Etc.”]

1) Where an employee has his/her categorized business cards using a personalized method of categorization whereby other persons may not search [for information] easily, even if in a situation where they may search freely through the employee’s business card case.

2) Where questionnaires (those collected) answered by employees have not been classified and organized by name, address, and so forth.

(*3) “Business” refers to the same activity performed repeatedly and continuously with a particular objective, and is regarded as an ordinary conventional business, which corresponds to every type of industry and not only to commercial business.

The phrase “[a business which] provides [Personal Information Databases, Etc.] for use in business operations” refers to the use of Personal Information Databases, Etc. for business purposes, and does not take into account any such specific purpose or method of use. More specifically, this broadly includes cases such as those where actual creation, processing, analysis and provision of Personal Information Databases, Etc. for the database business are businesses, those where [such databases] are used in management of customers/clients and delivery addresses etc. to perform business, and those where they are used only internally to manage the employment of employees, and the like.

(*4) In the event that Personal Information Databases, Etc. fulfill all the following requirements, the number of specific individuals identified by the Personal Information comprising such Personal Information Databases, Etc., shall not, under Cabinet Order Article 2, be included in the “Number of Specific Individuals”.

① All or part of the Personal Information Databases, Etc. was created by another person.

② Such Personal Information Databases, Etc. only consist of names or addresses (including place of residence, and including map or computer image displays indicating address or place of residence) or telephone numbers.

③ In the process of providing such Personal Information Databases, Etc. for use in business operations, changes are not made to the Personal Information Databases, Etc., such as adding new Personal Information, increasing specific individuals to be identified, or adding additional personal information.

[Cases included in the “number of specific individuals”]

1) The number of specific individuals identified by Personal Information comprising the database for personnel and labor management, and for customer management,
regularly updated and used at the company (reasoning: because this does not correspond to at least item (iii) out of items (i) - (iii) of (*4))

2) The number of specific individuals identified by Personal Information comprising an e-mail address book (where e-mail addresses and names have been combined and input) stored in electronic e-mail software (reasoning: because this does not correspond at least to item (ii) out of items (i) - (iii) of (*4))

3) The number of specific individuals identified by Personal Information comprising information from business cards (including department of affiliation and title) acquired by an employee, which said employee inputs and arranges using computer spreadsheet software, and which even other employees can search through (reasoning: because this does not correspond at least to items (i) and (ii) out of items (i) - (iii) of (*4))

4) The number of specific individuals identified by Personal Information comprising employee information including personnel evaluation information and the like, which the company itself organizes in order of Japanese syllabary, and files using an index using the Japanese syllabary. (reasoning: because this does not correspond at least to items (i) and (ii) out of the above)

[Cases not included in the “number of specific individuals”]

1) The number of specific individuals identified by Personal Information comprising a telephone directory provided by a telephone company or commercially purchased, and then used as it is (reasoning: because this corresponds to all of (i), (ii) and (iii) above)

2) The case where in the transportation business, although documents containing Personal Information are included among sealed packages for delivery entrusted by a customer, their existence is neither known, nor are they used in business (reasoning: not included because said information is not provided for use in business operations)

(2) “Personal Information relating to employment management (hereinafter “Employment Management Information”)” refers to Personal Information to be collected, stored, used and so forth by corporations and the like for the purpose of employment management of workers and the like, and this covers all information related to individual workers, including sensitive information such as medical history, income, and family relations, as well as information pertaining to persons other than the Principal.

Moreover, “Personal Information” refers to information pertaining to living individuals, and information which enables identification of a specific individual through name, date of birth, and other data included in such Personal Information. Foreign persons are also included in living individuals. Typical examples of Personal Information are name, gender, date of birth, but even information relating to attributes concerning the physical body, assets, social standing and status and so forth of the individual constitutes “Personal Information” if specific individuals are identifiable by combining such information with a name and so forth, and visual and auditory information are included.

Furthermore, even if a specific individual cannot be identified using only such information, other information which can be easily referred to and which enables identification constitutes “Personal Information”. Furthermore, information related to deceased persons which at the same
time pertains to a living individual such as a relative and so forth, constitutes information pertaining to the living individual in question.

[Cases corresponding to “Personal Information relating to employment management”]
1) Name of worker, etc.
2) Date of birth, contact details (address, place of residence, telephone number, e-mail address, etc.), and information related to position title or department of affiliation in said individual’s company, combined with the name of the worker, etc.
3) Of visual and auditory information recorded on videotape etc., information which enables identification of a specific worker etc.
4) E-mail address information which enables identification of a specific worker etc. (e-mail address, which, together with name and organization of affiliation, enables identification)
5) Information enabling identification of a specific worker etc., which, even if not recorded, can enable identification of a specific worker, etc., through recognition by supplementing known information. (Note: Although what specifically constitutes “known information” will differ from case to case, as a general rule, “known information” means information that the general public knows without doing any special research)
6) Information which, of information relating to employment management such as personnel evaluation information etc., enables identification of a specific worker, etc.
7) Information publicly disclosed through employee records etc. (name etc. of worker, etc.)
8) Personal Information related to family relations of worker etc., and Personal Information related to his/her family.

[Cases not corresponding to “Personal Information relating to employment management”]
1) Customer information, shareholder information
2) Information related to organizations such as corporations, etc. (organization information)
3) E-mail address information not enabling identification of specific workers, etc. (e-mail addresses whereby the name and organization of affiliation cannot be specified. However, this excludes cases where identification of specific worker, etc. is possible by referring easily to other information.)
4) Statistical information which does not enable identification of a specific worker, etc.

- Worker, etc.

(1) “Worker” refers to a living individual, who, regardless of the type of business, is employed in a business or place of business, and is paid wages, in the same way as in the case of a “worker” prescribed in Article 9 of the Labor Standards Law. If these terms and conditions are fulfilled, the term also applies to part-timers and contract employees, not only full-time employees.

(2) A person who, even if referred to as “officer”, falls under the term “worker”, where, given the actual situation, such person is recognized as being employed in a place of business and
being paid wages. An “officer” who exclusively makes managerial decisions and does not receive instructions from another person, shall not fall under “worker”.

(3) Persons trying to or who have tried to become workers employed by a “business” (present and past job applicants as well as participants of company information sessions) and retirees are included among the “etc.” of “workers, etc.”. Businesses must aim to achieve the proper handling of Personal Information of not only persons employed at present, but also job applicants and retirees.

(4) Workers dispatched to businesses receiving dispatched persons shall fall under “worker, etc.”, since there is a chain of command between the dispatched persons and such businesses, and such persons constitute “workers employed by the business”. Businesses must aim to achieve proper handling of individual information relating to employment management of dispatched workers working in the business, in accordance with the Guidelines.

(5) In order to protect the Personal Information of dispatched workers (including so-called registered dispatched workers) employed by their dispatching agency, it is a given that said employer must comply with the provisions of the Guidelines, but it should also be noted that in addition to the Guidelines, from the perspective of securing proper operation of business with regard to the dispatch of workers, and so forth, it must comply with “Guidelines Relating to Measures to be Taken by Dispatching Agencies” (Ministry of Health, Labor and Welfare, Notification 137, 1999) prescribed under the Law for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers (Law No. 88, 1985).

(6) Contractors under a service agreement handle their work independently from the party placing the order since the contracted work is their own work, and, therefore, cannot be referred to as “workers employed by a business”. Accordingly, with respect to businesses where contractors work under a service agreement, contractors do not fall under “workers, etc.” prescribed in the Guidelines.

(7) A decision needs to be made regarding students who participate in internships, in terms of the actual status of activities in each place of business, but in general it is difficult to apply the term “worker” to such students, and there seem to be many cases where it is difficult to regard information concerning such students as Employment Management Information. However, in view of the fact that, as with Employment Management Information, sensitive information could be included in information obtained from students during their internship, it is a given that proper measures be taken pursuant to the law, and that in accordance with Item III. of the Guidelines (see pp.11-31), securing of the proper handling of such Personal Information is asked for.
III. Matters Serving As Guidelines for Appropriate and Effective Implementation of Measures Taken By Businesses

1. Matters relating to specification of the purpose of use provided in Article 15 of the Law

Businesses must specify the purpose of use concretely and individually, not merely in abstract and general terms, to the extent that the principal, such as an employee, etc. can reasonably assume results of the use of the acquired personal information of that principal.

Related Provision

Article 15 Paragraph 1 of the Law

A business handling personal information must specify to the extent possible the purpose of use in the handling of personal information (“the purpose of use”).

[Comments]

- The Law sets out the specification of the purpose of use as a method of realizing appropriate handling of personal information. It is intended to realize appropriate handling of personal information by specifying the “purpose” in a manner that this piece of personal information is used for this particular “purpose”, not to restrict contents of personal information collected by businesses.

- Article 15 Paragraph 1 of the Law requires businesses handling personal information to specify the purpose of use as much as possible. The Guidelines set out the extent of the specification of the purpose as “instead of merely specifying the purpose in abstract and general terms, specifying it concretely and individually in such a manner that the principal, such as an employee, etc. can reasonably assume results of the use of the acquired personal information of that principal”.

- Concerning to what extent the purpose of use should be “specified concretely and individually”, it is not always necessary to enumerate in detail each specific and individual purpose of use. However, it is necessary to clarify purposes of use, even if in abstract terms, to the extent that it is possible to actually determine whether each handling is within the range necessary to achieve a purpose of use. In other words, it should be clarified to the extent that a conflict does not arise between a business handling personal information and the principal over whether or not the handling of personal information is within the scope necessary to achieve the purpose of use. To prevent an occurrence of such a conflict, it is desirable that pursuant to the provision of No.3-9 of the Guidelines (refer to page 30), prior notice be given to the labor union, etc. for consultation as the need arises.

- “Labor Union, etc.” means, when there is a labor union organizing a majority of employees, such labor union, and when there is not a labor union organizing a majority of employees, a representative of a majority of the employees.

- When specifying the purpose of use, the Law does not obligate businesses handling personal information to specify the purpose of use for each item of personal information. However, in terms of Employment Management Information, which includes sensitive
information such as medical history, income, and family relationships, it is desired that these be treated with more caution. In addition, it is expected that the purpose of use will differ according to categories of personal information. Therefore, in terms of Employment Management Information, it is desirable to specify the purpose of use by each item of personal information, to the extent possible. (However, in cases where it is possible to estimate the kind of information from the purpose of use, it is expected that there may be cases where the items of personal information do not have to be listed.)

- In the case when it has been planned in advance that personal information will be provided to a third party, the provision of personal information to a third party should be specified in the purpose of use.

- Businesses recruiting employees must remember that the “Guidelines For Proper Actions Taken by Employment Agency Businesses, Businesses Recruiting Employees, Businesses Acting As Recruiter, Businesses Supplying Employees, etc. as to Declaration of Equal Treatment and Working Conditions, Handling of Personal Information of Job Seekers, Responsibilities of Employment Agency Businesses, Accurate Indication of Contents of Recruitments, etc. stipulated by the Employment Security Law (Law No. 141 of 1947) (Notification of Ministry of Labor, No. 141 of 1999: hereinafter “Guidelines Under the Employment Security Law”) provide that they must collect personal information of the persons who want to be employees in compliance with the scope of the purpose of business operations concerned, and retain and use such personal information, in principle, within the scope of the purpose of the collection.

[Examples where the purpose of use is specifically and individually specified]
1) “Our Personnel Affairs Department staff will use the information for the purpose of executing personnel and labor management procedures only (pension, labor insurance, etc.”);
2) “We will use information concerning names of family members, addresses and phone numbers which you have entered in executing the employment contract as emergency contact information in the case of emergency”;
3) “Concerning the resident register certificate submitted to the personnel affairs department as proof of age by those under 18 years old who are to work for the Company, we will use the information exclusively for the purpose of complying with the provision of Article 57 Paragraph 1 of the Labor Standards Law”;
4) “We will use the results of this aptitude test as materials exclusively for the purpose of reviewing future personnel assignments in the office”.

[Examples where specification of the purpose of use is insufficient]
1) “For the purpose of business activities of the company”
2) “For the purpose of extensively grasping employees’ information”
### III. Matters Serving As Guidelines for Appropriate and Effective Implementation of Measures Taken By Businesses

2. Matters relating to employee’s consent provided in Article 16 of the Law and Article 23 Paragraph 1 of the Law

It is desirable that businesses should, when obtaining the consent of the principal, such as an employee, etc., notify that principal of the purpose of using the personal information or announce the purpose in advance and that principal has expressly given consent to the handling of the personal information verbally or in writing.

**Related Provisions**

**Article 16 of the Law**

1. A business handling personal information shall not handle personal information to an extent beyond that necessary to achieve the purpose of use specified pursuant to the previous Article without obtaining the prior consent of the principal.

2. A business handling personal information, if it acquires personal information due to succeeding to the business operations of another business handling personal information for reasons such as merger, shall not handle that personal information to an extent beyond that necessary in order to achieve the purpose of use prior to that succession without obtaining the prior consent of the principal.

3. The provisions of the previous two Paragraphs shall not apply in any of the cases described in the following Sub-paragraphs:

   1) If pursuant to a law or ordinance
   2) If necessary for the protection of human life, safety, or property, and when it is difficult to obtain the consent of the principal;
   3) If necessary in particular in order to improve public hygiene or promote the health of children, and when it is difficult to obtain the consent of the principal;
   4) If cooperation is necessary in the execution of an operation set forth by law or ordinance by an institution of the national government, a local public entity, or a person delegated thereby, and there is fear that the execution of that operation would be hindered by obtaining consent of the principal.

**Article 23 Paragraph 1 of the Law**

A business handling personal information shall not provide to any third party personal data without first acquiring the consent of the principal, except as set forth in the following Sub-paragraphs:

1) If pursuant to a law or ordinance

2) If necessary for the protection of human life, safety, or property, and when it is difficult to obtain the consent of the principal;

3) If necessary in particular in order to improve public hygiene or promote the health of children, and when it is difficult to obtain the consent of the principal;
4) If cooperation is necessary in the execution of an operation set forth by law or ordinance by an institution of the national government, a local public entity, or a person delegated thereby, and there is fear that the execution of that operation would be hindered by obtaining consent of the principal.

[Comments]

- As a method of realizing the appropriate handling of personal information, the Law requires the specification of the purpose of use as well as prohibiting in principle the handling of personal information without the prior consent of the principal to an extent beyond that necessary to achieve the specified purpose of use, and the provision of personal data to a third party without the prior consent of the principal.

- As to employment management information, in view of the fact that the information contains such sensitive information as clinical history, income or family relationships, the Guidelines specifically sets out matters to be kept in mind by businesses in obtaining the consent of the principal such as an employee, etc., providing that “it is desirable that the principal should expressly give his or her oral or verbal consent to the applicable handling of personal information after such principal has been notified about the purpose of use for such personal information or after a public announcement has been made regarding such purpose of use”.

- “To notify the principal” means that the principal is directly notified in a reasonable and appropriate method, depending on the situation of the handling of personal information, which enables the contents to be recognized by the principal.

[Examples falling into “to notify the principal”]

By referring to the following examples, notification should be made in a reasonable and appropriate method, depending on the situation, so that the contents are recognized by the principal:

1. In conducting an interview, contents are communicated verbally, or documents such as pamphlets are handed to the principal;
2. Notification is made verbally on the phone on the assumption that the subject principal has already been identified;
3. Documents are sent by mail, etc. to retirees and those who live at remote locations, or they are sent by e-mail, facsimile or other media normally used by the principal.

[Examples not falling into “to notify the principal”]

1. Under the situation where the subject principal has not been identified, notification is made verbally on the phone;
2. Documents are sent by mail, etc. to those whose present addresses are not accurately known, and necessary measures are not taken to confirm whether the documents have been received by the principal or not;
3. Emails are sent to those who do not normally use e-mail.

- “To announce” generally means making one’s own intention known far and wide. However, announcing should be made in a reasonable and appropriate method, depending on the
situation of the handling of personal information.
Concerning employment management information; in view of the fact that the information contains such sensitive information as clinical history, income or family relationships, the purpose of using personal information should be announced with consideration paid to choosing media which will enable information to be correctly communicated to the employee, etc., in view of the situation where the subject business is placed.

[Examples falling into “to announce”]
By referring to the following examples, consideration should be paid to choosing of a media that enables contents to be transmitted to the employee, etc., without fail, in view of the situation where the subject business is placed:
(1) Posting at an easily accessible place on the Company website;
(2) Circulating a note to the employees regarding the purpose of using employment management information of the existing employees;
(3) Distribution of pamphlets, company newsletters and the like;
(4) Posting on a bulletin board at the worksite where it is expected that employees periodically view.

“To obtain the consent of the principal” means that the subject business handling personal information recognizes the intention of the principal to give consent. The consent should be obtained using a method which is reasonable and appropriate for the principal to make a judgment regarding the consent.
In view of the fact that the employment management information contains such sensitive information as clinical history, income or family relationships, due consideration should be paid to the obtaining of the consent of the principal

[Examples falling into “to obtain the consent of the principal”]
The following examples are based on the assumption that to the principal the purpose of using the personal information has been notified or announced:
(1) Confirmation is obtained verbally or in writing from the principal as to the consent.
(2) Application sheets or documents in which the principal has given its consent by affixing its signature and seal are received and confirmed.
(3) An email is received from the principal informing that it has given its consent.
(4) The confirmation button on the website is clicked by the principal to give consent.
(5) Voice input is made by the principal to give consent.
III. Matters Serving As Guidelines for Appropriate and Effective Implementation of Measures Taken By Businesses

3. Matters relating to security control measures provided by Article 20 of the Law and supervision of employees provided by Article 21 of the Law

Businesses must endeavor to take the following measures for the purpose of security control of personal data relating to employment management.

(1) The business must, after identifying the employees who handle personal data relating to employment management and clarifying the powers of the employees, allow such employees to conduct the operations concerned;

(2) Personal data relating to employment management is handled only by those who are authorized to handle the personal data, to the extent that such personal data is necessary for the execution of operations.

(3) A person who handles personal data relating to employment management must not disclose to a third party personal data it has learned in the performance of business without permission nor use the same for any unjustifiable purpose. The same provision is applicable after it has resigned from the duty concerned.

(4) To carry out matters concerning management of the handling of personal data relating to employment management, a person responsible for personal data management is appointed out of those who are deemed to possess required knowledge and experience for conducting such matters.

(5) Persons responsible for personal data management relating to employment management and employees who handle personal data are awakened to the importance of their responsibilities and given required education and training so as to thoroughly understand concrete protective measures of personal data.

(Related Provisions)

Article 20 of the Law
A business handling personal information must adopt measures necessary and appropriate for preventing the unauthorized disclosure, loss or destruction of handled personal data and otherwise control the security of personal data.

Article 21 of the Law
If a business handling personal information allows an employee to handle personal data, it must provide necessary and appropriate supervision of that employee so as to achieve control of security of that personal data.

[Comments]
[General Remarks]
● Should personal information be subject to unauthorized disclosure or altered, private rights and interests may be exposed to the increased danger of being infringed. A business handling personal information must take appropriate and necessary measures to prevent unauthorized disclosure, loss or destruction of the handled personal information, including
clarification of the scope of persons entitled to handle personal information and measures for ensuring security of personal information.
For this purpose, appropriate measures must be taken in view of the content, the nature or the method of using personal information, and moreover, since the personal information relating to employment management contains clinical history, income, family relationships and other sensitive information, due consideration should be paid to the handling of such personal information.

- To conduct appropriate management of personal data, employees must carry out appropriate handling based on security control measures, and when unauthorized disclosure or any other problem has occurred due to the handling by an employee which is against the security control measures, it is highly likely that a business handling personal information is held responsible for having failed to exercise supervision over the management of personal data.

- The Guidelines provide that any arbitrary use of personal information is curbed by clarifying the powers of persons engaged in the handling thereof, that the personal information one has learned in its execution of businesses is appropriately handled, that persons with required knowledge and experience are selected as persons responsible for personal data management from the standpoint of thoroughly implementing security control of personal data, and that proper handling is secured by conducting necessary education and training upon those who handle personal data as well as persons responsible for personal data management. Based on the above provision of the Guidelines, measures must be taken according to the actual circumstances, depending on contents of personal data and methods of using the same.

[Related to items (1) and (2)]
- For persons who handle data relating to employment management, it is necessary to define, under internal regulations, etc., the necessary handling to do their jobs, and restrict the actual handling to the scope so defined. Consequently, persons who are not authorized to handle personal information must not be allowed to handle personal information.

[Examples of contents relating to security control to be described in internal regulations]
1) Allocate and specify persons responsible for such work as acquisition, input, transfer, transmission, use, processing, storage, backup, deletion, disposal
2) Management of the situation of implementation by each person responsible for allocated work such as acquisition, input, transfer, transmission, use, processing, storage, backup, deletion, disposal, and retention of records
3) Setting of ID and passwords which enable the identification and authentication of each person responsible for allocated work, and management of access records

[Related to items (3)]
- In terms of data relating to employment management which has become known in the course of doing his or her job, only authorized persons may handle such information to the extent necessary for the execution of business. Therefore, it goes without saying that even if a person is authorized to handle personal information, such personal information cannot be used for an unjust purpose such as resale to an entity that sells catalogs of names.
Since personal information relating to employment management contains sensitive information, “persons responsible for personal data management” are to be selected, and it is hoped that such information will be handled without fail. In light of the purpose of the Law, these Guidelines request that “persons responsible for personal data management” be selected at every business place that corresponds to a business handling personal information, and by doing so, these Guidelines aim to realize thorough security control over personal data.

“Persons responsible for personal data management” should be distinguished from “persons responsible for personal information protection management (chief privacy officer) defined under “the Guidelines for Businesses and Industries Relating to the Law of Personal Information Protection (Notification of Ministry of Health, Labor and Welfare and Ministry of Economy, Trade and Industry: No. 4 of 2004)” However, in managing personal data at every place of business, it is possible for a person to take on both roles.

<Reference>

Organizational Security Control Measures
Organizational security control measures mean that responsibilities and powers of employees (refer to the Article 21 of the Law) are defined as to security control, that regulations and manuals (“regulations, etc.”) concerning security control are improved and operated and that the state of the implementation thereof is confirmed.

[Matters Conducted as Organizational Security Control Measure]
(1) Matters conducted for the improvement of organizational structure enabling implementation of security control measures of personal data
   - Assignment of persons responsible for personal information protection management (chief privacy officers)

[Related to item (5)]
- Persons responsible for personal data management and those who handle personal data are required to be aware of responsibilities imposed and the importance of the handling of the same and to receive regular education and training so as to acquire the skill of properly handling personal data.

[Examples of Training Contents]
1) Improving, and making well-known to everyone, internal regulations, etc. relating to handling of personal data
2) Confirmation of methods of storing and disposing of personal data
3) Access control of personal data
4) Points to remember when processing of personal data is delegated

[Cases where necessary and proper security control measures are not taken]
1) Where persons responsible for personal data management and those handling personal data are still in a position to access personal data after they have been replaced or have left the post due to personnel transfers, etc. and there is unauthorized disclosure of personal data as a result;
2) Where a personal data storage facility or site is not locked and as a result, personal data has been taken out by a person who is not authorized to handle personal information;
3) Where PCs containing performance records of employees have been discarded without such records being completely deleted, and as a result, there is unauthorized disclosure of personal data.
4) Where there is no access control over personal data such as name, age, and gender of employees collected for the purpose of processing social insurance, and personal data has been taken out by a person who is not authorized to handle personal information, and as a result, there is unauthorized disclosure of personal data.
III. Matters Serving As Guidelines for Appropriate and Effective Implementation of Measures Taken By Businesses

4. Matters relating to supervision of delegatees provided in Article 22 of the Law
Businesses must keep in mind the following matters when delegating the handling of personal data relating to employment management:
(1) Businesses should establish criteria of selecting, as delegatee, entities who take sufficient measures for protection of personal information.
(2) Contents of the measures for protection of personal data taken by delegatees should be expressly defined in the delegation contract concerned. These measures specifically include:
1. Obligations are imposed on employees of the delegatee not to disclose or plagiarize personal information which has become known or available during the course of the handling of the personal data concerned;
2. When handing of the personal data is re-delegated, such re-delegation is notified in writing to the delegating party accordingly.
3. The term and other provisions of the delegation contract are clearly described.
4. Personal data is, after the purpose of use has been achieved, returned, discarded or deleted properly and securely by the delegatees.
5. Processing, alteration, etc. of personal data at delegatees (with the exception of that within the scope defined in the delegation contract concerned) is prohibited or restricted.
6. Making duplicates or copies (with the exception of ones for the purpose of backups necessary for security control and within the scope defined in the delegation contract concerned) of personal data by delegatees is prohibited.
7. Obligation of notification to the delegating party is imposed on delegatees upon occurrence of an accident such as unauthorized disclosure, etc. of personal data at the delegatees.
8. Responsibilities of delegatees are clarified in the event of an occurrence of an accident such as unauthorized disclosure, etc. of personal data at delegatees.

[Related Provisions]
Article 22 of the Law
If a business handling personal information delegates all or a portion of the handling of personal data, it must provide necessary and appropriate supervision of the person receiving delegation so as to achieve control of security of the personal data the handling of which has been so delegated.

[Comments]
[General Remarks]
- Businesses handling personal information must, when delegating the handling of personal data, exercise necessary and proper supervision over the delegatees: Article 23 Paragraph 4 Item 1 of the Law provides that delegatees are not considered to be “third parties” and consequently businesses handling personal information must exercise supervision to secure protection of personal information.
Private businesses are the ones who decide the form of contract, but in general, in the case of delegation, the delegatee receives data from the delegating party, and processes and compiles, etc. such data within the scope defined in the delegation contract.

Consequently, typical delegation arrangements include delegations for information processing such as data input, or for the delivery of goods by forwarding personal data (addresses, names etc.) to courier service agents, and it is assumed that the scope of processing and use of the data has been restricted in advance under a delegation contract concerned, etc.

When businesses handling personal information delegate input, compilation, output and other handling of employment management data, they must grasp the situation of protection and security of personal information at the delegatees and moreover, exercise necessary and proper supervision over the delegatees.

In terms of an arrangement whereby businesses handling personal information provide personal data to certified social insurance labor consultants who will prepare or submit applications as requested, such arrangements are generally deemed to be a delegation (see page 33). However, if such certified social insurance labor consultant is requested to provide labor management advice and will prepare new data for the execution of this task, this is no longer within the scope of delegation, and such delegatee will itself be treated as a business handling personal information with legal obligations such as notification of the purpose of use provided in Article 24 Paragraph 2 of the Law as well as disclosure provided in Article 25 Paragraph 1 of the Law.

[Related to Item (1)]

Selection of delegates requires establishing selection criteria, etc. in order to choose appropriate companies from the viewpoint of securing protection of personal information.

[Examples of Selection Criteria]
1) Storing methods and location are appropriate.
2) Concrete measures are taken to prevent unauthorized disclosure and misappropriation of personal data.
3) Employees who handle personal data are receiving education and training.
4) Proper inspection is conducted as to handling of personal data.

[Related to Item (2)]

Details of measures for the protection of personal information taken by delegates are clearly defined in the delegation contract, etc.

Matters incorporated into the delegation contract, etc. include prohibition of misappropriation, obligation of notification to the delegating party in the event of re-delegation, clear indication of the term of the delegation contract, etc. and return, disposal or deletion of personal data after the purpose of use has been achieved, and prohibition of making copies or duplicates, so as to prevent unauthorized disclosure of personal data. By imposing upon delegatees, an obligation of notification to the delegating party on an occurrence of an accident such as unauthorized disclosure as well as clarifying the
responsibility of the delegatee in such an event, it is desired that the delegate also sufficiently pay attention to the security of personal data management. Furthermore, once an accident such as unauthorized disclosure of personal data has occurred at a delegatee, preventive measures against further unauthorized disclosure of personal data must be taken by collaboration and coordination between the delegating party and the delegatee.

● It is desirable not to re-delegate or re-redelegate the handling of personal data as much as possible because re-delegation or re-redelegation expands the danger of unauthorized disclosure of personal data. However, when handling of personal data is re-delegated or re-redelegated, written notice of the re-delegation or re-redelegation should be given to the delegating party that has the obligation to supervise delegatees, and it is desirable that thorough security control measures are taken.

● “Etc.” under “the term of the delegation contract, etc.” means and includes the delegatees’ managing methods and specific processing methods of personal data (such as return or disposal) after the termination of the delegation contract.

[Examples of Managing Methods]
1) To restrict terminals enabling use and processing of personal data whenever necessary
2) To control access to personal data
3) To securely lock and manage storage facility or place for personal data

● Personal data after the purpose of use has been achieved must be returned to the delegating party, or disposed or deleted at the delegatee as soon as possible and without fail, so as to prevent plagiary, unauthorized disclosure, etc. of the data.

● “Etc.” under “alteration, etc. of data” means and includes alteration of data beyond the scope defined in the delegation contract or unjust addition of information, which should be prohibited or restricted.

● Making of copies or duplicates of personal data which is even within the scope defined in the delegation contract must be restricted to cases where they are necessary for the purpose of data backups.

[Examples where necessary and proper supervision is not exercised over delegates]
1) Where the delegating party has failed to grasp the management system at the delegatee including whether or not storage places or persons in charge of storage are designated at the delegate.
2) Where the delegating party has failed to conduct proper management or exercise regular supervision over the management methods of data relating to employment management conducted by the delegatee, and as a result, there is unauthorized disclosure of data relating to employment management from the delegatee.
3) Where data relating to employment management is not handled by the delegatee pursuant to the contents of the delegation contract and moreover, the delegating party has neglected to grasp such situation on a regular basis, and as a result, there is unauthorized disclosure of employment management data.
4) Where, when the delegatee delegates (re-delegates) data relating to employment management, a re-delegatee with insufficient data management structure has been selected and as a result, there is unauthorized disclosure of data relating to employment management.
III. Items that should be a guideline for a Business to appropriately and effectively implement measures

5. Items related to provision to a third party which is stipulated by Article 23 of the Law

A Business shall take note of the following items in conjunction with provision to a third party Personal Data regarding employment management (excluding cases that fall under Law Article 23 Paragraph 1 Sub-Paragraph 1 to Sub-paragraph 4)

(1) The party that is provided Personal Data shall not leak or plagiarize Personal Information that is obtained through handling Personal Data of the Principal.

(2) For re-provision of Personal Data of the Principal, approval of a Business in a written form shall be acquired in advance. However, it excludes cases falling under Law Article 23 Paragraph 1 Sub-Paragraph 1 to Sub-Paragraph 4.

(3) Period of data storage and other matters at the party that is provided Personal Data shall be made explicit.

(4) Personal Data shall be appropriately and definitely returned or disposed/deleted at the party that is provided Personal Data after the Purpose of Use is accomplished.

(5) Copies and reproduction of Personal Data at the party that is provided shall be prohibited (excluding cases that purpose is to back up necessary data for safety management).

[Related article]

Law Article 23

Business Handling Personal Information shall not provide to any third party Personal Data without first acquiring the consent of the Principal, except as set for the in the following Sub-paragraphs:

1. If pursuant to a law or ordinance
2. If necessary for the protection of human life, safety, or property and when it is difficult to obtain the consent of the Principal.
3. If necessary in particular in order to improve public hygiene or promote the health of children, and when it is difficult to obtain the consent of the Principal.
4. If cooperation is necessary in the execution of an operation set forth by law or ordinance by an institution of the national government, a local public entity, or a person delegated thereby, and there is fear that the execution of that operation would be hindered by obtaining consent of the Principal.

2. If a Business Handling Personal Information, with respect to Personal Data provided to a third party, decides to cease providing to a third party Personal Data identifying a Principal in accordance with the request of that Principal, and it has notified the Principal in advance of the matters set forth in the following Sub-paragraphs, or if the Principal is placed in circumstances in which such matters can be easily learned, such Business Handling Personal Information may provide that Personal Data to a third party notwithstanding the provisions of the previous Paragraph.

1. The fact that providing the Personal Data to a third party is included in the Purpose of Use;
2. Categories of Personal Data provided to a third party;
3. Means and methods of providing Personal Data to a third party
4. The fact that providing Personal Data identifying a Principal shall cease at the request of that Principal.

3. A Business Handling Personal Information, if revising matters set forth in Sub-paragraph 2 or Sub-paragraph 3 of the previous Paragraph, must first notify the Principal of the content changed, or place the Principal in circumstances in which the content changed can be easily learned.

4. In any case described in the following Sub-paragraphs, a person who has been provided with the Personal Data in question shall not be considered a third party with respect to the application of the provision of the previous three Paragraphs:

1. If a Business Handling Personal information delegates all or portion of the handling of Personal Data to the extent necessary to achieve the Purpose of Use.
2. If Personal Data is provided in accordance with succession to business operations for reasons such as merger;
3. If Personal Data is used jointly with a specified person, when the Principal is notified in advance of the fact of such joint use, the items of Personal Data to be used jointly, the range of jointly using person or persons, the Purpose of Use of the Personal Data, and the name or title of the person responsible for the management of that Personal data, or the Principal has been placed in circumstances whereby such matters can be easily learned.

5. If a Business Handling Personal Information changes the Purpose of Use provided in Sub-paragraph 3 of the previous Paragraph, or the name of or title of the person responsible for the management of Personal Data, it must notify the Principal in advance or the Principal must be placed in circumstances whereby such matters can be easily learned.

[Commentary]
[General introduction]

- For provision of Personal Data to a third party, provision of Personal Data to a third party without first acquiring consent of the Principal is prohibited in principle, as unlimited provision of Personal Information to third parties bears a high risk of unexpected violation of rights and welfare of that Principal.

- However, Personal Data can be provided to a third party without first acquiring consent of the Principal if it is pursuant to a law or if opt-out (*) applies in the provision to a third party.

(*) Opt-out in provision to a third party applies when the Principal has been notified or is placed in circumstances whereby such matters can be easily learned that providing the Personal Data to a third party is a Purpose of Use and about the categories of Personal Data to be provided and the means/methods of providing Personal Data to third parties, and that such provision to a third party shall cease at the request of that Principal.

- As for handling Personal Data by “a third party” in “provision to a third party”, it is possible that new data is created by processing and making additions on data provided by the information holder. “Provision to a third party” is different from “delegation” as it does not necessarily mean contracts will be entered into for handling Personal Data and a third party that is provided Personal Information can process such information and make additions.
freely.

[Related to (1) – (5)]

- Personal Information in particular regarding employment management needs to be handled even more carefully and unlimited provision of the data to a third party from the information holder must be prevented as information includes sensitive information such as clinical record, income and family relations information.
- Accordingly, when a third party that has received Personal Information provides it to another party, it is desired that appropriate handling of Personal Information is secured by the following means:
  1. Obtain prior written consent from the party that directly obtained Personal Information.
  2. Prevent arbitrary use, etc. by clarifying the authority of persons engaged in handling Personal Information.
  3. Clarify the period and means for the storage of Personal Data by a third party that receives Personal Data.
- “Others” in “Storage period and others” include management methods of Personal Data and concrete disposal measures (return, destroy and others) after accomplishing the Purposes of Use.

[Concrete management methods]

1. Limit, as necessary, terminals at which Personal Data can be used and processed
2. Limit access to Personal Data
3. Ensure locking of media that stores Personal Data

- Once the Purpose of Use is accomplished, Personal Data must be returned to the providers, or destroyed/deleted at the parties that received data with certainty at the earliest stage in order to prevent data from being misappropriated or leaked, etc.
- In addition, copying and reproducing Personal Data must be limited to those necessary for back-up purposes.
III. Items that should be a guideline for the enterpriser to appropriately and effectively implement measures

6. Items related to disclosure of Held Personal Data that is stipulated by Article 25 Paragraph 1 of the Law

A Business Handling Personal Information shall first discuss with labor unions and others where necessary, determine items related to disclosure of Held Personal Data which is not expected to be disclosed if there is fear that disclosure of all or a portion of such data that has been requested by the Principal and others to disclose would markedly impair appropriate execution of business operations of the relevant Business Handling Personal Information, and use its best efforts to take measures to keep employees and others informed.

[Related articles]

Law Article 25
If a Business Handling Personal Information has been requested by a Principal to disclose Held Personal Data identifying that Principal (including notification of nonexistence of Held Personal Information in such cases where Held Personal Data identifying that Principal does not exist), it must promptly disclose that Held Personal Data to the Principal in accordance with a method specified by government ordinance without delay. However, all or a portion of such information need not be disclosed where as a result of disclosure any of following Sub-paragraphs apply.

1. If there is fear that life, safety, and property or other right or the welfare of the Principal or a third party would be harmed;
2. If there is fear that the appropriate execution of business operations of the relevant Business Handling Personal Information would be markedly impaired;
3. If another law or ordinance would be violated.

2,3 (omit)

Government ordinance Article 6
The methods stipulated by government ordinance in Law Article 25 Paragraph 1 shall be the methods of delivery of written documents (and other methods if it is agreed by the Principal who has requested such data to disclose).

[Commentary]

- Legally, a Business Handling Personal Information must in principal disclose the Held Personal Data to the Principal without delay by means of delivery of written documents (or other means if the Principal requesting disclosure has agreed). However, if there is a risk that the appropriate execution of business operations would be markedly impaired as a result of disclosure of such Held Personal Data, such information need not be disclosed.
- In these Guidelines, as for Held Personal Data which is not expected to be disclosed because there is fear that disclosure of such data would markedly impair appropriate execution of business operations, the Business Handling Personal Information needs to use its best efforts to clarify contents of such data upon prior discussion with labor unions, etc. where necessary.
In addition, it is expected that Personal Information regarding personnel assessment and selection shall generally not be disclosed, and it is advisable that how to handle such information should be decided upon discussion with labor unions in advance. Furthermore, if items to be undisclosed are decided upon discussions with labor unions, the Business has to use its best efforts to keep employees informed of the contents of such decisions as much as possible (Refer to No. 3. 9 (page 30)).

In addition, if assessment standards are formulated, it is desirable to disclose the assessment standards, although the standards themselves do not fall under Personal Information.
III. Items that should be a guideline for the enterpriser to appropriately and effectively implement measures

7. Items related to suitable measures in light of the convenience to the Principal, which is stipulated in Article 29 Paragraph 2 of the Law

The Business Handling Personal Information must fully consider the place and time for browsing so that the Principal is able to make the Request of Disclosure, Etc. of Personal Data regarding employment management as smoothly as possible.

[Related Article]

Law Article 29 Paragraph 2

A Business Handling Personal Information shall have the right to request a Principal to disclose items sufficient for specifying the subject Held Personal Data with respect to a Request for Disclosure, Etc. In such cases, the Business Handling Personal Information must take suitable measures to provide information which contributes to the specification of relevant Held Personal Data and otherwise in light of the convenience to the Principal, so that the Principal is able to make the Request for Disclosure, Etc. easily and accurately.

[Commentary]

● Procedures for responding to Requests for Disclosure, Etc. and others are clearly indicated under the Law in order to lighten the burden of both the Principal and a Business Handling Personal Information. As part of this, the Law provides that “the Business Handling Personal Information must take suitable measures to provide information which contributes to the specification of relevant Held Personal Data and otherwise in light of the convenience to the Principal, so that the Principal is able to make the Request for Disclosure, Etc. easily and accurately”.

● As for “suitable measures in light of the convenience of the Principal”, it is required in these Guidelines that “The Business Handling Personal Information must fully consider the place and time for reviewing”. In concrete terms, the Business is required to take suitable measures so that the person is able to obtain relevant information which contributes to the specification of relevant Held Personal Data as easily as possible regardless of where he or she resides, works and his or her working hours.

● Examples of cases where the place and time for reviewing information appear fully considered include where in addition to posting notices and circulating memos in the workplace, the Business has published such information on the website which can be accessed easily.
III. Items that should be a guideline for the enterpriser to appropriately and effectively implement measures
8. Items regarding handling grievances which is stipulated in Article 31 of the Law
The Business Handling Personal Information must use its best efforts to establish a necessary system including establishing the counter to handle grievances and consultation to process grievances on handling Personal Information regarding employment management appropriately and promptly.

[Related Article]
Law Article 31

A Business Handling Personal Information must use best efforts to process grievances on handling Personal Information appropriately and promptly.

2. A Business Handling Personal Information must use its best efforts to establish a system required to achieve the purposes in the previous Paragraph.

[Commentary]
A Business Handling Personal Information must use its best efforts to process grievances regarding the handling of Personal Information appropriately and promptly. In addition, the Business must use its best efforts to establish a necessary system including establishing the counter to handle grievances and consultation to process grievances appropriately and promptly.

[Example cases of development of necessary systems]
1) Setting up a counter that handles grievances and consultations by employees, etc. regarding the handling of Personal Information regarding employment management, and placement of persons at such counter.
2) Establishing a system for processing grievances and consultations via telephone, mail, e-mail and fax.
3) Formulating and distributing manuals for the persons responsible for processing of grievances and consultations.
4) Deciding internal process relating to the processing of grievances, and informing all regarding such internal processes.
5) Transferring knowledge to the persons in charge of processing of grievances and consultations through training, etc.
III. Items that should be a guideline for the enterpriser to appropriately and effectively implement measures

9. Items that shall be taken into account when the Business Handling Personal Information must take measures to secure appropriate handling of Personal Information regarding employment management

(1) It is advisable that the Business shall notify and discuss where necessary with labor unions and others in advance when deciding issues regarding disclosure of Held Personal Information stipulated in 6 and other important issues about handling of Personal Information regarding employment management.

(2) It is advisable that the Business shall keep its employees informed when deciding important issues in (1) of 9.

[Commentary]
- When deciding important issues about handling Personal Information regarding employment management, it is advisable that the Business shall notify labor unions, etc. in advance, and consult with them when necessary. When important issues are decided, it is advisable that the Business will keeps the employees, etc. informed. It is important for both labor and management to be the main parties to the agreement, have common recognition regarding the agreed upon contents and thus prevent leakage of Personal Information and others.

(Please refer to page 11 for a definition of “Labor unions, etc.”).
IV. Handling of Personal Information regarding employment management by a business other than the Business Handling Personal Information.

A business other than the Business Handling Personal Information which is stipulated in Law Article 2 Paragraph 3 and who handles Personal Information regarding employment management shall use its best efforts to secure appropriate handling in line with No. 3.

*Please refer to commentary (Page 5 and 6-8) for “No.2 – definition of terms” for Law Article 2 Paragraph 3 and a Business Handling Personal Information which is stipulated in Law Article 2 Paragraph 3.

[Commentary]

- These guidelines are formulated pursuant to the Law and thus while the various obligations (refer to Pages 11-31) stipulated by Article 3 are not applied to businesses other than the Business Handling Personal Information under the Law, it is desirable that they use their best efforts to secure appropriate handling in line with these guidelines.

- As employment management information includes sensitive information such as clinical record, income and family relations, even the businesses other than the Business Handling Personal Information under the Law shall use their best efforts to secure appropriate handling of Personal Information regarding employment management in line with Article 3 in order to prevent damages given to the relevant Employee and the decrease in social credibility, etc. of the relevant business by leakage of such information.
<Reference 1> Delegation, provision to a third party and joint use

In both delegation arrangements and in the provision of Personal Information to third parties, Personal Information is transferred to an enterprise outside the Business. Whether a certain arrangement is considered a delegation or provision to a third party depends basically on the terms of the contract between the parties and the interpretation thereof, but treatment of delegation and provision to a third party is different under the Law Concerning Protection of Personal Information. In terms of provision to a third party, the Business Handling Personal Information needs to obtain the prior consent of the Principal or comply with the opt-out provisions of the Law (see page 25). Meanwhile, these are not required in delegation arrangements, but it is necessary for the Business Handling Personal Information to conduct necessary and appropriate supervision of the delegatee.

In addition, prior consent and opt-out are not needed in case that the personal information is jointly used within the scope of the Purpose of Use in order to provide comprehensive services among group companies, after the Principal is notified of the Purpose of Use, items of information to be jointly used, etc., or the Principal is placed in circumstances in which such matters can be easily learned. (Article 23 Paragraph 4 No. 3 of the Law)

<Examples of Delegation>
1) Personal Data is transferred to delegate information processing tasks such as inputting data.
2) Personal Data is transferred to delegate salary processing and other information processing tasks.

<Examples of provision to a third party>
1) Personal Data of a person who is to be dispatched to another company is handed over to the receiving company.
2) Personal Data is exchanged with or provided to parent/subsidiary/affiliate companies or group companies.
3) Employees’ health records are provided to an insurance company.
4) A recruiting company (such as a human resource consultant company) provides a client company with Personal Data of an individual such as income information, etc.

<Examples of joint use>
1) Group companies sharing employee information in order to deal with transfers of its employees among the group
2) Joint venture companies sharing employee information
3) Employers and labor unions, etc. sharing employee information
<Reference 2> Provision of Personal Information regarding Employment Management

- As Personal Information regarding employment management includes sensitive information such as clinical history, income and family relations, appropriate handling of information is needed, particularly when such information will be provided to a third party, where the risk is higher that leakage may occur. When obtaining the consent of the principal in order to provide personal information regarding employment management to a third party, it is desirable to specify the third party to the extent possible, and to make this known to the Principal. In addition, when getting prior consent of the Principal, it is desired that businesses obtain consent every time such information is to be provided to a third party, to the extent possible, so that the Principal's intent is accurately reflected.

- One requirement in providing for opt-out in the provision to third parties is to notify the Principal regarding the content of Personal Data to be provided, or place the Principal in circumstances in which such matters can be learned easily. “Circumstances in which the Principal can learn such matters easily” means that the Principal must be placed in circumstances that it is expected that the Principal will be able to learn without fail that [the opt-out regime] replaces the Principal’s consent, since personal information related to employment management includes sensitive information, and it is highly likely that such information was collected under the assumption that such information will not be provided easily to third parties.

<Examples of circumstances where the Principal can easily learn>
  1) [Information regarding opt-out] is continuously posted on a website where it can be assumed that the Principal will regularly browse.
  2) [Information regarding opt-out] is regularly published in a publication which is widely distributed within the company.
<Reference 3> Issues to consider when handling employment management information concerning health information

Employment management information concerning health information, such as results of health examinations, etc. require strict implementation of appropriate handling, and besides these Guidelines, “Items to consider for handling employment management information concerning health information” (No.102907 notice to Manager of Labor Standards Bureau dated on 29 Oct 2004. From hereinafter it is referred as “Items of Concern”) was formulated. Please refer to it together with the following points.

● When a business needs to collect health information from medical institutions, it is desirable for the business to obtain the consent of the employee after the purpose of acquiring such information is made clear, as well as to obtain the information by submission from the principal. (related to Items of Concern No. 3-1 (1))

When a business wants to obtain health information of employees from a medical institution, the Law provides that it is the obligation of the medical institution which provides information to a third party to obtain the consent of the Principal, not the business who receives such information. However, it is the business who actually uses such health information. Accordingly, the business should endeavor to obtain the consent of the Principal in advance, so that the medical institution will be able to obtain the employee’s consent smoothly.

In addition, as health information needs to be handled particularly carefully, it is desirable that the business receive information from the Principal, and not directly from the medical institutions.

● Health information that is to be handled by a party other than an occupational health business worker shall be appropriately processed so that it is limited to the range necessary for achieving the Purpose of Use (related to items of concern No. 3-2).

When appropriate diagnosis and health guidance for the employee are to be carried out based on test results of a health examination, specialized medical knowledge for diseases is required. Accordingly, it is advisable that specialists such as industrial physicians (occupational health business related worker) shall handle raw data such as test values.

Meanwhile, when health examination results are used in order to take employment measures (such as recommending taking time off, etc.), persons who are not specialists, such as the employee’s supervisor and human resource personnel, will be handling the health information of employees, but it is unnecessary for such persons to have raw data, and only a doctor’s findings should be necessary.

In such cases, such persons handling health information should be limited to the extent possible, and measures should be taken so that they handle only essential information which has gone through necessary processing by specialists.

● It is advisable that regulations regarded handling health information shall be formulated upon discussion with labor unions and others in the work place (related to items of concern No. 3-4 (1) (2))
Health information of employees is basically handled by specialists such as industry physicians for the purpose of securing the health of employees by persons in charge of employment management. Meanwhile there are cases where health information is handled by other medical institutions to which health examinations have been delegated or by supervisors of the employees and others who are not specialists and there are many opportunities of handling the information.

Accordingly, in terms of handling health information, it is desirable that provisions regarding handling of such information be established in internal company rules or the like, after discussions with the labor unions as necessary, and these rules be made known to employees and those handling such information, and such rules be followed in the handling of such information.

- The business should not obtain information regarding infectious diseases which are unlikely to infect others in the office such as HIV virus and hepatitis B or genetic information such as abnormal color sensation (related to items of concern No. 3-4 (4))

A business should not collect information regarding whether employees have HIV or Hepatitis B or C across the board, since it is unthinkable for such infections to spread when workers are engaged in normal day to day operations. In addition, there is no reason to make any accommodations in employment to such employees compared to other healthy employees, so unless there is a particular need in business operations, such information should not be obtained across the board.

In addition, the business should not obtain genetic information such as results of color test and others across the board, except in the case that there are some special reasons that the business needs to take into consideration.
Issues to consider in order to secure appropriate handling of personal information at the time of application for a job, temporary transfer to another company, change in employment and termination of employment

Issues for Businesses to consider regarding the handling of Personal Information related to employment management, other than those provisions to be complied with pursuant to the Law, are as follows. The issues are organized by stages in the work life of an employee – from application for a job, job transfers, to termination.

1) Application for employment

Personal Information that a business obtains from a job applicant is limited to that which serves the purpose of that particular job according to the Employment Security Law Guidelines. However such information may include sensitive information such as aptitude test results, and leakage of such information may cause significant damage to the Principal. In addition, there is a risk that Personal Information of rejected applicants will not be sufficiently protected compared to Personal Information of the currently employed employee. Therefore it is advisable that the following points shall be considered.

● Notification and disclosure of the Purpose of Use of personal information to an applicant have to be carried out by rational and appropriate means. For example, for disclosure, publication on the company’s website is not sufficient and the business needs to take care in selecting the appropriate media of communication so that such information is definitely communicated to the job applicant, such as by including such information in the application materials (please refer Pages 14-15 to “notification to the Principal” and “disclosure”).

● Use of Personal Information obtained from an applicant shall be, in principle, limited to that which is within the purpose of collection according to the Employment Security Law Guidelines, and use for other purposes shall be limited to cases where the Principal has agreed with such purpose or when pursuant to a law or ordinance.

When providing personal information obtained from job applicants to third parties, the business must either get the prior consent, or make clear the conditions required for opt-out in the written materials regarding in the job application forms. (Refer to Law Article 23 Paragraph 2 (Pages 24-25)). In either case, it is required that the party to which the information is to be provided shall be clearly stated so that the Principal can make a judgment regarding consent, etc.

When delegating the handling of Personal Data regarding an applicant, necessary and appropriate supervision for the delegate is needed based on the regulations 4 of III in these Guidelines (refer to page 20).

For information that is no longer necessary for hiring activities, such as the personal information of rejected job applicants, such information needs to definitely be destroyed, deleted or returned, including any copies. If such information is stored after the purpose of use is achieved, such information cannot be used outside the purpose of use, and must be subject to continuing security control measures.

2) Temporary or permanent transfers
When Personal Information about an employee is to be provided to a company to which such employee is to be temporarily or permanently transferred, this will generally be deemed to be a provision to a third party. It is desirable that the employer clearly indicate the possible range of companies to which he or she may be transferred on its website or the like, so that the Principal may make appropriate decisions as to whether to consent, etc.

When obtaining the prior consent of the Principal for the provision of Personal Information to a third party in connection with a company transfer, it is desirable for businesses to get consent every time such information is to be provided to a third party, to the extent possible, so that the Principal's intent is accurately reflected. (refer to Pages 34)

3) Termination

Keeping in mind the provisions of Labor Standards Law Article 109, which provides for the storage of payroll information for a certain period, in terms of Personal Information of terminated employees, if the purpose of use has been achieved, that portion, including copies, should be returned, destroyed or deleted appropriately and definitely at the time the purpose of use is achieved. In case that personal information is retained after the Purpose of Use is achieved, use of such information is not permitted for purposes other than the Purpose of Use, and must be subject to continuing security control measures.

If Personal Information pertaining to the terminated employee is to be provided to the terminated employee's new employer or new prospective employer, such provision is a provision to a third party, so prior consent of the Principal is required.