

## Amended Act on the Protection of Personal Information (Tentative Translation)

This is the translation of the amended Act on the Protection of Personal Information, coming into force within 2 years from the promulgation, September 9, 2015.

### NOTICE

\*This translation has not yet been proofread or corrected by a native English speaker or legal translation expert; this translation may be revised in the future.

\*Only the original Japanese texts of the Act has a legal effect, and the translations are to be used solely as reference materials to aid in the understanding of Japanese Act.

### Table of Contents

Chapter I General Provisions (Articles 1 to 3)

Chapter II Responsibilities of the National and Local Governments (Articles 4 to 6)

Chapter III Measures to Protect Personal Information

Section 1 Basic Privacy Policy (Article 7)

Section 2 National Measures (Articles 8 to 10)

Section 3 Measures by Local Governments (Articles 11 to 13)

Section 4 Cooperation between the National and Local Governments (Article 14)

Chapter IV Obligations of Business Operators Handling Personal Information,

Section 1 Obligations of Business Operators Handling Personal Information (Articles 15 to 35)

Section 2 Obligations of Business Operators Handling De-Identified Information (Articles 36 to 39)

Section 3 Supervision (Articles 40 to 46)

Section 4 Promotion of the Protection of Personal Information in the Private Sector (Article 47 to 58)

Chapter V Personal Information Protection Commission (Articles 59 to 74)

Chapter VI Miscellaneous Provisions (Article 75 to 81)

Chapter VII Penal Provisions (Article 82 to 88)

Chapter I General Provisions

(Purpose)

Article 1 This Act aims to protect the rights and interests of individuals while ensuring due consideration that proper and effective use of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched quality of life for the people of Japan among other useful applications; by setting forth basic principles for the proper handling of personal information, creating government's basic policy with regard to this, and establishing other particulars to serve as a basis for measures to protect personal information, as well as by clarifying the responsibilities, etc. of the national and local governments and establishing the obligations, etc. that business operators handling personal information are required to fulfill, in light of the significantly expanded uses to which personal information is being put as our advanced information- and communication-based society evolves.

(Definitions)

Article 2

(1) The term "personal information" as used in this Act means information about a living individual, and falls under one of the following items:

(i) information that can be used to identify that specific individual due to its inclusion of a name, date of birth, or other description contained (any and all matters (that excludes individual identification codes) written, recorded or otherwise expressed using voice, movement or other methods in documents, drawings or electromagnetic records (meaning records made by electromagnetic format (electronic, magnetic or any other format that cannot be recognized through the human senses; the same applies in next paragraph, item (ii)); the same applies in Article 18, paragraph (2); the same applies hereinafter) in such information (this includes any information that can be cross-checked against other information and thereby used to identify that specific individual).

(ii) Information that contains individual identification codes

(2) The term "personal identification code" as used in this Act means any character, letter, number, symbol or other marking that falls under one of the following items specified by Cabinet Order.

(i) Any character, letter, number, symbol or other marking converted from a distinguishing part of a specific individual's body so that it may be used with a computer, and any such information that can identify the specific individual.

(ii) Any character, letter, number, symbol or other marking that is allocated to an individual in regards to the use of services provided or the purchase of goods sold, or that is entered into cards or other documents issued to an individual or recorded by electromagnetic format, and any such information that can identify the using individual, the purchasing individual, or the individual being issued through the allocation of differing character, letter, number, or symbol, or writing or recording of such information so as to differentiate among said using individual, purchasing individual, or individual being issued.

(3) The term "sensitive personal information" used in this Act means a personal information that contains descriptions that have been specified by Cabinet Order to require special consideration in handling so as to avoid any unfair discrimination, prejudice or other

disadvantage to an individual based on person's race, creed, social status, medical history, criminal records or the fact that a person has incurred damages through an offense, etc.

(4) The term “personal information database etc.” used in this Act means a set of information which includes personal information as set forth below (this excludes sets of information specified by Cabinet Order to have little possibility of harming the rights and interests of an individual considering the manner such personal information is used).

(i) a set of information structurally organized to enable a computer to be used to retrieve certain personal information from it; or,

(ii) in addition to what is listed in the preceding item, a set of information specified by Cabinet Order as being structurally organized to be easily retrieved certain personal information.

(5) The term "business operator handling personal information" as used in this Act means a business operator that has a personal information database etc. for business use; however, the following entities are excluded;

(i) national government organs;

(ii) local governments;

(iii) incorporated administrative agencies and other such entities (meaning independent administrative agencies and other such entities as provided in Article 2, paragraph (1) of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (Act No. 59 of 2003); the same applies hereinafter);

(iv) local incorporated administrative agencies (meaning local incorporated administrative agencies as provided in Article 2, paragraph (1) of the Local Incorporated Administrative Agencies Act (Act No. 118 of 2003); the same applies hereinafter);

(6) The term “personal data” as used in this Act means personal information compiled in a personal information database etc.

(7) The term “retained personal data” as used in this Act means personal data that a business operator handling personal information has the authority to disclose; to correct, add or delete content from; to discontinue use of; to erase; or to discontinue provision to a third party, other than what Cabinet Order provides for as data which is likely to harm the public interest or other interests, if its presence or absence is known and other than data that will be deleted within the period of less than one year that Cabinet Order specifies.

(8) The term “person” as used in this Act in relation to personal information means the specific individual that the personal information can be used to identify.

(9) The term “the de-identified information” as used in this Act, according to the categories of personal information set forth below, means information regarding an individual that is gained from processing personal information so as to prevent the identification of a specific individual taking measures prescribed by the items below, and that do not allow restoring of said personal information.

(i) The deletion of a part of descriptions that contains personal information falling under paragraph (1), item (i) above (this includes replacing said part of descriptions with other descriptions through methods that do not allow for the restoring of said part of descriptions).

(ii) The deletion of all personal identification codes that contain personal information falling under paragraph (1), item (i) above (this includes replacing said personal identification code with other descriptions through methods that do not allow for the restoring of said part of personal identification codes).

(10) The term “business operator handling de-identified information” as used in this Act means a business operator using for its business a set of information which includes de-identified information, which is structurally organized to enable a computer to be used to retrieve certain de-identified information, and which is other set of de-identified information that Cabinet Order provides for as being structurally organized to enable certain de-identified information to be easily retrieved from it (this is referred to as “de-identified information database etc.” in Article 36, paragraph (1)). However, the business operators set forth in one of the items of paragraph (5) are excluded.

(Basic Principle)

Article 3 The proper handling of personal information must be pursued in view of the fact that personal information should be handled cautiously based on the philosophy of respecting the autonomy of the individual.

## Chapter II Responsibilities, etc. of the National and Local Governments

(Responsibilities of the National Government)

Article 4 The National Government is responsible for comprehensively formulating and implementing the necessary measures to ensure the proper handling of personal information in conformity with the purport of this Act.

(Responsibilities of Local Governments)

Article 5 Local governments are responsible for formulating and implementing the necessary measures to ensure the proper handling of personal information based on the characteristics of the area, in conformity with the purport of this Act.

(Legislative Measures etc.)

Article 6 The Government must take the necessary legislative and other measures to ensure that special measures will be taken for the protection of personal information, especially that personal information which requires the strict implementation of proper handling so that the rights and interests of individuals can be further protected in view of the nature and the method of utilization of the personal information. Concurrently, the Government must also coordinate with the governments of other countries through cooperation with international organs and other international frameworks to take the measures necessary to building a system for personal information that is internationally integrated.

## Chapter III Measures for the Protection of Personal Information, etc.

### Section 1 Basic Policy on the Protection of Personal Information

Article 7

(1) The Government must establish a basic policy (hereinafter referred to as a “Basic Policy”) so as to further comprehensive and integrated measures to protect personal information.

(2) The Basic Policy must provide for the following matters:

(i) the basic approach of action for the promotion of measures to protect personal information.

(ii) the matters of measures to protect personal information that are to be taken by the national government;

(iii) the basic matters of the measures to protect personal information that are to be taken by local governments;

(iv) the basic matters of the measures to protect personal information that are to be taken by incorporated administrative agencies and other such entities;

(v) the basic matters of the measures to protect personal information that are to be taken by local incorporated administrative agencies;

(vi) the basic matters of the measures to protect personal information that are to be taken by business operators handling personal information, business operators handling de-identified information and accredited personal information protection organizations as provided in Article 50, paragraph (1);

(vii) matters about the smooth processing of complaints about the handling of personal information;

(viii) other material matters for the promotion of measures to protect personal information.

(3) The Prime Minister must prepare a draft Basic Policy created by the Personal Information Protection Commission, and ask for Cabinet approval.

(4) Following the Cabinet approval under the preceding paragraph, the Prime Minister must disclose the Basic Policy to the public without delay.

(5) The provisions of the preceding two paragraphs apply mutatis mutandis to amendments to the Basic Policy.

## Section 2 National Measures

(Support for Local Governments, etc. )

Article 8 The national government must take necessary measures such as providing information and formulating guidelines to ensure the business operators and others properly and effectively implement the measures that they are required to take, in order to support action that the people, business operators and others take to ensure the proper handling of personal information.

(Complaint Processing Measures)

Article 9 The national government must take the necessary measures to ensure the appropriate, prompt processing of complaints arising between business operators and persons with regard to the handling of personal information.

(Measures to Ensure Proper Handling of Personal Information)

Article 10 The national government must take the necessary measures to ensure the proper handling of personal information by business operators handling personal information as provided in the next Chapter, by effecting an appropriate division of roles between the national and local governments.

### Section 3 Local Government Measures

(Protection of Personal Information Held by Local Governments, etc.)

#### Article 11

(1) A local government must endeavor to take the necessary measures to ensure the proper handling of the personal information it holds, in consideration of such factors as the nature of the personal information and the purpose, etc. for which it holds that personal information.

(2) A local government must endeavor to take the necessary measures to ensure the proper handling of personal information that is held by the local incorporated administrative agencies it has established, in accordance with the nature of the agency and the content of its operations.

(Support for Area Business Operators)

Article 12 A local government must endeavor to take the necessary measures to support business operators and residents within its territory so as to ensure the proper handling of personal information.

(Mediation, etc. for Complaint Processing)

Article 13 A local government must endeavor to provide mediation for complaint processing and take other necessary measures to ensure that any complaint arising between an enterprise and a person with regard to the handling of personal information is handled appropriately and promptly.

### Section 4 Cooperation between the National and Local Governments

Article 14 National and local governments must cooperate in taking measures to protect personal information.

## Chapter IV Obligations, etc. of Business Operators Handling Personal Information

### Section 1 Obligations of Business Operators Handling Personal Information

(Specifying the Purpose of Use)

#### Article 15

(1) In handling personal information, the business operator handling personal information must specify as precise as possible about the purpose for which it uses that information (hereinafter referred to as "Purpose of Use") .

(2) A business operator handling personal information must not change the Purpose of Use

beyond a scope that makes it reasonable to consider the Purpose of Use after the change to be related to what it was before the change.

(Restriction due to Purpose of Use)

#### Article 16

(1) A business operator handling personal information must not handle personal information beyond the scope necessary for achieving of the Purpose of Use specified pursuant to the provisions of the preceding Article without in advance obtaining the person's consent to do so.

(2) If, due to a merger or other such circumstances, a business operator handling personal information acquires personal information when succeeding to the business of another business operator handling personal information, it must not handle that personal information beyond the scope necessary for achieving pre-succession Purpose of Use for that personal information without in advance obtaining the person's consent to do so.

(3) The provisions of the preceding two paragraphs do not apply in the following cases:

(i) the business operator handles the personal information outside its Purpose of Use based on law and regulations;

(ii) it is necessary for the business operator to handle the personal information outside its purpose of use in order to protect the life, body, or property of an individual, and it is difficult to obtain the consent of the person;

(iii) there is a special need for the business operator to handle the personal information outside its purpose of use in order to improve public health or promote healthy child development, and it is difficult to obtain the consent of the person;

(iv) it is necessary for the business operator to handle the personal information outside its purpose of use in order to cooperate with a national government organ, local government, or person or business operator entrusted thereby with performing the affairs prescribed by laws and regulations, and obtaining the consent of the person is likely to interfere with the performance of those affairs.

(Proper Acquisition)

#### Article 17

(1) A business operator handling personal information must not acquire personal information through deception or other wrongful means.

(2) A business operator handling personal information must not acquire sensitive personal information without in advance obtaining the person's consent to do so, except in the following cases;

(i) the business operator obtain the sensitive personal information based on law and regulations;

(ii) it is necessary for the business operator to obtain the sensitive personal information in order to protect the life, body, or property of an individual, and it is difficult to obtain the consent of the person;

(iii) there is a special need for the business operator to obtain the sensitive personal information in order to improve public health or promote healthy child development, and it is difficult to obtain the consent of the person;

(iv) it is necessary for the business operator to obtain the sensitive personal information in order to cooperate with a national government organ, local government, or person or business operator entrusted thereby with performing the affairs prescribed by laws and regulations, and obtaining the consent of the person is likely to interfere with the performance of those affairs.

(v) the sensitive personal information has been made public by the person, national government organ, local government, a business operator set forth in one of the items of Article 76, paragraph (1), and any other person or business operator prescribed by rules of the Personal Information Protection Commission;

(vi) Other cases that are prescribed by Cabinet Order as corresponding to any of the preceding cases.

(Notice, etc. of the Purpose of Use at the Time of Acquisition)

#### Article 18

(1) Unless the Purpose of Use has already been disclosed to the public, a business operator handling personal information must promptly notify the person of that Purpose of Use or disclose this to the public once it has acquired personal information.

(2) Notwithstanding the provision of the preceding paragraph, a business operator handling personal information must explicitly specify the purpose of use to the person in advance if acquiring, as a result of concluding a contract with the person, personal information about the person which appears in a written contract or other document (this includes electromagnetic records; hereinafter the same applies in this paragraph); or if acquiring, directly from the person, personal information about that person which appears in a document; provided, however, that this does not apply if there is an urgent necessity to dispense with this requirement in order to protect the life, body or property of an individual.

(3) If a business operator handling personal information changes the Purpose of Use, it must notify the person of the altered Purpose of Use or disclose this to the public.

(4) The provisions of the preceding three paragraphs do not apply in the following cases:

(i) notifying the person of the Purpose of Use or disclosing this to the public is likely to harm the life, body, property, or other rights or interests of the person or a third party;

(ii) notifying the person of the Purpose of Use or disclosing this to the public is likely to harm the rights or legitimate interests of the business operator handling personal information;

(iii) it is necessary to cooperate with a national government organ or a local government in performing the affairs prescribed by laws and regulations, and notifying the person of the Purpose of Use or disclosing this to the public is likely to interfere with the performance of those affairs;

(iv) the Purpose of Use is considered to be clear, in light of the circumstances in which the personal information is acquired.

(Maintenance the Accuracy of Data)

Article 19 A business operator handling personal information must endeavor to keep the content of personal data accurate and up to date, within the scope necessary for achieving the Purpose of Use, and delete such personal data without delay when its use is no longer required.

(Security Measures)

Article 20 A business operator handling personal information must take the necessary and appropriate measures to ensure the secure management of personal information, such measures to prevent leakage, loss or damage to the personal data it handles.

(Supervision of Employees)

Article 21 In having an employee handle personal data, a business operator handling personal information must exercise the necessary and appropriate supervision over that employee to ensure the secure management of the personal data.

(Supervision of Entrusted persons)

Article 22 If a business operator handling personal information entrusts another business operator with all or part of the handling of personal data, it must exercise the necessary and appropriate supervision over the business operator it entrusts, so as to ensure the secure management of the personal data.

(Restriction of Provision to a Third Party)

Article 23

(1) A business operator handling personal information must not provide a third party with personal data without in advance obtaining the person's consent to do so, except in the following cases:

(i) the business operator provides the third party with personal data based on laws and regulations;

(ii) it is necessary for the business operator to provide the third party with the personal data in order to protect the life, body, or property of an individual, and it is difficult to obtain the consent of the person.

(iii) there is a special need for the business operator to provide the third party with the personal data in order to improve public health or promote healthy child development, and it is difficult to obtain the consent of the person;

(iv) it is necessary for the business operator to provide the third party with the personal data in order to cooperate with a national government organ, local government, or an individual or a business operator entrusted thereby with performing the affairs prescribed by laws and regulations, and obtaining the consent of the person is likely to interfere with the performance of those affairs.

(2) Notwithstanding the provisions of the preceding paragraph, if a business operator handling personal information agrees, at the request of a person, to stop providing a third

party with any personal data it provides to third parties which can be used to identify the person, but then as prescribed by rules of the Personal Information Protection Commission, notifies the person of the following information in advance or makes that information readily accessible to the person in advance, and notifies the Personal Information Protection Commission in advance, the business operator may provide that personal data to a third party:

(i) the fact that providing the data to a third party constitutes the Purpose of Use;

(ii) the items of the personal data it will provide to the third party;

(iii) the means in which it will provide the data to a third party;

(iv) the fact that it will stop providing personal data that can be used to identify the person to a third party at the request of the person;

(v) the means to receive the request of the person.

(3) Before changing a particular set forth in item (ii), (iii) or (v) of the preceding paragraph, the business operator handling personal information must in advance, as prescribed by rules of the Personal Information Protection Commission, notify the person of the matters of the change or make those details readily accessible to the person, and must notify the Personal Information Protection Commission.

(4) When the Personal Information Protection Commission receive the notification under paragraph (2), it must disclose the items of the notification to the public, as prescribed by rules of the Personal Information Protection Commission. The same applies for notifications made under the preceding paragraph.

(5) In the following cases, the individual or business operator being provided with the personal data must not be deemed to be a third party as regards the application of the provisions of each preceding paragraph:

(i) if the business operator handling personal information entrusts with all or part of the handling of personal data within the scope necessary for achieving the Purpose of Use;

(ii) if the personal data is provided when a business operator succeeds to the business of the business operator due to a merger or other such circumstances;

(iii) if personal data which is used jointly with a specific individual or business operator is provided to the individual or business operator, and the individual or business operator notify the person of this in advance as well as notify the person of the items of the personal data of which the specific individual or business operator have joint use, the extent of the joint users, the user's purposes of use, and the name of the individual or business operator responsible for managing the personal data, or the individual or business operator make the foregoing information readily accessible to the person in advance.

(6) If a user's purpose of use or the name of the individual or business operator responsible for managing the personal data provided for in item (iii) of the preceding paragraph changes, the business operator handling personal information must notify the person of the content of the change in advance or make the content readily accessible to the person in advance.

(Restrictions on Provision to a Third Parties in Other Countries)

Article 24 A business operator handling personal information must, when providing personal data to a third party ( this excludes individuals or business operators that put into place a system compliant with the standards prescribed by rules of the Personal Information Protection Commission as is necessary to continuously take of measures corresponding with measures that business operators handling personal information ought to carry out pursuant to the provisions of this Section with regard to handling of personal data; the same applies in this Article hereinafter.) in a foreign country (any country or territory outside of the region of Japan; the same applies hereinafter) (excluding countries prescribed by rules of the Personal Information Protection Commission to be foreign countries possessing personal information protection systems recognized to be at the same level as Japan's in terms of protecting the rights and interests of individuals; the same applies hereinafter in this Article), obtain the prior consent of the person for the provision of such personal data to a third party in a foreign country, except in cases set forth in each item of paragraph (1) of the preceding Article. The provisions of that the preceding Article do not apply in this case.

(Creating Records, etc. of Provisions to a Third Party)

#### Article 25

(1) A business operator handling personal information must, when providing personal data to a third party (this excludes business operators provided for in each item of Article 2, paragraph (5); the same applies hereinafter in this Article and the next Article), make a record of the matters as prescribed by rules of the Personal Information Protection Commission, regarding the date such personal data was provided, the name of the third party, as well as other matters prescribed by rules of the Personal Information Protection Commission. However, this provision does not apply to cases of such personal data provision falling under any of the items of Article 23, paragraph (1) or paragraph (5) (any of the items of Article 23, paragraph (1) for the provision of personal data under the preceding Article).

(2) A business operator handling personal information must store records set forth in the preceding paragraph, from the day when the said records are created for a period of time prescribed by rules of the Personal Information Protection Commission.

(Confirmation Upon Receiving, etc.)

#### Article 26

(1) A business operator handling personal information must, upon being provided personal data from a third party, confirm the following matters prescribed by rules of the Personal Information Protection Commission. However, this provision does not apply to cases of such personal data provision fall under any of the items of Article 23, paragraph (1) or paragraph (5).

(i) The name and address of the third party, and the name of the representative (the representative or the manager for an association or foundation that are not juridical person) for juridical person;

(ii) The details of the acquisition of the personal data by the third party.

(2) While the business operator handling personal information carries out the confirmation under the preceding paragraph, the third party of the preceding paragraph must not falsely present to the business operator handling personal information the matters related to the confirmation.

(3) When the business operator handling personal information carries out the confirmation under the paragraph (1), the business operator must, prescribed by rules of the Personal Information Protection Commission, make records of the date on which such personal data was provided, matters related to the confirmation, and other matters prescribed by rules of the Personal Information Protection Commission.

(4) A business operator handling personal information must store such records beginning with the day on which the said records are created and for a period of time prescribes by rules of the Personal Information Protection Commission.

(Disclosure, etc. of Matters about the Retained Personal Data)

#### Article 27

(1) A business operator handling personal information must make the following matters about the retained personal data accessible to persons (making that matters accessible includes providing answers without delay as requested by persons):

(i) the name of the business operator handling personal information;

(ii) the Purpose of Use of all retained personal data (unless this falls under Article 18, paragraph (4). items (i) through (iii));

(iii) the procedures for dealing with requests under the provisions of the following paragraph, paragraph (1) of the next Article; Article 29, paragraph (1), or Article 30, paragraph (1) or paragraph (3) (including the amount of the fee, if one is set pursuant to the provision of Article 33, paragraph (2));

(iv) information other than as set forth in the preceding three items which is specified by Cabinet Order as needing to be made accessible in order to ensure the proper handling of retained personal data.

(2) If a business operator handling personal information is requested by a person to notify the person of the Purpose of Use of the retained personal data that can be used to identify the person, the business operator must notify the person without delay; provided, however, that this does not apply in a case falling under one of the following items:

(i) the Purpose of Use of the retained personal data that can be used to identify the person has been made clear pursuant to the provisions of the preceding paragraph;

(ii) a case falling under Article 18, paragraph (4), item (i) through (iii).

(3) If a business operator handling personal information decides not to notify the person of the Purpose of Use of the retained personal data as requested pursuant to the preceding paragraph, the business operator must notify the person of this without delay.

(Disclosure)

#### Article 28

(1) The person may request the business operator handling personal information to disclose the retained personal data that can be used to identify the person.

(2) When the business operator handling personal information is requested under the

provision of the preceding paragraph, the business operator must disclose the retained personal data without delay using the means that Cabinet Order provides for. However, in case falling under one of the following items, the business operator may choose not to disclose all or part of the retained personal data:

(i) if disclosure is likely to harm the life, body, property, or other rights or interests of the person or a third party;

(ii) if disclosure is likely to seriously interfere with the proper implementation of the business of the business operator handling personal information;

(iii) if disclosure would violate any other law or regulation.

(3) If a business operator handling personal information decides not to disclose all or part of the retained personal data as requested pursuant to the provision of the preceding paragraph (1), or there is no retained personal data, the business operator must notify the person of this without delay.

(4) If, pursuant to the provisions of any other law and regulation, all or part of the retained personal data that can be used to identify a person is to be disclosed to the person by a means equivalent to what is prescribed in the main clause of paragraph (2), the provisions of paragraph (1) and (2) do not apply to either the whole or the relevant part of the retained personal data.

(Corrections etc.)

#### Article 29

(1) The person may request the business operator handling personal information to correct, add, or delete (hereinafter referred to as “corrections etc.” hereinafter in this Article) the content of the retained personal data that can be used to identify the person, when the content of the retained personal data is not factual.

(2) If a business operator handling personal information is requested under the provision of the preceding paragraph, unless another law or regulation specifies special procedures for such corrections, etc. to the data, the business operator must undertake the necessary investigations without delay within the scope that is necessary for achieving the Purpose of Use, and, on the basis of the results, correct the retained data.

(3) Once a business operator handling personal information either corrects all or part of the retained personal data that it has been requested to correct under the provision of paragraph (1), or decides not to make such a correction etc., the business operator must notify the person of this (and of the content of the corrections etc. if made) without delay.

(Discontinuance etc. of using personal data.)

#### Article 30

(1) The person may request the business operator handling personal information to discontinue using or delete (hereinafter referred to as “Discontinuance, etc.” in this Article) the retained personal data that can be used to identify the person, when the personal data is handled in violation of the provisions of Article 16 or was acquired in violation of the provisions of Article 17.

(2) If a business operator handling personal information receives the request under the provision of the preceding paragraph, and there are found to be grounds for that request, the business operator must discontinue of the relevant retained personal data without delay to the extent necessary to redress the violation; however, that this does not apply if the discontinuance, etc. of the relevant retained personal data would require a costly expenditure or prove otherwise difficult, and the business operator takes the necessary alternative measures to protect the rights and interests of the person.

(3) The person may request the business operator handling personal information to discontinue providing the relevant retained personal data to a third party when the retained personal data that can be used to identify the person is being provided to the third party in violation of the provisions of Article 23, paragraph (1) or Article 24.

(4) If a business operator handling personal information receives a request under the provision of the preceding paragraph and there are found to be grounds for that request, the business operator must discontinue providing the relevant retained personal data to a third party without delay; however, that this does not apply if to stop providing the third party with the relevant retained personal data would require a costly expenditure or prove otherwise difficult, and the business operator takes the necessary alternative measures to protect the rights and interests of the person.

(5) Once a business operator handling personal information either discontinues all or part of the retained personal data that it has been requested to discontinue using pursuant to the provision of paragraph (1), or decides not to discontinue the use of it, or once a business operator handling personal information either discontinues providing all or part of the retained personal data to a third party that it has been requested under the provision of the preceding paragraph (3) or decides not to discontinue providing the retained personal data to a third party, the business operator must notify the person of this without delay.

(Explanation of Reasons)

Article 31 If, pursuant to the provisions of Article 27, paragraph (3); Article 28, paragraph (3); Article 29, paragraph (3), paragraph (3), item (v) of the preceding Article, a business operator handling personal information notifies a person that has requested it to take measures that it will not take all or part of the requested measures or that it will take different measures, the business operator must endeavor to explain its reasons for this to the person.

(Procedures for Dealing with Requests for Disclosure and Other Handling)

Article 32

(1) A business operator handling personal information may establish, as prescribed by Cabinet Order, how it will accept demands under the provision of Article 27, paragraph (2), or requests that may be made under the provisions of Article 28, paragraph (1), Article 29, paragraph (1), Article 30, this Article, paragraphs (1) or (3) (hereinafter referred to as request for disclosure etc.” and Article 53, paragraph (1)). In this such case, any person making a request for disclosure etc. must comply with the procedures.

(2) A business operator handling personal information may request a person requesting disclosure or other handling to present sufficient matters to identify the retained personal data that would be subject to the disclosure or other handling. In such a case, the business operator handling personal information must provide information to help the person identify the relevant retained personal data or take other appropriate measures in consideration of

the person's convenience, so as to allow the person to easily and accurately request disclosure or other handling.

(3) A person may request disclosure or other handling thorough a representative, as prescribed by Cabinet Order.

(4) In establishing procedures for dealing with requests for disclosure and other handling pursuant to the preceding three paragraphs, a business operator handling personal information must take care to ensure that the procedures do not impose an excessive burden on persons.

(Fees)

#### Article 33

(1) When a business operator handling personal information is requested to notify a person of the Purpose of Use under the provision of Article 27, paragraph (2), or receives a request to make disclosure under the provision of Article 28, paragraph (1), it may collect a fee for taking the relevant measures.

(2) If a business operator handling personal information collects a fee pursuant to the provisions of the preceding paragraph, it must fix the amount of that fee within a scope that can be considered reasonable in consideration of actual costs.

(Claims in Advance)

#### Article 34

(1) Should a person attempt to file a lawsuit regarding the request under the provisions of Article 28, paragraph (1), Article 29, paragraph (1), Article 30, paragraphs (1) or (3), such a lawsuit may not be filed unless the request is made in advance to the business operator, which the lawsuit is to be filed against, and two weeks have passed since the arrival date of the request. However, this provision does not apply when the business operator which the lawsuit is to be filed against has rejected that request.

(2) The request of the preceding paragraph is deemed to have arrived at the time that such a request should normally arrive.

(3) The provisions of the preceding two paragraphs applies mutatis mutandis regarding filings for provisional injunctions regarding the request under the provisions of Article 28, paragraph (1), Article 29, paragraph (1), Article 30, paragraphs (1) or (3).

(Processing of Complaints by Business Operators Handling Personal Information)

#### Article 35

(1) A business operator handling personal information must endeavor to process complaints about the handling of personal information appropriately and promptly.

(2) A business operator handling personal information must endeavor to establish the necessary systems for achieving the purpose referred to in the preceding paragraph.

### Section 2 Duties of Business Operators Handling De-identified Information

(Creation of De-identified Information)

Article 36

(1) When a business operator handling personal information creates de-identified information (this is limited to information comprising the de-identified information database etc.; hereinafter the same applies), the business operator processes such personal information in accordance with the requirement of the standard prescribed by the rules of the Personal Information Protection Commission so that any person is unable to identify a specific individual and restore the personal information used in the creation of the de-identified information.

(2) When a business operator handling personal information creates de-identified information, the business operator must take measures to ensure the secure management of such information in accordance with standards prescribed by rules of the Personal Information Protection Commission in such a way that prevents the leakage of any description deleted from the personal information used in the creation of the de-identified information, as well as the leakage of any personal identification code and information regarding the processing method carried out pursuant to the preceding paragraph.

(3) When a business operator handling personal information creates de-identified information, the business operator must, as prescribed by rules of the Personal Information Protection Commission, disclose the items of the information regarding the individual included within such de-identified information to the public.

(4) When a business operator handling personal information creates de-identified information and provides a third party with such de-identified information, the business operator must disclose in advance, the items of the information regarding the individual included within such de-identified information provided to the third party and the method such information will be provided to the public, as prescribed by rules of the Personal Information Protection Commission, and must explicitly specify to the third party that the information provided is de-identified information.

(5) When a business operator handling personal information creates de-identified information and handles the de-identified information itself, the business operator must not cross reference the de-identified information against other information to identify the person related to the personal information used to create the de-identified information.

(6) When a business operator handling personal information creates de-identified information, the business operator must, itself, endeavor to take the necessary and appropriate measures for securely managing of such de-identified information, to carry out processing of complaints about the creation and other handling of such de-identified information, and to take other necessary measures for ensuring the proper handling of such de-identified information, and must also endeavor to disclose the content of those measures to the public.

(Provision of De-Identified Information)

Article 37 When a business operator handling de-identified information provides de-identified information (this excludes de-identified information created by itself; hereinafter the same applies to this Section) to a third party, the business operator must, disclose in advance the items of the information regarding the individual included within such de-identified information provided to the third party and the method such information was

provided to the public, as prescribed by rules of the Personal Information Protection Commission, and must explicitly specify to the third party that the information provided is de-identified information.

(Prohibition of Actions Leading to Identification)

Article 38 In handling de-identified information, a business operator handling de-identified information must not acquire descriptions deleted from the personal information, personal identification codes, nor information related to the processing method carried out pursuant to the provisions of Article 36, paragraph (1), nor reference the de-identified information against other information for the purpose of identifying the person related to the personal information used in the creation of the de-identified information.

(Security Measures)

Article 39 A business operator handling de-identified information must, itself, endeavor to take the necessary and appropriate measures for securely managing de-identified information, to carry out processing of complaints about the handling of such de-identified information, and to take other necessary measures for ensuring the proper handling of such de-identified information, and must also endeavor to disclose the content of those measures to the public.

Section 3 Supervision

(Reports and On-Site Inspections)

Article 40

(1) The Personal Information Protection Commission may request to submit any necessary reports or documentation regarding the handling of personal information or de-identified information (hereinafter referred to as “personal information etc.”) from business operators handling personal information or business operators handling de-identified information (hereinafter referred to as “business operators handling personal information etc.”), and the Commission may dispatch its officers to enter the offices and other necessary locations of the business operator handling personal information etc., or inquire about the handling of personal information etc., or inspect books, document and other items to the extent that is necessary for implementing the provisions of preceding two Sections and this Section.

(2) Officers carrying out on-site inspections pursuant to the provision of the preceding paragraph must carry identification demonstrating their credentials, and, present this identification if requested to do so by a relevant person.

(3) The authority of the on-site inspection under the paragraph (1) must not be construed with the authority for a criminal investigation.

(Guidance and Advice)

Article 41 The Personal Information Protection Commission may guide or advise a business operator handling personal information etc. on the handling of personal information etc. to the extent that this is necessary for implementing the provisions of preceding two Sections.

(Recommendations and Orders)

Article 42

(1) If a business operator handling personal information violates one of the provisions of Articles 16 through 18, Articles 20 through 22, Article 23 (excluding paragraph (4)), Article 24, Article 25, Article 26 (excluding paragraph (2)), Article 27, Article 28 (excluding paragraph (1)), Article 29, paragraphs (2) or (3), Article 30, paragraphs (2), (4) or (5), Article 33, paragraph (2), or Article 36 (excluding paragraph (6)), or if a business operator handling de-identified information violates one of the provisions of Articles 37 or 38, and the Commission finds it necessary to do so in order to protect the rights and interests of an individual, the Commission may recommend a business operators handling personal information etc. to stop committing violation and to take the necessary measures to rectify the violation.

(2) If a business operator handling personal information etc. which receives a recommendation under the provisions of the preceding paragraph does not take the measures as recommended, without a legitimate reason for failing to do so, and the Personal Information Protection Commission finds that serious harm to the rights and interests of individuals is imminent, the Commission may order the business operator handling personal information etc. to take the measures as recommended.

(3) Notwithstanding the provisions of the preceding two paragraphs, if a business operator handling personal information violates one of the provisions of Article 16, Article 17, Articles 20 through 22, Article 23, paragraph (1), Article 24, Article 36, paragraphs (1), (2) or (5), or if a business operator handling de-identified information violates the provisions of Article 38, and the Personal Information Protection Commission finds it necessary for measures to be taken urgently due to the fact that serious harm is being done to the rights and interests of an individual, the Personal Information Protection Commission may order the business operator handling personal information etc. to stop committing the violation and to take the necessary measures to rectify the violation.

(Restrictions on the Exercise of Authority by the Personal Information Protection Commission)

#### Article 43

(1) In collecting a report or materials from a business operator handling personal information etc. or in carrying out an on-site inspection, in guiding it, advising it, recommending it or issuing an order to it pursuant to the provisions of one of the preceding three Articles, the Personal Information Protection Commission must not interfere with the freedom of expression, academic freedom, freedom of religion, or freedom of political activity.

(2) In light of the purport of the provision of the preceding paragraph, the Personal Information Protection Commission must not exercise the authority thereof over any action of a business operator handling personal information providing a person set forth in one of the items of Article 76, paragraph (1) with personal information etc. (but only if that person will handle the personal information for the purpose prescribed in the relevant item).

(Delegation of Authority)

#### Article 44

(1) If the Personal Information Protection Commission finds it necessary for issuing a recommendation or an order effectively under the provisions of Article 42 to a business operator handling personal information etc., owing to a need to ensure the proper handling of personal information etc. in an urgent and intensive manner or any situation prescribed

by Cabinet Order, the Commission may delegate authority to the Minister having jurisdiction over the business undertaking in which the business operator handling personal information is engaged (herein after referred to as “Minister having jurisdiction over the business”) under Article 40, paragraph (1), as prescribed by Cabinet Order,

(2) When the Minister having jurisdiction over the business exercises the authority delegated pursuant to the provision of the preceding paragraph, the Minister must, as prescribed by Cabinet Order, report the results to the Personal Information Protection Commission.

(3) The Minister having jurisdiction over the business may, as prescribed by Cabinet Order, delegate authority all or part delegated pursuant to the provision of paragraph (1) and the authority under the preceding paragraph to the head of local branch bureaus and departments pursuant to the provisions in Article 43 of the Act for Establishment of the Cabinet Office (Act No. 89 of 1999) or other heads of departments or organs as prescribed by Cabinet Order.

(4) The Minister with jurisdiction over the issue may delegate authority (This is limited to matters related to the jurisdiction of the Financial Services Agency, and excludes matters prescribed by Cabinet Order.) delegated pursuant to the provisions of paragraph (1) and the authority under the paragraph (2) to the Commissioner of the Financial Services Agency.

(5) The Commissioner of the Financial Services Agency may, as prescribed by Cabinet Order, delegate a part of the authority delegated pursuant to the provision of the preceding paragraph to the Securities and Exchange Surveillance Commission.

(6) The Commissioner of the Financial Services Agency may, as prescribed by Cabinet Order, delegate a part of the authority (This excludes the authority delegated to the Securities and Exchange Surveillance Commission pursuant to the provision of the preceding paragraph.) delegated pursuant to the provision of paragraph (4) to the Director-General of the Local Finance Bureau or the Director-General of the Local Finance Branch Bureau

(7) The Securities and Exchange Surveillance Commission may, as prescribed by Cabinet Order, delegate a part of the authority delegated pursuant to the provision of paragraph (5) to the Director-General of the Local Finance Bureau or the Director-General of the Local Finance Branch Bureau.

(8) In regards to the affairs related to the authority delegated to the Director-General of the Local Finance Bureau or the Director-General of the Local Finance Branch Bureau, pursuant to the provision of the preceding paragraph, the Securities and Exchange Surveillance Commission directs and supervises the Director-General of the Local Finance Bureau or the Director-General of the Local Finance Branch Bureau.

(9) In the case of paragraph (5), the request for investigation regarding the request for submission of reports or materials (including when the Director-General of the Local Finance Bureau or the Director-General of the Local Finance Branch Bureau carry out pursuant to the provision of paragraph (7)) made by the Securities and Exchange Surveillance Commission may only be performed by the Securities and Exchange Surveillance Commission.

(Requests of the Minister Having Jurisdiction Over the Business)

Article 45 The Minister having jurisdiction over the business may request the Personal Information Protection Commission to take the appropriate measures in compliance with the

provisions of this Act, when the Minister recognizes actions by an business operator handling personal information etc. that violates the provisions of the preceding two Sections, as well as other circumstances when it is recognized that there is a need to secure the appropriate handling of personal information etc. by business operators handling personal information etc.

(The Minister Having Jurisdiction Over the Business)

Article 46 The Minister having jurisdiction over the business under the provisions of this Section is as specified below.

(i) For such handling of personal information etc. by a business operator handling personal information etc. as is related to employment management: the Minister of Health, Labor and Welfare (with handling of personal information as is related to the employment management of mariners, this is the Minister of Land, Infrastructure, Transport and Tourism) and the Minister or the National Public Safety Commission concerned with jurisdiction over the business operator handling personal information etc. (hereinafter referred to as “minister, etc.” in the next item);

(ii) For the handling of personal information etc. by a business operator handling personal information etc. outside of the preceding item: the Minister etc. concerned with jurisdiction over the business of the business operator handling personal information etc..

#### Section 4 Furthering the Protection of Personal Information in the Private Sector

(Accreditation)

Article 47

(1) A corporation (or an association or foundation without legal personality that has made provisions for a representative or manager, the same applies in (b) of item (iii) of the next Article) seeking to perform businesses as set forth in one of the following items with the aim of ensuring that the business operator handling personal information etc., handle that personal information etc. properly may be accredited to do so by the Personal Information Protection Commission:

(i) complaint processing under the provisions of Article 52 for complaints about the handling of personal information etc. by business operator handling personal information etc. which are covered by the corporation’s businesses (hereinafter each such business operator is referred to as a “covered business operator”);

(ii) providing covered business operators with information about matters that contribute to ensuring the proper handling of personal information etc.;

(iii) services beyond what is set forth in the preceding two items which are necessary for ensuring the proper handling of personal information etc. by covered business operators.

(2) A business operator seeking the accreditation referred to in the preceding paragraph must apply to the Personal Information Protection Commission as prescribed by Cabinet Order.

(3) After granting an accreditation as referred to in paragraph (1), the Personal Information Protection Commission must issue public notice indicating this.

(Conditions for Ineligibility)

Article 48 A person falling under one of the following items may not be accredited as referred to in paragraph (1) of the preceding Article:

(i) a business operator that has been sentenced pursuant to any provision of this Act, if two years have not yet passed since the business operator finished serving the sentence or ceased to be subject to its enforcement;

(ii) a business operator whose accreditation has been revoked pursuant to the provisions of Article 58, paragraph (1), if two years have not yet passed since the revocation;

(iii) a business operator with an executive officer (or with the representative or manager, in an association or foundation without legal personality that has made provisions for the representative or manager; hereinafter the same applies in this Article.) that falls under one of the following categories:

(a) a person that has been sentenced to imprisonment or a heavier punishment or that has been sentenced pursuant to any provisions of this Act, if two years have not yet passed since the individual served out the sentence or was exempted from the execution of the sentence;

(b) a person that, during the 30 days before the revocation, was the officer of a corporation whose accreditation has been revoked pursuant to the provisions of Article 58, paragraph (1), if two years have not yet passed since the revocation.

(Accreditation Standards)

Article 49 The Personal Information Protection Commission must not grant an accreditation unless the Commission finds the application for accreditation referred to in Article 47, paragraph (1) to conform to all of the following requirements:

(i) the applicant has established the necessary methods of business implementation to allow it to perform the businesses set forth in the items of Article 47, paragraph (1).

(ii) the applicant's knowledge, capabilities, and financial base are sufficient to allow it to perform businesses set forth properly and reliably in the items of Article 47, paragraph (1);

(iii) if the applicant engages in business other than the businesses set forth in the items of Article 47, paragraph (1), its engagement in that business is unlikely to give rise to unfairness in the businesses set forth in the items of that paragraph.

(Notification of Discontinuation)

Article 50

(1) Before discontinuing the businesses it has been accredited to perform (hereinafter referred to as "accredited businesses"), a business operator accredited as referred to in Article 47, paragraph (1) (hereinafter referred to as an "accredited personal information protection organization") must notify in advance the Personal Information Protection Commission of this as prescribed by Cabinet Order.

(2) Upon receiving notification under the provisions of the preceding paragraph, the Personal Information Protection Commission must issue public notice indicating this.

(Covered Business Operators)

Article 51

(1) Each covered business operator of an accredited personal information protection organization must be a business operator handling personal information etc. that is a member of the accredited personal information protection organization or a business operator handling personal information etc. that has agreed to become a member of the accredited personal information protection organization.

(2) An accredited personal information protection organization must disclose the names of its covered business operators to the public.

(Complaint Processing)

Article 52

(1) If a person or other related person files for an accredited personal information protection organization to resolve a complaint about the handling of personal information etc. by a covered business operator, in addition to complying with any request for a consultation about this, providing the person or other party with the necessary advice, and investigate the circumstances to which the complaint pertains, the organization must notify the covered business operator of the substance and content of the complaint and request that it resolve the complaint expeditiously.

(2) If an accredited personal information protection organization finds that it is necessary in connection with the resolution of a complaint under a filing referred to in the preceding paragraph, the organization may request the covered business operator to provide a written or oral explanation or to submit materials.

(3) If a covered business operator has had a request under the provisions of the preceding paragraph from an accredited personal information protection organization, it must not refuse this request without a legitimate reason for doing so.

(Personal Information Protection Guidelines)

Article 53

(1) In order to ensure the proper handling of personal information etc. by its covered business operators, an accredited personal information protection organization must endeavor to hear the opinion of a person representing the consumer or other related persons and to create guidelines (hereinafter referred to as “personal information protection guidelines”), in keeping with the spirit of this Act, for how to specify the Purpose of Use related to personal information, for measures to ensure secure management of the personal information, for procedures to deal with person’s requests for disclosure and other matters, for how to create de-identified information, for measures to ensure secure management of de-identified information, and for other such particulars.

(2) When an accredited personal information protection organization has created personal information protection guidelines pursuant to the provision of the preceding paragraph, they must notify the Personal Information Protection Commission prescribed by rules of the Personal Information Protection Commission, without delay, of these personal information protection guidelines. The same applies when these guidelines are changed.

(3) When the Personal Information Protection Commission receives a notification of the personal information protection guidelines under the preceding paragraph, the Personal Information Protection Commission must, as prescribed by rules of the Personal Information Protection Commission, disclose the personal information protection guidelines to the public,

(4) After personal information protection guidelines are disclosed pursuant to the provisions of the preceding paragraph, an accredited personal information protection organization must guide, recommend, and take other necessary measures to cause its covered business operators to observe the personal information protection guidelines.

(Prohibition of Use outside the Purposes)

Article 54 It is prohibited for an accredited personal information protection organization to use information acquired in the course of accredited businesses for purposes other than the authorized businesses use for which the information is provided.

(Restriction on Name Use)

Article 55 A business operator that is not an accredited personal information protection organization must not use a name referring to that business operator as an accredited personal information protection organization, and must not use any other name that is confusingly similar to this.

(Collection of Reports)

Article 56 The Personal Information Protection Commission may have an accredited personal information protection organization provide a report on accredited businesses, to the extent that this is necessary for implementing the provisions of this section.

(Orders)

Article 57 The Personal Information Protection Commission may order an accredited personal information protection organization to improve the implementation method for its accredited businesses, to amend its personal information protection guidelines, or to take any other necessary measures, to the extent that is necessary for implementing the provisions of this section.

(Revocation of Accreditation)

Article 58

(1) The Personal Information Protection Commission may revoke the accreditation of an accredited personal information protection organization if:

- (i) it comes to fall under Article 48, item (i) or (iii);
- (ii) it ceases to conform to a requirement referred to in one of the items of Article 49;
- (iii) it violates the provisions of Article 54;
- (iv) it fails to comply with an order as referred to in the preceding Article;
- (v) it was accredited as referred to in Article 47, paragraph (1) by wrongful means.

(2) After revoking an accreditation pursuant to the provisions of the preceding paragraph, the Personal Information Protection Commission must issue public notice indicating this.

## Chapter V Personal Information Protection Commission

### (Establishment)

#### Article 59

(1) A Personal Information Protection Commission (hereinafter referred to as the “Commission”) is established pursuant to the provisions of Article 49, paragraph (3) of the Act for Establishment of the Cabinet Office.

(2) The Commission is administratively attached to the Prime Minister.

### (Duties)

Article 60 The duties of the Commission are to ensure the proper handling of personal information (this includes guiding, advising and taking other measures for Persons in Charge of Affairs Using the Individual Number, etc. (Person in Charge of Affairs Using the Individual Number, etc. prescribed in Article 12 of the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure) (Act No. 27 of 2013; hereinafter referred to as the “Number Use Act”)) in order to protect the rights and interests of individuals while ensuring due consideration that proper and effective use of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched lifestyle for the Japanese citizens among other usefulness of personal information.

### (Jurisdictional Affairs)

Article 61 The Commission, in order to accomplish the duties set forth in preceding Article, is responsible for the following affairs:

(i) matters related to the formulation and promotion of the Basic Policy.

(ii) matters related to supervision of the handling of personal information and de-identified information; carrying out the necessary mediation of the filing regarding complaints and cooperation with business operators processing of the complaints (This excludes matters set forth in item (iv)).

(iii) matters related to accredited personal information protection organizations

(iv) matters related to supervision or monitoring of the handling of Specific Personal Information (Specific Personal Information prescribed in Article 2, paragraph (8) of the Number Use Act; the same applies in Article 63, paragraph (4)); carrying out the necessary mediation of the filing regarding complaints and cooperation with business operators processing of the complaints.

(v) matters related to the Specific Personal Information Protection Assessment (Specific Personal Information Protection Assessment prescribed in Article 27, paragraph (1) of the Number Use Act.)

(vi) matters related to public relations and awareness raising activities about the protection,

and appropriate and effective use of personal information.

(vii) matters related to the necessary investigations and research for implementing the affairs set forth in the preceding items.

(viii) matters related to international cooperation pertaining to jurisdictional affairs.

(ix) in addition to those set forth in the preceding items, matters that are assigned to the Commission pursuant to the provisions of laws (this includes orders based on laws).

(Independence of Exercising Authority)

Article 62 The chairperson and members of the Commission exercise their authorities independently.

(Organization etc.)

Article 63

(1) The Commission is composed of the chairperson and eight Commission members.

(2) Four of the Commission members are part-time members.

(3) The chairperson and members of the Commission are appointed from among the people of good character and sound knowledge, with the consent of both Houses of the Diet, by the Prime Minister.

(4) The chairperson and members of the Commission include a person who has knowledge and experience in the protection of, and appropriate and effective use of personal information, a person who has knowledge and experience in the protection of consumers, a person who has knowledge and experience in information processing technology, a person who has knowledge and experience in administrative fields used in specific personal information, a person who has sufficient knowledge and experience in matters related to the practice of private enterprises, and a person recommended by a federation, ( meaning a federation under Article 263-3, paragraph (1) of the Local Autonomy Act (Act No. 67 of 1947) that has made notification under the provisions of said paragraph).

(Term of office, etc.)

Article 64

(1) The term of office of the chairperson and members of the Commission is five years; provided, however, that the term of office of the chairperson or a member chosen filling a vacancy is the remaining term of office of the predecessor.

(2) The chairperson and members of the Commission may be reappointed.

(3) When the term of office of the chairperson or a member of the Commission expires, said chairperson or member continues to perform their duties until their successor is appointed.

(4) When the term of office of a chairperson or a member of the Commission expires, if the Prime Minister is unable to obtain the consent of both Houses because the Diet is not in session or the House of Representatives has been dissolved, notwithstanding the provisions of paragraph (3) of the preceding Article, the Prime Minister may appoint a chairperson or a

member of the Commission from among those people who have the qualifications prescribed in said paragraph.

(5) In the case of the preceding paragraph, the later approval of both Houses of the Diet must be obtained at the first Diet after the appointment. In this case, if the later approval of both Houses of the Diet cannot be obtained, the Prime Minister must, immediately, dismiss the chairperson or member of the Commission.

(Guarantee of Status)

Article 65 The chairperson and members of the Commission, except if they fall under any of the following items, are not dismissed against their will while holding office:

(i) they receive an order to commence bankruptcy proceedings;

(ii) they are punished for violation of this Act or Number Use Act;

(iii) they are punished by imprisonment without required labor or a heavier punishment; or

(iv) the Commission finds that the chairperson or a member of the Commission is incapable of executing his/her duties due to a mental or physical disorder, or , has contravened the duties of his/her position or has committed misconducts inappropriate for a chairperson or a member of the Commission.

(Dismissal)

Article 66 The Prime Minister, if the chairperson or a member of the Commission falls under one of the items of the preceding Article, must dismiss said chairperson or member of the Commission.

(Chairperson of the Commission)

Article 67

(1) The chairperson of the Commission presides over the business of the Commission and represents the Commission.

(2) The Commission must in advance and from among the full-time members of the Commission, designate a person to substitute the chairperson in case the chairperson is prevented from attending to duties.

(Meetings)

Article 68

(1) The meetings of the Commission are called by the chairperson of the Commission.

(2) The Commission may not, unless four or more members of the Commission are present, hold a meeting nor make any decision.

(3) Any matter before the Commission is decided by a majority of members present and in case of a tie, by the chairperson.

(4) Findings pursuant to the provision of Article 65, item (iv), notwithstanding the

provisions of the preceding paragraph, must be made by the unanimous consent of all members present except the member concerned.

(5) With regard to application of the provisions of paragraph (2) of this Article if the chairperson is prevented from attending to duties, the person who substitutes the chairperson as set forth in paragraph (2) of the preceding Article is deemed to be the chairperson.

(Expert Advisors)

#### Article 69

(1) Expert advisors may be appointed on the Commission to conduct investigations of specialized matters.

(2) Expert advisors are appointed by the Prime Minister based on a request made by the Commission.

(3) Expert advisors are relieved from their position when their investigation regarding the specialized matter is complete.

(4) Expert advisors are on a part-time basis.

(Secretariat)

#### Article 70

(1) In order to handle the affairs of the Commission, a secretariat is established for the Commission.

(2) The secretariat consists of the secretary-general and other officials.

(3) The secretary-general, under the direction of the chairperson of the Commission, administers the affairs of the secretariat.

(Prohibition of Political Campaigning etc.)

#### Article 71

(1) The chairperson and members of the Commission, while holding office, must not become an officer of political parties and other political organizations, or actively carry out a political campaign.

(2) The chairperson and full-time members of the Commission, while holding office, must not engage in other jobs with remuneration, run business for profit or operate other businesses seeking monetary profit unless they are authorized by the Prime Minister.

(Confidentiality)

Article 72 The chairperson, members of the Commission, Expert Advisors and officials of the secretariat must not leak or steal any secret that may have come to their knowledge in the course of their duties. The same applies after they retire from their duties.

(Remuneration)

Article 73 The remuneration of the chairperson and members of the Commission is specified separately by law.

(Establishment of Rules)

Article 74 The Commission may establish Rules on Personal Information Protection Commission in order to enforce laws or Cabinet Orders with regard to the affairs under its jurisdiction or based on a special delegation by law or Cabinet Orders.

## Chapter VI Miscellaneous Provisions

(Scope of Applicability)

Article 75 The provisions of Article 15, Article 16, Article 18 (This excludes paragraph (2).), Articles 19 through 25, Articles 27 through 36, Article 41, Article 42, paragraph (1), Article 43, and Article 76 also applies when a business operator handling personal information acquires personal information of an individual in Japan regarding the provisions of goods or service, and that personal information or the de-identified information created using that personal information is handled outside of Japan.

(Exclusion from Application)

Article 76

(1) The provisions of Chapter IV do not apply to a business operator handling personal information etc. which is set forth in one of the following items if all or part of the purpose for which it handles that personal information is the purpose prescribed in each item:

(i) broadcasting organizations, newspapers, news services, and other journalistic organizations (this includes individuals who work in news reporting): use in news reporting;

(ii) a business operator in the business of creating literary works: use in the creation of literary works;

(iii) a college, university, or other academic or research-oriented institution or organization, or any business operator belonging to the same: use in academics or research;

(iv) a religious organizations: use in a religious activity (this includes activities incidental thereto);

(v) a political organization: use in a political activity (this includes activities incidental thereto).

(2) The “News reporting” prescribed in item (i) of the preceding paragraph means informing the general public objective facts by presenting them as the truth (this includes stating an opinion or position based on such facts).

(3) A business operator handling personal information etc. as set forth in one of the terms of paragraph (1) must, itself, endeavor to take the necessary and appropriate measures for securely managing personal data or de-identified information, to carry out processing of complaints about the handling of personal information etc., and to take other necessary measures for ensuring the proper handling of personal information etc., and must also endeavor to disclose the content of those measures to the public.

(Affairs Handled by Local Governments)

Article 77 It may be decided, as prescribed by Cabinet Order, that the affairs that this Act prescribes as being part of the authority of the Commission or Article 44, paragraph (1) or (4) prescribes as being part of an authority of a Minister having jurisdiction over the business or the Commissioner of the Financial Services Agency may be handled by the heads of local governments or by other executive agencies.

(Provision of Information to Foreign Authorities)

Article 78

(1) The Commission may provide information, which they deem to be helpful to the duties (this limits to the duties corresponding to the duties of the Commission prescribed in this Act; the same applies in the subsequent paragraph) of foreign authorities (hereinafter referred to as “Foreign Authorities” in this Article) executing foreign laws and regulations equivalent to the Act.

(2) When disseminating information under the preceding paragraph, appropriate measures must be taken so that said information is not used for purposes other than for performing the duties of Foreign Authorities, and is not used for the investigation into criminal cases (this limits when the fact of a crime has already been specified) or inquiries (hereinafter collectively referred to as “investigations etc.”) in foreign countries without the consent under the following paragraph.

(3) The Commission may, having received a request from a Foreign Authority, give consent for the information which it has provided pursuant to the provision of paragraph (1) to be used for the investigation into criminal cases pertaining to said request, except for cases falling under one of the following items:

(i) When a crime subject to the investigation into criminal cases pertaining to said request is a political crime, or when it is found that said request has been made for the purpose of conducting an investigation into a political crime;

(ii) When the action that is subject to the criminal offense investigation etc. related to the request was committed in Japan, and this action does not constitute a criminal offense according to the laws of Japan;

(iii) When the requesting country has not ensured that it will accept a similar request from Japan;

(4) The Commission must, before giving the consent set forth in the preceding paragraph, obtain confirmation from the Minister of Justice that the request does not fall under items (i) and (ii) of the preceding paragraph, and the confirmation from the Minister of Foreign Affairs for the request that does not fall under item (iii) of the preceding paragraph.

(Reporting to the Diet)

Article 79 The Commission must, through the Prime Minister, annually report the progress of its jurisdictional affairs to the Diet and must also make public its outline.

(Communication and Cooperation)

Article 80 The Prime Minister and heads of the administrative organs (meaning the organs established in the Cabinet pursuant to law (other than the Cabinet Office), organs under the supervision of the Cabinet, the Cabinet Office, the Imperial Household Agency, the institutions prescribed in Article 49, paragraphs (1) and (2) of the Act for Establishment of the Cabinet Office, and the institutions prescribed in Article 3, paragraph (2) of the National Government Organization Act (Act No. 120 of 1948)) involved in putting this Act into effect must be in close communication and cooperate with one another.

(Delegation to Cabinet Order)

Article 81 Beyond what is prescribed in this Act, particulars that need to be provided for in order for this Act to be implemented are prescribed by Cabinet Order.

#### Chapter VII Penal Provisions

Article 82 A person who leaks or steals secrets violating the provisions of Article 72 is subject to imprisonment with required labor for not more than two years or to a fine of not more than 1,000,000 yen.

Article 83 A business operator handling personal information (this includes executives, representatives or managers when the business operator is a corporation (or of an association or foundation without legal personality that has made provisions for a representative or manager; hereinafter the same applies in Article 87, paragraph (1)), its employees or former employees who provides the handled personal information database etc. (this includes copies or processed versions all or part), handled regarding their duties, for wrongful gain for either themselves or a third party, or steals such, is subject to imprisonment with required labor for not more than one year or to a fine of not more than 500,000 yen.

Article 84 A business operator violating an order under Article 42, paragraphs (2) or (3) is subject to imprisonment with required labor for not more than six months or to a fine of not more than 300,000 yen.

Article 85 A business operator falling under one of the following items is subject to a fine of not more than 300,000 yen.

(i) a business operator failing to report or to submit documentations under Article 40, paragraph (1), or making a false report, or submitting falsified documentations, or failing to answer the questions of the investigating officer or gives false testimony for such, or refusing, abstracting or avoiding the investigation;

(ii) A business operator failing to report under Article 56, or making a false report.

Article 86 The provisions of Articles 82 and 83 applies to any person or business operator outside of Japan who commits the criminal offenses of this Articles.

#### Article 87

(1) If the representative of a corporation, or the agent, employee or other workers of a corporation or individual commits a violation referred to in Articles 83 through 85 in connection with the business of the corporation or individual, in addition to the offender being subject to punishment, the corporation or individual is subject to the fine prescribed in the relevant Article.

(2) When the provisions of the preceding paragraph apply to an association or foundation

without legal personality, the representative or manager of the association or foundation represents it in respect of procedural actions, and the provisions of law on criminal proceedings that have a corporation as the defendant or suspect apply *mutatis mutandis*.

Article 88 A business operator falling under one of the following items is subject to a non-criminal fine of not more than 100,000 yen:

- (i) A business operator violating the provisions of Article 26, paragraph (2), or Article 55;
- (ii) A business operator failing to make a notification under Article 50, paragraph (1), or making a false notification.