COMMENTARY FOR GUIDELINES FOR PROTECTION OF PERSONAL INFORMATION IN TELECOMMUNICATIONS BUSINESS
(MIC Notice No. 152 of 2017; Last Amendment: MIC Notice No. 297 of 2017)

September 2017 (Updated in February 2021)

Ministry of Internal Affairs and Communications

COMMENTARY FOR GUIDELINES FOR PROTECTION OF PERSONAL INFORMATION IN TELECOMMUNICATIONS BUSINESS

Table of Contents

Explanatory Notes:

"Act":	Act on the Protection of Personal Information (Act No. 57 of 2003)
"Cabinet Order":	Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003)
"Rules":	Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3 of 2016)

* Unless otherwise noted, the laws and regulations, etc., cited in this Commentary for Guidelines shall be those in force as of January 1, 2021.

1 Purpose and Applicability

1-1 Purpose

Article 1

The purpose of these Guidelines is to enhance the smooth provision of telecommunications services and to protect the rights and interests of users by setting forth basic matters which telecommunications carriers must comply with in relation to matters pertaining to the secrecy of communications and other appropriate handling of personal information in light of the public nature of telecommunications business and the significantly expanded utilization of personal information as our advanced information- and communication-based society evolves.

Telecommunications business is directly associated with the secrecy of communications and is of an extremely important public nature, and it is also anticipated that information which is in need of privacy protection is handled in such business. Accordingly, personal information handled in such business is in great need of protection. Furthermore, as a result of sophistication and diversification of telecommunications services, an advanced information and communications society has been realized, enabling speedy and broad distribution and utilization of a wealth of highly processed information, and as a result, providing a great deal of convenience to people's lives. On the other hand, if any personal information acquired in connection with the provision of such telecommunications services is handled inappropriately or any personal information is handled inappropriately by using such telecommunications services, individuals may suffer irreparable damage.

In light of the above, the Guidelines are intended to provide specific guidelines under Articles 6 and 8 of the Act and the relevant provisions of the Telecommunications Business Act (Act No. 86 of 1984) for the purpose of enhancing the convenience of telecommunications services by securing unrestricted distribution within the prescribed scope and protecting the rights and interests of users, by presenting to telecommunications carriers as specific guidelines as possible with regard to matters attributable to the secrecy of communications and other matters relating to appropriate handling of personal information in light of the Act and the "*Basic Policy on the Protection of Personal Information*" (Cabinet Decision of April 2004; partially amended in June 2018) under the provisions of Article 7, paragraph (1) of the Act, Article 4 of the Telecommunications Business Act and other relevant provisions and from the perspective of privacy protection.

In the Guidelines, where the phrases "must" and "shall not" are used with respect to a certain matter, it means that the failure to comply with such matter may be found as a violation of the Act or the Telecommunications Business Act.

On the other hand, where the phrases such as “it is appropriate”, “must strive”, and “it is desirable” are used with respect to a certain matter, it means that the failure to comply with such matter may not be immediately found as a violation of the Act or the Telecommunications Business Act, but telecommunications carriers are expected to strive to comply with such matter to the extent possible in line with the characteristics or scale of respective telecommunications carriers, in light of the overall vision of the Act (“Personal information, considering it should be carefully handled under the vision of respecting the personality of an individual, shall be made subject to the proper handling.”) (Article 3 of the Act) and the purposes of the Telecommunications Business Act (Article 1 of said Act). However, it is not intended to restrict activities necessary for the public interest and legitimate business activities in light of the purport expressed in the purpose of the Act (Article 1 of the Act) and the purpose of the Telecommunications Business Act (Article 1 of said Act).

Specific examples illustrated in these Guidelines are intended to be typical cases for the purpose of helping telecommunications carriers’ understanding, and such examples are not intended to be comprehensive or to restrict the cases to those illustrated herein. Furthermore, it should be noted that even a specific example given herein could have an element requiring separate consideration on a case-by-case basis.

Additionally, there may be cases where an accredited personal information protection organization (*) prepares or amends a personal information protection policy or where a trade association, etc., prepares or amends self-regulatory rules (such as the trade association guidelines) targeting member companies of such trade association, etc., and in such cases, the covered business operators of such accredited personal information protection organization and the member companies of such trade association, etc., are required to take measures for the handling of personal information in line with such policy or rules in addition to the Act and these Guidelines. In particular, importantly, an accredited personal information protection organization should keep in mind that, due to amendment to the Act, such organization must take necessary measures to ensure that the covered business operators comply with its personal information protection guidelines (see Article 53, paragraph (4) of the Act).

(*) Under the accredited personal information protection organization system, the Personal Information Protection Commission accredits a private sector body which conducts activities of processing complaints against covered business operators and providing information to covered business operators, for the purpose of appropriate handling of personal information and information by business operators handling personal

information or anonymously processed information, and the system is intended to ensure the reliability of such activities and promote the protection of personal information through private sector bodies.

(For Reference)

Article 1 of the Act

This Act aims to protect an individual's rights and interests while considering the utility of personal information including that the proper and effective application 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; by setting forth the overall vision for the proper handling of personal information, creating a governmental basic policy with regard to this, and establishing other matters to serve as a basis for measures to protect personal information, as well as by clarifying the responsibilities etc. of the central and local governments and establishing obligations etc. that a personal information handling business operator shall fulfill, in light of the significantly expanded utilization of personal information as our advanced information- and communication-based society evolves.

Article 3 of the Act

Personal information, considering it should be carefully handled under the vision of respecting the personality of an individual, shall be made subject to proper handling.

Article 6 of the Act

The government shall, considering the nature and utilization method of personal information, take necessary legislative and other action so as to be able to take discreet action for protecting personal information that especially requires ensuring the strict implementation of its proper handling in order to seek enhanced protection of an individual's rights and interests, and shall take necessary action in collaboration with the governments in other countries to construct an internationally conformable system concerning personal information through fostering cooperation with an international organization and other international framework.

Article 8 of the Act

The central government shall provide information, develop guidelines to ensure the proper and effective implementation of action to be taken by a business operator etc., and take other necessary action in order to support measures for the protection of personal information developed or implemented by a local government and activities undertaken by a Japanese citizen, or a business operator etc. in relation to seeking the proper handling of personal

information.

Article 47 of the Act

(1) A corporation (including a non-corporate body which has appointed a representative or administrator; the same shall apply in the succeeding Article, item (iii), (b)) which intends to render the following services in order to ensure the proper handling of personal information etc. by a personal information handling business operator etc. may receive an accreditation from the Personal Information Protection Commission.

(i) dealing with a complaint under the provisions of Article 52 about the handling of personal information etc. by a personal information handling business operator covered by the services (hereinafter referred to as a "covered business operator")

(ii) providing a covered business operator with information concerning a matter contributory to ensuring the proper handling of personal information etc.

(iii) besides those set forth in the preceding two items, rendering necessary services related to ensuring the proper handling of personal information etc. by a covered business operator

(2) A person who intends to receive an accreditation under the preceding paragraph shall, as prescribed by cabinet order, apply to the Personal Information Protection Commission.

(3) The Personal Information Protection Commission shall, when having granted an accreditation under the paragraph (1), announce to the public to that effect.

Article 53 of the Act (paragraph (4))

(4) An accredited personal information protection organization shall, when a personal information protection guideline has been announced to the public pursuant to the provisions of the preceding paragraph, take action against a covered business operator such as providing guidance or recommendation necessary to make the covered business operator follow the said personal information protection guideline.

1-2 Applicability (in Relation to Article 2, Paragraph 1)

Article 2 (Paragraph 1)

1. The provisions in these Guidelines shall be interpreted and operated as those setting forth basic matters which telecommunications carriers must comply with in appropriately handling personal information.

These Guidelines apply to telecommunications carriers that fall under the category of

personal information handling business operators and anonymously processed information handling business operators to whom the Act applies (hereinafter referred to as "Personal Information Handling Business Operators, etc."), regardless of the type, scale, etc., of such telecommunications carriers.

Additionally, as set forth in Article 3, Item (1), the term "telecommunications carriers" in the Guideline refers to those who conduct a telecommunications business set forth in Article 2, item (iv) of the Telecommunications Business Act. Furthermore, because the Telecommunications Business Act applies where a foreign corporation, etc. (meaning a corporation or organization based abroad, or an individual with an address abroad; the same shall apply hereinafter) conducts a telecommunications business to provide telecommunications services from overseas for parties located in Japan, in addition to where a foreign corporation, etc. conducts a telecommunications business to provide telecommunications services in Japan, the Guidelines are deemed to be applicable to such foreign corporation, etc.

1-3 Application (in Relation to Article 2, Paragraphs 2 and 3)

Article 2 (Paragraphs 2 and 3) 2. Telecommunications carriers must comply with the provisions of the Act on the Protection of Personal Information (hereinafter referred to as the "Act") and Article 4 and other relevant provisions of the Telecommunications Business Act (Act No. 86 of 1984) and otherwise handle personal information appropriately in accordance with the provisions of these Guidelines. 3. With regard to various types of information specified in Chapter III, telecommunications carriers must comply with the common principles concerning the handling of personal information specified in Chapter II and otherwise handle the same appropriately in accordance with the provisions of Chapter III.

The Guidelines clarify the criteria for the applicability of the Act on telecommunications carriers and also clarify basic matters which telecommunications carriers, which are particularly required to ensure the strict implementation of proper handling of personal information, are required to comply with in light of Article 4 of the Telecommunications Business Act relating to the secrecy of communications and other relevant provisions. Furthermore, while the Guidelines are based on the provisions of the "*Guidelines for the Act on the Protection of Personal Information*" (of November 30, 2016 by the Personal Information Protection Commission), the Guidelines present, in an integrated fashion, rules applicable to telecommunications carriers, together with the provisions that are required in view of the secrecy of communications and other

circumstances unique to telecommunications carriers. Accordingly, this means that, if a telecommunications carrier complies with the provisions of these Guidelines, such telecommunications carrier complies with the Act and the Guidelines for the Act on the Protection of Personal Information in respect of telecommunications business.

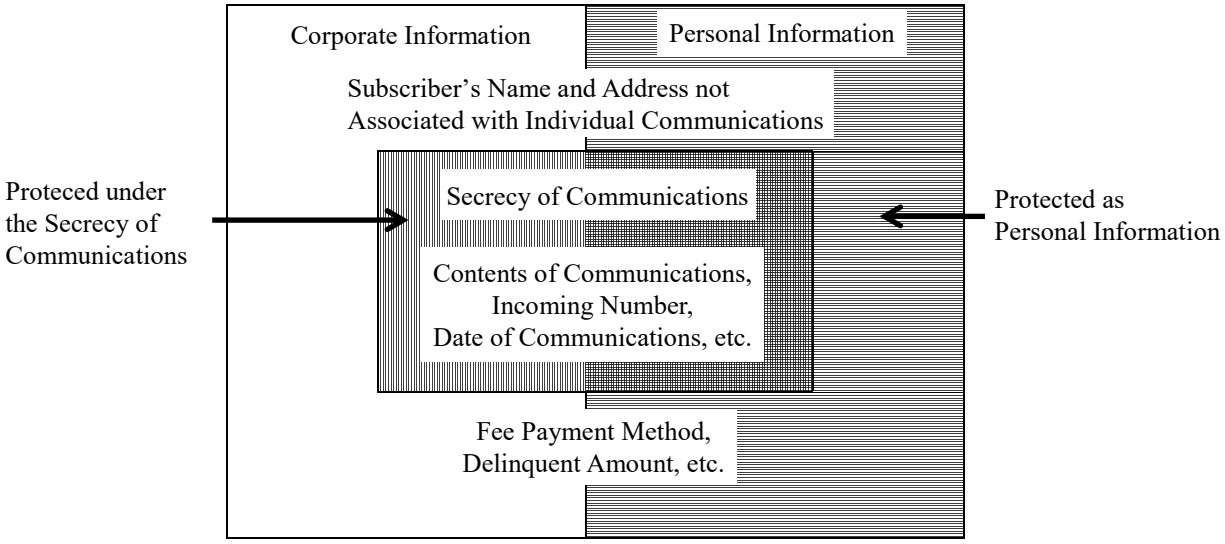
Incidentally, for the handling of personal data which will be transferred from the EU and the United Kingdom area based on an adequacy decision (which for the EU means a decision that the EU Commission makes, pursuant to Article 45 of the GDPR (*), to recognize that a certain country or region, etc., ensures an adequate level of protection of personal data and for the United Kingdom means a decision that is equivalent to this), please see the "*Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU and the United Kingdom based on an Adequacy Decision*" (Personal Information Protection Commission Public Notice No. 4 of 2018) prescribed by the Personal Information Protection Commission.

On the other hand, under Article 4 of the Telecommunications Business Act relating to the secrecy of communications and other relevant provisions, matters covered by the secrecy of communications are protected, regardless of whether information pertains to individuals or to corporations or other entities, and accordingly, the matters concerning corporations and other entities are also protected (see the chart below), and the target and rules in respect of the secrecy of communications may be broader than the scope of the Guidelines.

Additionally, the provisions in Chapter III (Articles 32 through 38) are special provisions supplementary to the provisions of Chapter II (Articles 4 through 31), and any matter not specifically provided with regard to various types of information specified in Chapter III (Articles 32 through 38) shall be governed by the provisions in Chapter II (Articles 4 through 31).

(*) REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

● Relationship between Personal Information and Secrecy of Communications



2 Definitions

2-1 Telecommunications Carrier, etc. (in Relation to Article 3)

Article 3

The terms used in these Guidelines shall have the same meanings as the terms used in Article 2 of the Act, and additionally, the terms in the items below shall have the meanings set forth in the respective items below.

(1) "Telecommunications carrier" means a person who conducts telecommunications business (as defined in Article 2, Item (4) of the Telecommunications Business Act).

(2) "Telecommunications services" means telecommunications services as defined in Article 2, Item (3) of the Telecommunications Business Act.

(3) "Telecommunications services and incidental services" means telecommunications services provided by a telecommunications carrier as a business as well as services incidental thereto.

(4) "User" means a person who uses telecommunications services.

(5) "Subscriber" means a person who executes a contract with a telecommunications carrier to receive the provision of telecommunications services.

In order to cover a broad range of personal information handled by parties which conduct a telecommunications business, the terms used in the Guidelines do not necessarily have the same meanings as those of the terms in the Telecommunications Business Act.

"Telecommunications carrier": Under the Telecommunications Business Act, the term refers to the person that has completed administrative procedures of registration and notification to operate a telecommunications business; however, because it is unreasonable to exclude those who operate such business by reason of the failure to complete such mandatory procedures, the Guidelines are applicable to those who conduct a telecommunications business under the Telecommunications Business Act, regardless of whether such procedures have been completed. Additionally, the Guidelines are also applicable to those who conduct a business set forth in the respective items of Article 164, paragraph (1) of said Act, and who are not covered by the Telecommunications Business Act, given that the provisions of Article 4 (Protection of Secrecy) of said Act are applicable to such persons, and such persons also need to protect the personal information. Furthermore, the Guidelines are also applicable to those who conduct a telecommunications business for non-profit purposes because they are also required to handle personal information in an appropriate manner. Additionally, because the provisions of the Telecommunications Business Act apply regardless of the scale of business, telecommunications carriers of all different scales are expected to take the same measures under the Guidelines.

"Telecommunications services": The term is defined as intermediating other persons' communications through the use of telecommunications facilities, or other acts of providing telecommunications facilities for use in other persons' communications (Article 2, paragraph (3) of the Telecommunications Business Act).

"Telecommunications services and incidental services": The term refers telecommunications services provided by a telecommunications carrier in order to meet the demands of other persons and includes services incidental thereto. Services which are deemed incidental to telecommunications services are: services which are provided as part of telecommunications services and are not inseparable from such services (such as filtering on the network, lease of router and other network devices, and system development and maintenance) and services based on the use of telecommunications services provided by a telecommunications carrier (such as a device location search, security, payment settlement, device sale and warranty, distribution of application software, videos and music, electronic money award service, and telephone directory operations).

In addition to the above, where a certain service is provided under the same ID, etc., linked with personal information associated with the telecommunications service provided by a telecommunications carrier, then such service will fall under the category of telecommunications services.

"User": Under the Telecommunications Business Act, the term refers to a person who executes a contract with a telecommunications carrier to receive telecommunications services. However, as in the case of a subscribed telephone, because persons other than the contracting person may use telecommunications services, the Guidelines cover whoever uses telecommunications services in order to protect such person's personal information.

"Subscriber": The term refers to a person who falls under the category of "user" under the Telecommunications Business Act.

(Note) The Guidelines are applicable to personal information related to telecommunications services provided by telecommunications carriers (*). However, especially where such personal information is used for any other business, if personal data related to telecommunications services are linked with personal data related to the other business under the same ID, etc., and managed in the same database, then it is appropriate to handle such data under appropriate security controls in light of the purport of the Guidelines.

(*) This includes cases separately prescribed in the Guidelines as cases requiring special attention with respect to the handling of personal information in relation to the operations closely associated with the provision of telecommunication services.

2-2 Personal Information

"Personal Information" (*1) means "information relating to a living individual," (*2) (*3) which refers to those containing a name, date of birth, or other descriptions, etc. (meaning any and all matters whereby a specific individual can be identified (including those which can be readily collated with other information (*4) and thereby identify a specific individual) (Article 2, paragraph (1), item (i) of the Act) or those containing an individual identification code (*5) (item (ii) of said paragraph).

The Guidelines do not apply to information relating to the deceased except for information relating to both the deceased and a living individual; however, telecommunications carriers are required to handle information relating to the deceased in an appropriate manner as with information relating to a living individual, and it is desirable to handle information relating to the deceased in an appropriate manner by taking security control measures and other measures set forth in the Guidelines basically in the same manner as with information relating to living individuals.

Incidentally, under the Telecommunications Business Act, the secrecy of communications is protected even after the death of a communicating person.

"Information relating to an individual" is not limited such individual's name, address, gender, birthdate, facial image, or such other information that identifies such individual, and extends to all information that indicates facts, assessments and evaluations relating to such individual's body, assets, occupation, title and other attributes, and includes evaluation information, information made public by way of publications, etc., or visual and audio information, regardless of whether the foregoing is concealed by encryption, etc.

<Examples of Personal Information>

Case 1) A principal's name

Case 2) Information that combines a principal's name with his/her birthdate, contact information (address, domicile, telephone number, and/or email address), and/or information regarding his/her title or position in a company

Case 3) Visual data by which a principal may be recognized, such as data recorded in a security camera

Case 4) Audio recording data by which a specific individual may be identified because of the inclusion of the principal's name or for such other reason

Case 5) Email address by which a specific individual may be identified (for instance, in the case of an email address such as kojin_ichiro@example.com because it would suggest that it is an email address of one Kojin Ichiro who belongs to a company named Example)

Case 6) Information concerning to an individual which is added to certain personal information after the acquisition thereof (Even if a specific living individual cannot be identified when certain information is acquired, if after such acquisition, such specific living individual can be identified with additional information or as a result of collation, then such information will become personal information at that point in time.)

Case 7) Information which is publicly available by way of a means such as an Official Gazette, telephone directory, employee directory, statutory disclosure document (such as an annual securities report), newspaper, web page, and SNS (social network service), and with which a specific individual may be identified

(*1) It must be kept in mind that, under the Act, the terms such as "personal information", "personal data" (see 2-7 (Personal Data)), "retained personal data" (see 2-8 (Retained Personal Data)), "special care-required personal information" (see 2-4 (Special Care-Required Personal Information)), and "anonymously processed information" (see 2-9 (Anonymously Processed Information)) have distinctive meanings, and the duties imposed on Personal Information Handling Business Operators, etc. are different for the respective types of information.

(*2) If information concerning the deceased also relates to any living individual such as a surviving family member, then such information is treated as information concerning such surviving individual.

(*3) Because a legal entity or such other organization is not an "individual", information concerning a legal entity or such other organization itself is not treated as "personal information" (provided that information concerning its officers, employees, etc. is treated as personal information). Additionally, "individuals" are not limited to Japanese nationals and include foreigners.

(*4) Where certain information "can be readily collated with other information", it means that such information can be easily collated with other information in a general manner in the course of ordinary business although a determination should be made on a case-by-case basis in light of actual circumstances of a telecommunications carrier. For example, if such collation is difficult because it requires an inquiry to another business operator, for instance, then it can be generally recognized that information cannot be readily collated.

(*5) With respect to the individual identification code, see 2-3 (Individual Identification Code).

（For Reference）

Article 2 of the Act (paragraph (1)) (1) “Personal information” in this Act means that information relating to a living individual which falls under any of each following item: (i) those containing a name, date of birth, or other descriptions etc. (meaning any and all matters (excluding an individual identification code) stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record (meaning a record kept in an electromagnetic form (meaning an electronic, magnetic or other forms that cannot be recognized through the human senses; the same shall apply in the succeeding paragraph, item (ii)); the same shall apply in Article 18, paragraph (2)); hereinafter the same) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual) (ii) those containing an individual identification code

2-3 Individual Identification Code (in Relation to Article 2, paragraph (2) of the Act)

An “individual identification code” means any character, letter, number, symbol or other code prescribed by the Cabinet Order as those by which a specific individual may be identified, and any information containing the same is treated as personal information (see 2-2 (Personal Information)) (*).

Specifics of the individual identification code are as set forth in Article 1 of the Cabinet Order and Articles 2 through 4 of the Rules.

Article 1, item (i) of the Cabinet Order sets forth that an “individual identification code” means any character, letter, number, symbol or other code produced by having converted any of the following bodily features thereinto so as to be provided for use in computers “which conform to standards prescribed by rules of the Personal Information Protection Commission as sufficient to identify a specific individual”. Such standards are set forth in Article 2 of the Rules, and those that conform to such standards and are thus treated as individual identification codes are as described below.

a. Base sequence constituting deoxyribonucleic acid (DNA) taken from a cell:
genome data (i.e., codes showing a base sequence constituting deoxyribonucleic acid (DNA) taken from a cell) that makes it possible to identify an individual based on genotype data, such as whole nuclear genome sequencing data, whole exome sequencing data, whole-genome single-nucleotide polymorphism (SNP) data, sequencing data

comprised of 40 or more mutually independent SNPs, short tandem repeat (STR) with four bases repeated at nine or more loci, etc.

b. Appearance decided by facial bone structure and skin color as well as the position and shape of eyes, nose, mouth or other facial elements:
feature information which is extracted from facial bone structure and skin color as well as the position and shape of eyes, nose, mouth or other facial elements and which is made capable of identifying an individual when used by a device or software aimed at recognizing an individual.

c. A linear pattern formed by an iris' surface undulation:
feature information which is extracted from a linear pattern formed by an iris' surface undulation and which is made capable of identifying an individual when used by a device or software aimed at recognizing an individual.

d. Vocal cords' vibration, glottis' closing motion as well as the shape of vocal tract and its change when uttering:
feature information relating to vocal cords' vibration, glottis' closing motion as well as the shape of vocal tract and its change when uttering, which is extracted from voice and which is made capable of identifying an individual when used by a device or software aimed at recognizing an individual.

e. Bodily posture and both arms' movements, step size and other physical appearance when walking:
feature information which is extracted from bodily posture and both arms' movements, step size and other physical appearance when walking and which is made capable of identifying an individual when used by a device or software aimed at recognizing an individual.

f. Intravenous shape decided by the junctions and endpoints of veins lying under the skin of the inner or outer surface of hands or fingers:
feature information which is extracted, by using infrared light, visible light, etc., from the intravenous shape, etc. decided by the junctions and endpoints of veins lying under the skin of the inner or outer surface of hands or fingers and which is made capable of identifying an individual when used by a device or software aimed at recognizing an individual.

g. A finger or palm print:
(finger print) feature information which is extracted from a finger print formed by ridges, etc. on the surface of a finger and which is made capable of identifying an individual when used by a device or software aimed at recognizing an individual.
(palm print) feature information which is extracted from a palm print formed by ridges, wrinkles, etc. on the surface of a palm and which is made capable of identifying an individual when used by a device or software aimed at recognizing an individual.

h. Combination:
a combination of feature information which is extracted from those listed in b. through g. in Article 1, item (i) of the Cabinet Order and which is made capable of identifying an individual when used by a device or software aimed at recognizing an individual.

(*) The phrase "to identify a specific user or purchaser, or recipient of issuance" (Article 2, paragraph (2), item (ii) of the Act) means making any character, letter, number, symbol or other codes differently assigned or, stated or recoded for the said user, etc.

(For Reference)

Article 2 of the Act (paragraph (2))
(2) An "individual identification code" in this Act means those prescribed by cabinet order which are any character, letter, number, symbol or other codes falling under any of each following item.
(i) those able to identify a specific individual that are a character, letter, number, symbol or other codes into which a bodily partial feature of the specific individual has been converted in order to be provided for use by computers
(ii) those character, letter, number, symbol or other codes which are assigned in regard to the use of services provided to an individual or to the purchase of goods sold to an individual, or which are stated or electromagnetically recorded in a card or other document issued to an individual so as to be able to identify a specific user or purchaser, or recipient of issuance by having made the said codes differently assigned or, stated or recoded for the said user or purchaser, or recipient of issuance

Article 1 of the Cabinet Order
Those character, letter, number, symbol or other codes prescribed by cabinet order under

Article 2, paragraph (2) of the Act on the Protection of Personal Information (hereinafter referred to as the "Act") shall be those set forth in the following.

(i) Those character, letter, number, symbol or other codes produced by having converted any of the following bodily features thereinto so as to be provided for use in computers which conform to standards prescribed by rules of the Personal Information Protection Commission as sufficient to identify a specific individual.

(a) base sequence constituting Deoxyribonucleic Acid (alias DNA) taken from a cell;

(b) appearance decided by facial bone structure and skin color as well as the position and shape of eyes, nose, mouth or other facial elements;

(c) a linear pattern formed by an iris' surface undulation;

(d) vocal cords' vibration, glottis' closing motion as well as the shape of vocal tract and its change when uttering;

(e) bodily posture and both arms' movements, step size and other physical appearance when walking;

(f) Intravenous shape decided by the junctions and endpoints of veins lying under the skin of the inner or outer surface of hands or fingers;

(g) a finger or palm print.

(ii) Number of passport set forth in Article 6, paragraph (1), item (i) of the Passport Act (Act No. 267 of 1951)

(iii) Basic pension number set forth in Article 14 of the National Pension Act (Act No. 141 of 1959)

(iv) Number of a driver's license set forth in Article 93, paragraph (1), item (i) of the Road Traffic Act (Act No. 105 of 1960)

(v) Resident record code set forth in Article 7, item (xiii) of the Basic Resident Registration Act (Act No. 81 of 1967)

(vi) Individual number set forth in Article 2, paragraph (5) of the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013)

(vii) Those character, letter, number, symbol or other codes prescribed by rules of the Personal Information Protection Commission which are stated on a certificate set forth in the following in a way to give each person who receives its issuance a different one.

(a) A health insurance card under Article 9, paragraph (2) of the National Health Insurance Act (Act No. 192 of 1958);

(b) An insured person's certificate under Article 54, paragraph (3) of the Act on Assurance of Medical Care for Elderly People (Act No. 80 of 1982)

(c) An insured person's certificate under Article 12, paragraph (3) of the Long-Term Care Insurance Act (Act No. 123 of 1997)

(viii) Any other character, letter, number, symbol or other codes prescribed by rules of the Personal Information Protection Commission as equivalent to each preceding item.

Article 2 of the Rules

Standards prescribed by rules of the Personal Information Protection Commission under Article 1, item (i) of the Order to Enforce the Act on the Protection of Personal Information (hereinafter referred to as the "Order") shall be to convert for the purpose of being provided for use in computers an appropriate scope by using an appropriate method so as to ensure the level of ability to identify a specific individual.

Article 3 of the Rules

Character, letter, number, symbol or other codes prescribed by rules of the Personal Information Protection Commission under Article 1, item (vii) of the Order shall be, for a certificate set forth in each following item, those prescribed in each said item respectively.

(i) a certificate set forth in Article 1, item (vii), (a) of the Order; Insurer's number, insured person's symbol and number set forth in Article 111-2, paragraph 1 of the National Health Insurance Act (Act No.192 of 1958)

(ii) a certificate set forth in Article 1, item (vii), (b) of the Order; Insurer's number and insured person's number set forth in Article 161-2, paragraph 1 of the Act on Ensuring Medical Care for Elderly People (Act No.80 of 1982)

(iii) a certificate set forth in Article 1, item (vii), (c) of the Order; Number and insurer's number of the certificate set forth in the same item, (c)

Article 4 of the Rules

Character, letter, number, symbol or other codes prescribed by rules of the Personal Information Protection Commission under Article 1, item (viii) of the Order shall be those set forth in the following.

(i) insurer's number under in Article 3, paragraph (11) of the Health Insurance Act (Act No. 70 of 1922), and an insured person's symbol and number under the same Article, paragraph (12)

(ii) insurer's number under in Article 2, paragraph (10) of the Seaman's Insurance Act (Act No. 73 of 1939) and an insured person's symbol and number under in the same Article, paragraph (11)

(iii) number of a passport under in Article 2, item (v) of the Immigration Control and Refugee Recognition Act (Act No.319 of 1951) (excluding those issued by the Japanese government)

(iv) number of a residence card under Article 19-4, paragraph (1), item (v) of the Immigration Control and Refugee Recognition Act
(v) insurer's number, and subscriber symbol and number under Article 45, paragraph (1) of the Act on Private School Employee Mutual Aid (Act No. 245 of 1953)
(vi) insurer's number, and member symbol and number under Article 112-2, paragraph (1) of the National Public Service Personnel Mutual Aid Associations Act (Act No. 128 of 1958)
(vii) insurer's number, and member symbol and number under Article 144-24-2, paragraph (1) of the Mutual Aid Association for Local Government Officials Act (Act No. 152 of 1962)
(viii) insured person's number of an employment insurance certificate under Article 10, paragraph (1) of the Employment Insurance Act (the Ministry of Labour Ordinance No. 3 of 1975)
(ix) number of special permanent resident certificate under Article 8, paragraph (1), item (iii) of the Special Act on the Immigration Control of, Inter Alia, Those who have Lost Japanese Nationality Pursuant to the Treaty of Peace with Japan (Act No. 71 of 1991)

2-4 Special Care-Required Personal Information (in Relation to Article 2, paragraph (3) of the Act)

"Special care-required personal information" means personal information of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to a principal, including descriptions, etc. in (1) through (11) below.

As a general rule, a principal's consent is required in order to acquire such special care-required personal information and provide the same to third parties, and it should be kept in mind that third-party provision prescribed in Article 23, paragraph (2) of the Act (third-party provision through opt-out) is not permitted (see 3-2-3 (Acquisition of Special Care-Required Personal Information), 3-5-1 (Principle of Restriction on Third-Party Provision), and 3-5-2 (Third-Party Provision through Opt-Out)).

Incidentally, information which is merely suggestive of the information listed below (e.g. information, etc. concerning a purchase or lending of a book on religion) is not included in special care-required personal information.

(1) Race:

This broadly refers to race, family origin, or ethnic or tribal origin. Additionally, a mere reference to a nationality or the "foreigner" status is that to a legal status, and such

information itself is not covered by this category of race. Furthermore, skin color is not covered by this category because it is merely suggestive of one's race.

(2) Creed:
This refers to an individual's fundamental notions or views and includes both thought and faith.

(3) Social status:
This refers to a status which is fixated to an individual's circumstances and which such individual cannot easily get out of by his/her ability during his/her lifetime, and this does not include a mere occupational position or academic background.

(4) Medical history:
This refers to a history of illnesses contracted by an individual, and portions describing a specific medical history (e.g. a specific individual's having cancer, schizophrenia, etc.) are covered by this category.

(5) Criminal record:
This refers to a previous criminal conviction, i.e., a fact of a guilty verdict which has become final.

(6) Fact of having suffered damage by a crime:
This refers to a fact that an individual has suffered damage by a crime, whether physically, mentally, or financially. More specifically, among acts which may meet elements prescribed in the penal laws and regulations, a case where a criminal procedure was instituted is covered by this category.

(7) Fact of having physical disabilities, intellectual disabilities, mental disabilities (including developmental disabilities), or other physical and mental functional disabilities prescribed by rules of the Personal Information Protection Commission (in relation to Article 2, item (i) of the Cabinet Order):
This refers to information described in (i) through (iv) below. In addition to those, information which leads to the identification of such disability at present or in the past (e.g. an individual's receiving a welfare service for disabilities at present or in the past pursuant to the Act on the Comprehensive Support for the Daily and Social Life of Persons with Disabilities (Act No. 123 of 2005)) is also covered by this category.

(i) Information which leads to the identification of any of the "physical disabilities set forth in the appended table of the Act for Welfare of Persons with Physical Disabilities (Act No. 283 of 1949)"

- Diagnosis or assessment that a medical doctor or a Recovery Consultation Office for Persons with Physical Disabilities makes to the effect that an individual has a physical disability set forth in the appended table (including a description of disability in the appended table or information concerning the degree thereof)
- Issuance of a physical disability certificate by a prefectural governor, a mayor of the designated city, or a mayor of the core city and possession of such certificate at present or in the past (including a description of disability in the appended table or information concerning the degree thereof)
- A physical disability set forth in the appended table as it is apparent from a principal's appearance

(ii) Information which leads to the identification of any of the "intellectual disabilities referred to under the Act for the Welfare of Persons with Intellectual Disabilities (Act No. 37 of 1960)"

- Diagnosis or assessment that a medical doctor, a Child Counselling Office, a Rehabilitation Consultation Office for the Mentally Challenged, a Mental Health and Welfare Center, or a National Institute of Vocational Rehabilitation makes to the effect that an individual has an intellectual disability (including information concerning the degree of such disability)
- Issuance of a mental disability certificate by a prefectural governor or a mayor of the designated city and possession of such certificate at present or in the past (including information concerning the degree of such disability)

(iii) Information which leads to the identification of any of the "mental disabilities referred to under the Act for the Mental Health and Welfare of the Persons with Mental Disabilities (Act No.123 of 1950) (including developmental disabilities prescribed in Article 2, paragraph (1) of the Act on Support for Persons with Development Disabilities (Act No. 167 of 2004), and excluding intellectual disabilities under the Act for the Welfare of Persons with Intellectual Disabilities)"

- Diagnosis or assessment that a medical doctor or a Mental Health and Welfare Center makes to the effect that an individual has a mental disability or developmental disability (including information concerning the degree of such disability)
- Issuance of a mental disability certificate by a prefectural governor or a mayor

of the designated city and possession of such certificate at present or in the past (including information concerning the degree of such disability)

(iv) Information which leads to the identification of "a disease with no cure methods established therefor or other peculiar diseases of which the severity by those prescribed by cabinet order under Article 4, paragraph (1) of the Act on Comprehensive Support for Daily and Social Lives of Persons with Disabilities is equivalent to those prescribed by the Minister of Health, Labor and Welfare under the said paragraph"

- Diagnosis that a medical doctor makes to the effect that an individual is continuously and substantially limited in daily and social lives due to a disability resulting from a peculiar disease prescribed by the Minister of Health, Labor and Welfare (including a name of the disease and the degree thereof)

(8) Results of a medical check-up or other examination (hereinafter referred to as a "medical check-up, etc." in the succeeding item) for the prevention and early detection of a disease conducted on a principal by a medical doctor or other person engaged in duties related to medicine (hereinafter referred to as a "medical doctor, etc." in the succeeding item) (in relation to Article 2, item (ii) of the Cabinet Order) (*):

This refers to the results of tests that reveals an examinee's health condition, such as a heath examination, health check-up, specified health examination, health test, stress check, and genetic test conducted for the prevention and early detection of a disease (excluding those conducted in the process of medical examination).

More specifically, the results of a health check-up conducted under the Industrial Safety and Health Act (Act No. 57 of 1972), the results of a stress check conducted under said Act, and the results of a specified health examination conducted under the Act on Assurance of Medical Care for Elderly People (Act No. 80 of 1982) are covered by this category. Furthermore, this category is not limited to the results, etc. of health examinations set forth in laws, but also covers the results of tests carried out or subsidized by an insurer or a business operator at its discretion, such as a comprehensive medical examination. Additionally, this category also covers the results, etc. relating to a principal's genetic form or the likelihood of contracting certain diseases based on such genetic form as such results are obtained through a genetic test conducted by a non-medical institution. For clarity, this category does not cover a fact that an individual had a health check-up, etc.

Incidentally, if information regarding an individual's health such as his/her height,

weight, blood pressure, pulse, and body temperature may be obtained in a manner not associated with the operation of health check-ups and medical examinations and other relevant services, then such information is not covered by this category.

(9) Fact that guidance for the improvement of the mental and physical conditions, or medical care or prescription has been given to a principal by a medical doctor, etc. based on the results of a health check-up, etc. or by reason of disease, injury or other mental and physical changes (in relation to Article 2, item (iii) of the Cabinet Order) (*)

The "fact that guidance for the improvement of the mental and physical conditions, or medical care or prescription has been given to a principal by a medical doctor, etc. based on the results of a health check-up" refers to the substance of health guidance given by a medical doctor or public health nurse to those who particularly need to maintain their health as a result of a health check-up, etc.

Specific examples of such guidance covered by this category are: the substance of health guidance given by a medical doctor or public health nurse under the Industrial Safety and Health Act, the substance of face-to-face guidance given by a medical doctor under said Act, the substance of specified health guidance given by a medical doctor, public health nurse, or managerial dietitian under the Act on Assurance of Medical Care for Elderly People. Furthermore, this category is not limited to the substance of health guidance set forth in laws, but also covers the substance of health guidance carried out or subsidized by an insurer or a business operator at its discretion. Additionally, the fact that health guidance, etc. was given is also covered by this category.

The "fact that medical care has been given to a principal by a medical doctor, etc. based on the results of a health check-up, etc. or by reason of disease, injury or other mental and physical changes" refers to all information which may be acquired by medical doctors, dentists, pharmacists, nurses, or other medical care professionals with regard to patients' physical conditions, medical conditions, therapeutic conditions, etc. in the process of medical treatment at hospitals, clinics, and other facilities at which medical care is provided, and for instance, medical records, etc. are covered by this category. Additionally, the fact of a visit to a hospital, etc. for medical purposes is also covered by this category.

The "fact that a prescription has been given to a principal by a medical doctor, etc. based on the results of a health check-up, etc. or by reason of disease, injury or other mental and physical changes" refers to all information which may be acquired by pharmacists (including where medical doctors or dentists prepare drugs based on their own prescriptions) with regard to patients' physical conditions, medical conditions,

therapeutic conditions, etc. in the process of prescription at hospitals, clinics, pharmacies and other facilities at which medical care is provided, and information such as prescription records, medication records, and matters contained in personal medicine booklets are covered by this category. Additionally, the fact of receiving a prescription at a pharmacy, etc. is also covered by this category.

Incidentally, if information regarding an individual's health such as his/her height, weight, blood pressure, pulse, and body temperature may be obtained in a manner not associated with the operation of health check-ups and medical examinations and other relevant services, then such information is not covered by this category.

(10) Fact that an arrest, search, seizure, detention, institution of prosecution or other procedures related to a criminal case have been carried out against a principal as a suspect or defendant (in relation to Article 2, item (iv) of the Cabinet Order):

The fact that procedures related to a criminal case have been carried out against a principal as a suspect or defendant is covered by this category. The fact that a principal was questioned for a criminal investigation against another person as a suspect, or the fact that a principal was interviewed as a witness are not covered by this category because the principal is not treated as a suspect or defendant.

(11) Fact that an investigation, measure for observation and protection, hearing and decision, protective measure or other procedures related to a juvenile protection case have been carried out against a principal as a juvenile delinquent or a person suspected thereof under Article 3, paragraph (1) of the Juvenile Act (Act No. 168 of 1948) (in relation to Article 2, item (v) of the Cabinet Order):

The fact that a protective measure or other procedures related to a juvenile protection case have been carried out against a principal is covered by this category.

(*) Information that a genetic test reveals may include those that may bring about discrimination or prejudice (e.g. information regarding any disease which could be contracted in the future or choice of therapeutic medication), and such information may be covered as "results of a medical check-up or other examination for the prevention and early detection of a disease conducted on a principal by a medical doctor or other person engaged in duties related to medicine" (in relation to Article 2, item (ii) of the Cabinet Order) or the "fact that guidance for the improvement of the mental and physical conditions, or medical care or prescription has been given to a principal by a medical doctor, etc. based on the results of a health check-up,

etc. or by reason of disease, injury or other mental and physical changes" (in relation to Article 2, item (iii) of the Cabinet Order).

(For Reference)

Article 2 of the Act (paragraph (3))

(3) "Special care-required personal information" in this Act means personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.

Article 2 of the Cabinet Order

Those descriptions etc. prescribed by cabinet order under Article 2, paragraph (3) of the Act shall be those descriptions etc. which contain any of those matters set forth in the following (excluding those falling under a principal's medical record or criminal history)

(i) the fact of having physical disabilities, intellectual disabilities, mental disabilities (including developmental disabilities), or other physical and mental functional disabilities prescribed by rules of the Personal Information Protection Commission;

(ii) the results of a medical check-up or other examination (hereinafter referred to as a "medical check-up etc." in the succeeding item) for the prevention and early detection of a disease conducted on a principal by a medical doctor or other person engaged in duties related to medicine (hereinafter referred to as a "doctor etc." in the succeeding item);

(iii) the fact that guidance for the improvement of the mental and physical conditions, or medical care or prescription has been given to a principal by a doctor etc. based on the results of a medical check-up etc. or for reason of disease, injury or other mental and physical changes;

(iv) the fact that an arrest, search, seizure, detention, institution of prosecution or other procedures related to a criminal case have been carried out against a principal as a suspect or defendant;

(v) the fact that an investigation, measure for observation and protection, hearing and decision, protective measure or other procedures related to a juvenile protection case have been carried out against a principal as a juvenile delinquent or a person suspected thereof under Article 3, paragraph (1) of the Juvenile Act.

Article 5 of the Rule

Physical and mental functional disabilities prescribed by rules of the Personal Information

Protection Commission under Article 2, item (i) of the Order shall be those disabilities set forth in the following.

(i) physical disabilities set forth in an appended table of the Act for Welfare of Persons with Physical Disabilities (Act No.283 of 1949)

(ii) intellectual disabilities referred to under the Act for the Welfare of Persons with Intellectual Disabilities (Act No.37 of 1960)

(iii) mental disabilities referred to under the Act for the Mental Health and Welfare of the Persons with Mental Disabilities (Act No.123 of 1950) (including developmental disabilities prescribed in Article 2, paragraph (2) of the Act on Support for Persons with Development Disabilities, and excluding intellectual disabilities under the Act for the Welfare of Persons with Intellectual Disabilities)

(iv) a disease with no cure methods established thereof or other peculiar diseases of which the severity by those prescribed by cabinet order under Article 4, paragraph (1) of the Act on Comprehensive Support for Daily and Social Lives of Persons with Disabilities (Act No. 123 of 2005) is equivalent to those prescribed by the Minister of Health, Labor and Welfare under the said paragraph

2-5 Personal Information Database, etc. (in Relation to Article 2, paragraph (4) of the Act)

"Personal information database, etc." means a collective body of information comprising personal information which is systematically organized so as to be able to search for particular personal information using a computer. In addition, even where a computer is not used, those including a table of contents, index or other similar arrangement to facilitate search of information that has been systematically organized by arranging personal information processed on paper according to a certain rule (e.g. in the order of the Japanese alphabet) that enables specified personal information to be readily searched for by others.

However, those described in (1) through (3) below are not covered by this category because such information has little possibility of harming an individual's rights and interests considering the utilization method of such information.

(1) those which have been issued for the purpose of being sold to a large number of unspecified persons and the issuance of which has not been conducted in violation of the provisions of a law or order based thereon;

(2) those which can be, or could have been, purchased at any time by a large number of unspecified persons;

(3) those which are being provided for their original purpose without adding other information

relating to a living individual.

<Examples of Personal Information Database, etc.>

Case 1) Email address book stored in an emailing software program (where email addresses are associated with names)

Case 2) Electronic file in which log information relating to the use of a service on the Internet by its users is organized and saved by user IDs (where user IDs can be easily collated with personal information)

Case 3) Business card information where such information is entered and organized by employees by using spreadsheet software in a business PC (regardless of an owner thereof)

Case 4) Registration card information where an employee dispatching company files such cards by organizing them in the Japanese alphabetical order and indexing them in the Japanese alphabetical order

<Examples that are not recognized as Personal Information Database, etc.>

Case 1) Even where employees have their business card holders freely accessible by others, if business cards are assorted in a unique manner that does not allow them to be readily searchable by others

Case 2) Where post card responses to a questionnaire are not assorted or organized by names, addresses, etc.

Case 3) Commercially available telephone directories, residential maps, employee directories, car navigation systems, etc.

(For Reference)

Article 2 of the Act (paragraph (4))

(4) A "personal information database etc." in this Act means those set forth in the following which are a collective body of information comprising personal information (excluding those prescribed by cabinet order as having little possibility of harming an individual's rights and interests considering their utilization method).

(i) those systematically organized so as to be able to search for particular personal information using a computer;

(ii) besides those set forth in the preceding item, those prescribed by cabinet order as having been systematically organized so as to be able to easily search for particular personal information.

Article 3 of the Cabinet Order

(1) Those prescribed by cabinet order as having little possibility of harming an individual's rights and interests considering their utilization method under Article 2, paragraph (4) of the Act shall be those falling under all of each following item.

(i) those which have been issued for the purpose of being sold to a large number of unspecified persons and the issuance of which has not been conducted in violation of the provisions of a law or order based thereon;

(ii) those which can be, or could have been, purchased at any time by a large number of unspecified persons;

(iii) those which are being provided for their original purpose without adding other information relating to a living individual.

(2) Those prescribed by cabinet order under Article 2, paragraph (4), item (ii) of the Act shall be a collective body of information including a table of contents, index or similar others to facilitate search of information that has been systematically organized by arranging personal information contained in the database according to a certain rule that enables specified personal information to be readily searched for.

2-6 Personal Information Handling Business Operator (in Relation to Article 2, paragraph (5) of the Act)

"Personal information handling business operator" means a person providing a personal information database, etc. for use in business; however, excluding a central government organization, a local government, an incorporated administrative agency, etc. as prescribed in the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (Act No. 59 of 2003), and a local incorporated administrative agency as prescribed in the Local Incorporated Administrative Agencies Act (Act No. 118 of 2003).

For this purpose, the term "business" in the phrase "providing for use in business" means activities of a similar nature that are conducted repetitiously and continuously for a certain purpose and that are recognized as business under social norms, whether for profits or non-profit.

Additionally, any person who provides a personal information database, etc. for use in business falls under the category of a personal information handling business operator, regardless of a scale of the number of specified individuals identifiable by personal information comprising such personal information database, etc.

Incidentally, if a non-judicial association without rights (unincorporated association) or an individual provides a personal information database, etc. for use in business, then such association or individual also falls under the category of a personal information handling business operator.

(For Reference)

Article 2 of the Act (paragraph (5))

(5) A "personal information handling business operator" in this Act means a person providing a personal information database etc. for use in business; however, excluding a person set forth in the following;

(i) a central government organization;

(ii) a local government;

(iii) an incorporated administrative agency etc. (meaning an independent administrative agency etc. prescribed in Article 2, paragraph (1) of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (Act No. 59 of 2003); hereinafter the same);

(iv) a local incorporated administrative agency (meaning a local incorporated administrative agency prescribed in Article 2, paragraph (1) of the Local Incorporated Administrative Agencies Act (Act No. 118 of 2003); hereinafter the same);

2-7 Personal Data (in Relation to Article 2, paragraph (6) of the Act)

"Personal data" means personal information constituting a personal information database, etc. administered by a telecommunications carrier.

Incidentally, personal information constituting those excluded from personal information database, etc. because it has little possibility of harming an individual's rights and interests considering the utilization method of such information (e.g. commercially available telephone directory, residential map, etc.) is not treated as personal data (see 2-5 "Personal Information Database, etc.").

<Examples of Personal Data>

Case 1） Personal information extracted from a personal information database, etc. and stored in an external recording medium

Case 2） Personal information extracted from a personal information database, etc. and printed out onto paper forms

<Examples that are not recognized as Personal Data>

Case) Personal information contained in forms for input before such personal information becomes part of a personal information database, etc.

(For Reference)

Article 2 of the Act (paragraph (6))
(6) "Personal data" in this Act means personal information constituting a personal information database etc.

2-8 Retained Personal Data (in Relation to Article 2, paragraph (7) of the Act)

"Retained personal data" (*1) means "personal data" which a telecommunications carrier has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of (such actions shall be referred to hereinafter as "disclosure, etc.") (*2).

However, personal data that are described below or that are set to be deleted within a period of no longer than six months (except for updating) are not "retained personal data".

(1) Those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would harm a principal or third party's life, body or fortune.

(2) Those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would encourage or induce an illegal or unjust act.

Case 1) Personal data which pertain to a principal falling under the category of anti-social forces and which are held by a telecommunications carrier in order to prevent damage, etc. due to an unreasonable demand by anti-social forces such as an organized crime group (*boryokudan*)

Case 2) Personal data which pertain to a principal who makes unreasonable demands, such as a suspicious person or a vicious complainer and which are held by a telecommunications carrier in order to prevent damage, etc. from such demand

(3) Those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would undermine national security, destroy a trust relationship with a foreign country or international organization, or cause disadvantage in negotiations with a foreign country or international organization.

(4) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would hinder the maintenance of public safety and order such as the prevention, suppression or investigation of a crime.

Case 1) Personal data acquired for the first time as a result of an investigative inquiry,

etc. by the police

Case 2) Personal data such as inquiry records, response records, and lists of inquiry subjects prepared by a telecommunications carrier who received an investigative inquiry, etc. by the police with respect to subscriber information, etc., in the process of responding to such inquiries (*For clarity, the subscriber information itself falls under the category of "retained personal data".)

Case 3) Information as to whether or not any report was made as to a suspicious deal (hereinafter referred to as a "suspicious deal") under Article 8, paragraph (1) of the Act on Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007) as well as personal data newly prepared in making such report

Case 4) Personal data containing information pertaining to accounts used for bank transfer fraud

(*1) It must be kept in mind that, under the Act, the terms such as "personal information" (see 2-2 (Personal Information)), "personal data" (see 2-7 (Personal Data)), "retained personal data", "special care-required personal information" (see 2-4 (Special Care-Required Personal Information)), and "anonymously processed information" (see 2-9 (Anonymously Processed Information)) have distinctive meanings, and the duties imposed on Personal Information Handling Business Operators, etc. are different for the respective types of information.

(*2) For instances, etc. in which specific actions such as disclosure, etc. are required, see 3-6-2 (Disclosure of Retained Personal Data), et seq. Additionally, if several personal information handling business operators are involved in the handling of personal data due to subcontracting, etc., determinations as to which personal information handling business operators have the authority to make disclosure, etc. are made based on actual contractual and other circumstances.

(For Reference)

Article 2 of the Act (paragraph (7))

(7) "Retained personal data" in this Act means personal data which a personal information handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of, and which shall be neither those prescribed by cabinet order as likely to harm the public or other interests if their presence or absence is made known nor those set to be deleted within a period of no longer than one year that is prescribed by cabinet order.

Article 4 of the Cabinet Order

Article 4 Those prescribed by cabinet order under Article 2, paragraph (7) shall be those set forth in the following.

(i) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would harm a principal or third party's life, body or fortune;

(ii) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would encourage or induce an illegal or unjust act;

(iii) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would undermine national security, destroy a trust relationship with a foreign country or international organization, or suffer disadvantage in negotiations with a foreign country or international organization;

(iv) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would hinder the maintenance of public safety and order such as the prevention, suppression or investigation of a crime.

Article 5 of the Cabinet Order

A period prescribed by cabinet order under Article 2, paragraph (7) of the Act shall be six months.

2-9 Anonymously Processed Information (in Relation to Article 2, paragraph (9) of the Act)

For the definition of anonymously processed information, see the "*Guidelines for the Act on the Protection of Personal Information (for Anonymously Processed Information)*" (Personal Information Protection Commission Public Notice No. 9 of 2016) prescribed by the Personal Information Protection Commission.

(For Reference)

Article 2 of the Act (paragraph (9))

(9) "Anonymously processed information" in this Act means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each following item in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information.

(i) personal information falling under paragraph (1), item (i); Deleting a part of descriptions etc. contained in the said personal information (including replacing the said part of

descriptions etc. with other descriptions etc. using a method with no regularity that can restore the said part of descriptions etc.)

(ii) personal information falling under paragraph (1), item (ii); Deleting all individual identification codes contained in the said personal information (including replacing the said individual identification codes with other descriptions etc. using a method with no regularity that can restore the said personal identification codes)

2-10 Anonymously Processed Information Handling Business Operator (in Relation to Article 2, paragraph (10) of the Act)

For the definition of an anonymously processed information handling business operator, see the "*Guidelines for the Act on the Protection of Personal Information (for Anonymously Processed Information)*" prescribed by the Personal Information Protection Commission.

(For Reference)

Article 2 of the Act (paragraph (10))

(10) An "anonymously processed information handling business operator" in this Act means a person who provides for use in business a collective body of information comprising anonymously processed information which has been systematically organized so as to be able to search using a computer for specific anonymously processed information or similar others prescribed by cabinet order as systematically organized so as to be able to search easily for specific anonymously processed information (referred to as an "anonymously processed information database etc." in Article 36, paragraph (1)). However, a person set forth in each item of paragraph (5) is excluded.

Article 6 of the Cabinet Order

Those prescribed by cabinet order under Article 2, paragraph (10) of the Act mean a collective body of information including a table of contents, index or similar others to facilitate search of information that has been systemically organized by arranging anonymously processed information contained in the database etc. according to a certain rule that enables specified anonymously processed information to be readily searched for.

2-11 "Informing a Principal"

"Informing a principal" means directly notifying a principal, and depending on the nature of business and how personal information is handled, such notification must be made in a reasonable

and appropriate manner so that the substance of such notification will be recognized by the principal.

<Examples of Informing a Principal>

Case 1) Notification by direct delivery of a flier or other document.

Case 2) Notification by verbal communications or by way of an interactive voice response system, etc.

Case 3) Notification by email, facsimile, etc. or sending a document by mail, etc.

(For Reference)

Article 18 of the Act (paragraph (1))

(1) A personal information handling business operator shall, in case of having acquired personal information except in cases where a utilization purpose has been disclosed in advance to the public, promptly inform a principal of, or disclose to the public, the utilization purpose.

* (For Reference) In addition to the above, the provisions below mainly relate to "informing a principal".

(i) In relation to the utilization purpose:
Article 18, paragraphs (3) and (4) of the Act (see 3-1-2 (Altering a Utilization Purpose); 3-2-7 (Where Notification, etc. of Utilization Purpose is Not Required))

(ii) In relation to the third-party provision:
Article 23, paragraphs (2) and (3), paragraph (5), item (iii), and paragraph (6) of the Act (see 3-5-2 (Third-Party Provision through Opt-Out); 3-5-4 (Cases where the Recipient is not Deemed a Third Party))

(iii) In relation to requests, etc. for disclosure, etc.:
Article 27, paragraphs (2) and (3) of the Act, Article 28, paragraph (3) of the Act, Article 29, paragraph (3) of the Act, and Article 30, paragraph (5) of the Act (see 3-6-1 (Public Disclosure, etc. of Matters Concerning Retained Personal Data); 3-6-2 (Disclosure of Retained Personal Data); 3-6-3 (Correction, etc. of Retained Personal Data); and 3-6-4 (Utilization Cease, etc. of Retained Personal Data)).

2-12 "Disclosure to the Public"

"Disclosure to the Public" means communicating one's intentions widely to the public (making announcement so that a large number of unspecified persons will know), and depending on the nature of business and how personal information is handled, such publication must be made

in a reasonable and appropriate manner.

<Examples of Disclosure to the Public>

Case 1) Posting at a location which can be visited in one action or so

Case 2) Posting of a poster, or placement or distribution of a brochure, etc. at a company's store, office, etc. or a location expected to be visited by customers

Case 3) (In the case of teleshopping) posting in a brochure, catalog, etc. for teleshopping

(For Reference)

Article 18 of the Act (paragraph (1))

(1) A personal information handling business operator shall, in case of having acquired personal information except in cases where a utilization purpose has been disclosed in advance to the public, promptly inform a principal of, or disclose to the public, the utilization purpose.

* (For Reference) In addition to the above, the provisions below mainly relate to "disclosure to the public".

(i) In relation to the utilization purpose:
Article 18, paragraph (3) of the Act (see 3-1-2 (Altering a Utilization Purpose))

(ii) In relation to anonymously processed information:
Article 36, paragraphs (3), (4) and (6), Article 37, and Article 39 of the Act (see 3-8 (Duties of Anonymously Processed Information Handling Business Operators, etc.))

(iii) Other provision:
Article 76, paragraph (3) of the Act

2-13 "Principal's Consent"

A "principal's consent" means the principal's manifestation of intention to give a consent that his/her personal information may be handled in the manner indicated by the personal information handling business operator (on condition that the principal's identity has been verified).

Furthermore, "to obtain a principal's consent" or "a principal's consent having been obtained" means that the relevant telecommunications carrier recognizes the principal's manifestation of intention to give such consent, and depending on the nature of business and how personal information is handled, such recognition must be made in a reasonable and appropriate manner required in order for the principal to make a determination as to giving such consent.

Not only where a separate consent has been obtained, but where contractual terms and

conditions relating to the telecommunications services contain clauses relating to the third-party provision of personal information, and if a contract relating to the telecommunications services is executed under such contractual terms and conditions (*1) and such clauses are valid under private law (*2), it is interpreted to mean that "a principal's consent is being sought" or "a principal's consent has been obtained". However, if it is recognized that the clauses, etc. of the contractual terms and conditions permitting unlimited third-party provision are harming the user's interests, then an order for improvement of business activities under the Telecommunications Business Act may be issued.

However, with regard to the handling of personal information protected under the secrecy of communications (including not only the content of communications, but also the elements of communications such as the addresses, names, and sending locations of the party to the communications, date of each communication, as well as the existence of a fact of any communication such as the number of times of communications), individual, specific and clear consent of the party to the communication is required, and such consent cannot be given by his/her agent, etc. in the absence of his/her specific entrustment.

Additionally, regarding minors, adult wards, those under curatorship, and those under assistance, who cannot judge the consequences of their consent as to the handling of personal information, it is required to obtain consent from those in parental authority or their legal representatives, etc.

(*1) Even where the provision concerning the third-party provision of personal information is implemented by amending the contractual terms and conditions, if such amendment is valid under private law and the amended provision is recognized as binding on the parties to the contract before the amendment, then it is interpreted to mean that the "principal's consent" has been obtained.

(*2) If the provision is contrary to the public order or morals under Article 90 of the Civil Code (Act No. 89 of 1896), or if there is a mistake in an element under Article 95 of the Civil Code, or if consumers' interests under Article 10 of the Consumer Contract Act (Act No. 61 of 2000) are unilaterally harmed, or if the consent is otherwise found invalid under private law, then because there is no valid consent, the consent cannot be obtained for this purpose.

<Examples of a Principal of Consent>

Case 1) The principal's verbal manifestation of intention to give the consent

Case 2) Receipt of a document (including electromagnetic records) from the principal indicating his/her consent

Case 3) Receipt of email from the principal indicating his/her consent

Case 4) The principal's placing a check mark in the relevant portion to give the consent

Case 5) The principal's clicking on the button to indicate his/her consent

Case 6) Voice input, or input by touching a touch panel, button or switch by the principal to give the consent

(For Reference)

Article 16 of the Act (paragraph (1))

(1) A personal information handling business operator shall not handle personal information without obtaining in advance a principal's consent beyond the necessary scope to achieve a utilization purpose specified pursuant to the provisions under the preceding Article.

* (For Reference) In addition to the above, the provisions below mainly relate to a "principal's consent".

(i) In relation to the utilization purpose:
Article 16, paragraph (2), and paragraph (3), items (ii) through (iv) of the Act (see 3-1-5 (Succession of Business); 3-1-6 (Exceptions to Restrictions by Utilization Purpose))

(ii) In relation to the acquisition of special care-required personal information:
Article 17, paragraph (2) of the Act (see 3-2-3 (Acquisition of Special Care-Required Personal Information))

(iii) In relation to the third-party provision:
Article 23, paragraph (1) and Article 24 of the Act (see 3-5-1 (Principle of Restrictions on Third-Party Provision); 3-5-5 (Restriction on Provision to a Third-Party in a Foreign Country))

2-14 "Provision"

"Provision" means making personal data, retained personal data or anonymously processed information available to those other than oneself. Even where personal data, retained personal data or anonymously processed information are not physically provided, if personal data, retained personal data or anonymously processed information are available for use by using the network, etc. (or the authority to use the same is granted), then it constitutes "provision".

(For Reference)

Article 2 of the Act (paragraph (7))

(7) "Retained personal data" in this Act means personal data which a personal information handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of, and which shall be neither those prescribed by cabinet order as likely to harm the public or other interests if their presence or absence is made known nor those set to be deleted within a period of no longer than one year that is prescribed by cabinet order.

Article 23 of the Act (paragraph (1))

(1) A personal information handling business operator shall, except in those cases set forth in the following, not provide personal data to a third party without obtaining in advance a principal's consent.

(i) through (iv) *omitted*

* (For Reference) In addition to the above, the provisions below mainly relate to "provision".

(i) In relation to the third-party provision:
Article 23, paragraphs (2) and (5), and Articles 24, 25 and 26 of the Act (see 3-5-2 (Third-Party Provision through Opt-Out); 3-5-4 (Where a Person is Not Deemed a Third Party); 3-5-5 (Restriction on Provision to a Third Party in a Foreign Country); 3-5-6 (Keeping, etc. of a Record on a Third-Party Provision); and 3-5-7 (Confirmation, etc. when Receiving a Third-Party Provision))

(ii) In relation to requests for suspension of third-party provision of retained personal data:
Article 30, paragraphs (3), (4) and (5) of the Act (see 3-6-4 (Utilization Cease, etc. of Retained Personal Data))

(iii) In relation to anonymously processed information:
Article 36, paragraph (4) and Article 37 of the Act (see 3-8 (Duties of Anonymously Processed Information Handling Business Operators, etc.))

3 Duties of Telecommunications Carriers (in Relation to Chapter II)

3-1 Utilization Purpose of Personal Information (in Relation to Articles 4 and 5 and Article 8, Paragraph 3)

3-1-1 Specifying a Utilization Purpose (in Relation to Article 4, Paragraph 1)

Article 4 (Paragraph 1)
1. A telecommunications carrier shall, in handling personal information, specify the purpose of utilizing the personal information (hereinafter referred to as a "utilization purpose") as explicitly as possible.

In handling personal information, a telecommunications carrier must specify the utilization purpose as explicitly as possible, but in specifying the utilization purpose, such utilization purpose should not be described just in abstract or general terms, but it is desirable to describe for what business personal information is ultimately used and for what purpose personal information is used by the telecommunications carrier specifically to the extent that a principal can anticipate such use generally and reasonably (*).

Additionally, if personal information is anticipated to be provided to a third party, such provision must be clearly specified in specifying the utilization purpose (see 3-5-1 (Principle of Restrictions on Third-Party Provision)).

<Examples of Explicit Specification of Utilization Purpose>

Case) Where a telecommunications carrier acquires an individual's name, mailing address, email address, etc., in selling its products, the utilization purpose is explicitly presented, for instance, by stating that such information "will be used to send products in xxx business, to provide relevant post-sale services, and to provide information regarding new products and services."

<Examples where Utilization Purpose is Not Explicitly Specified>

Case 1) "For business activities"

Case 2) "For marketing activities"

(*) If, in the eyes of a principal who is identifiable by personal information, the scope of utilization of such principal's personal information is specified to the extent that such principal can reasonably expect in view of the business description set forth in Articles of Incorporation, etc., or if the scope of utilization purpose can be anticipated by clearly indicating the type of business, then it could be deemed sufficient; however, in many cases, just by clearly indicating the type of business, it cannot be recognized that the utilization purpose has been specified as explicitly as possible. Moreover, where a business is clearly indicated by using a phrase such

as “xxx business” for the purpose of specifying the utilization purpose, it is desirable to specify such business description to the extent that can help in specifying such business in the eyes of the principal.
Additionally, using abstract and general terms such as “business activities” and “enhancement of customer services” to specify the utilization purpose cannot be regarded as specifying the utilization purpose as explicitly as possible.

(For Reference)

Article 15 of the Act (paragraph (1)) (1) A personal information handling business operator shall, in handling personal information, specify the purpose of utilizing the personal information (hereinafter referred to as a “utilization purpose”) as explicitly as possible.

3-1-2 Altering a Utilization Purpose (in Relation to Article 4, Paragraphs 2 and 3, and Article 8, Paragraph 3)

Article 4 (Paragraph 2) 2. A telecommunications carrier shall, in case of altering a utilization purpose, not do so beyond the scope recognized reasonably relevant to the pre-altered utilization purpose. Article 8 (Paragraph 3) 3. A telecommunications carrier shall, in case of altering a utilization purpose, inform a principal of, or disclose to the public, a post-altered utilization purpose.

The utilization purpose specified pursuant to 3-1-1 (Specifying a Utilization Purpose) above may be amended within the scope that the amended utilization purpose is found reasonably relevant to that before the amendment; in other words, within the scope that the amended utilization purpose is objectively recognized as the extent that a principal can normally expect under social norms in comparison with the utilization purpose before the amendment (*1). A principal must be informed of the amended utilization purpose (*2), or the amended utilization purpose must be disclosed to the public (*3).

Additionally, where personal information is to be handled beyond the extent necessary in order to achieve the specified utilization purpose (including the utilization purpose amended within the scope set forth in Article 4, Paragraph 2), the principal’s consent must be obtained in accordance with Article 5, Paragraph 1. However, where such handling is necessary for the purpose of protecting the principal’s body, etc., and where any case set out in the respective items of Article 5, Paragraph 3 (except in the cases set out in Article 5, Paragraph 4 (see 3-1-7 (Exceptions to Personal Information Protected under the Secrecy of Communications in Relation

to Restriction due to a Utilization Purpose))) applies, for instance, if it is difficult to obtain the principal's consent, then without obtaining the principal's consent in advance, personal information may be handled beyond the extent necessary in order to achieve the specified utilization purpose (see 3-1-6 (Exceptions to Restrictions by Utilization Purpose)).

(*1) The "scope that [the amended utilization purpose] is objectively recognized as the extent that a principal can normally expect under social norms" refers to the scope that ordinary people can expect in their judgment by comparing the initial utilization purpose and the amended utilization purpose, not in the principal's subjective views or by the telecommunications carrier's arbitrary judgment, and such shall be determined by comprehensively taking into consideration the degree of relevance with the initially specified utilization.

(*2) For "informing a principal", see 2-11 (Informing a Principal).

(*3) For "disclosure to the public", see 2-12 (Disclosure to the Public).

(For Reference)

Article 15 of the Act (paragraph (2))

(2) A personal information handling business operator shall, in case of altering a utilization purpose, not do so beyond the scope recognized reasonably relevant to the pre-altered utilization purpose.

Article 18 of the Act (paragraph (3))

(3) A personal information handling business operator shall, in case of altering a utilization purpose, inform a principal of, or disclose to the public, a post-altered utilization purpose.

3-1-3 Scope of Utilization Purpose (in Relation to Article 4, Paragraph 3)

Article 4 (Paragraph 3)

3. A telecommunications carrier shall make efforts so that the utilization purpose specified pursuant to Paragraph 1 will not go beyond the scope necessary in order to provide telecommunications services and incidental services.

This provision is intended to confirm that, given that personal information under Article 6 may be acquired only to the extent necessary in order to provide telecommunications services, the utilization purpose specified pursuant to Paragraph 1 likewise may not go beyond the extent necessary to provide telecommunications services.

However, the "extent necessary in order to provide telecommunications services" is not limited to the extent directly necessary for telecommunications services currently provided, but

includes those relevant to such services (for instance, a survey by questionnaire for the provision of a new service). Additionally, if any utilization purpose is to be specified beyond the extent necessary in order to provide telecommunications services, then it is appropriate to obtain the principal's consent with respect to the use for such utilization purpose.

3-1-4 Restriction due to a Utilization Purpose (in Relation to Article 5, Paragraph 1)

Article 5 (Paragraph 1)
1. A telecommunications carrier shall not handle personal information without obtaining in advance a principal's consent beyond the necessary scope to achieve a utilization purpose specified pursuant to the provisions under the preceding Article.

If a telecommunications carrier intends to handle personal information beyond the extent necessary in order to achieve the utilization purpose specified pursuant to Article 4, Paragraph 1, the principal's consent (*) must be obtained in advance.

However, using personal information (by email or telephone, etc.) for the purpose of obtaining such consent is not considered to be an unintended use even if such use is not mentioned as the initially specified utilization purpose.

(*) For the "principal's consent", see 2-13 (Principal's Consent).

(For Reference)

Article 16 of the Act (paragraph (1))
(1) A personal information handling business operator shall not handle personal information without obtaining in advance a principal's consent beyond the necessary scope to achieve a utilization purpose specified pursuant to the provisions under the preceding Article.

3-1-5 Succession of Business (in Relation to Article 5, Paragraph 2)

Article 5 (Paragraph 2)
2. A telecommunications carrier shall, in case of having acquired personal information accompanied with succeeding a business from another personal information handling business operator because of a merger or other reason, not handle the personal information without obtaining in advance a principal's consent beyond the necessary scope to achieve the pre-succession utilization purpose of the said personal information.

If a telecommunications carrier acquires personal information in connection with a

succession of business from another personal information handling business operator due to a merger, spin-off, business transfer, etc., and if such personal information is handled within the scope necessary in order to achieve the utilization purpose specified prior to the succession of such personal information, then such use is not considered to be an unintended use, and the principal's consent (*) is not required.

Additionally, if after the succession of business, personal information is to be handled beyond the extent necessary in order to achieve the utilization purpose before the succession, the principal's consent must be obtained in advance; however, using personal information (by email or telephone, etc.) for the purpose of obtaining such consent is not considered to be an unintended use even if such use is not mentioned as the utilization purpose before the succession.

(*) For the "principal's consent", see 2-13 (Principal's Consent).

(For Reference)

Article 16 of the Act (paragraph (2))

(2) A personal information handling business operator shall, in case of having acquired personal information accompanied with succeeding a business from another personal information handling business operator because of a merger or other reason, not handle the personal information without obtaining in advance a principal's consent beyond the necessary scope to achieve the pre-succession utilization purpose of the said personal information.

3-1-6 Exceptions to Restrictions by Utilization Purpose (in Relation to Article 5, Paragraph 3)

Article 5 (Paragraph 3)

3. The provisions under the preceding two paragraphs shall not apply to those cases set forth in the following:
   (1) cases based on laws and regulations;
   (2) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent;
   (3) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent;
   (4) cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs.

In the cases set forth below, the principal's consent (*) is not required even if such consent is required in handling his/her personal information beyond the extent necessary in order to

achieve the specified utilization purpose.

(*) For the "principal's consent", see 2-13 (Principal's Consent).

(1) Cases based on laws and regulations (in relation to Article 5, Paragraph 3, Item (1)):

Article 5, Paragraph 1 or 2 shall not apply to cases based on laws and regulations, and in such cases, without obtaining the principal's consent in advance, his/her personal information may be handled beyond the extent necessary in order to achieve the specified utilization purpose.

Case 1) When responding to an investigative inquiry of the police (Code of Criminal Procedure (Act No. 131 of 2011), Article 197, paragraph (2))
Case 2) When accommodating an investigation under a warrant issued by a judge (Code of Criminal Procedure, Article 218)
Case 3) When accommodating an examination by a tax office on income tax, etc. (Act on General Rules for National Taxes (Act No. 66 of 1962), Article 74-2, etc.)
Case 4) When accommodating an inquiry from a bar association (Attorney Act (Act No. 205 of 1949), Article 23-2)
Case 5) When accommodating an active epidemiological investigation conducted by a public health center (Act on the Prevention of Infectious Diseases and Medical Care for Patients with Infectious Diseases (Act No. 114 of 1998), Article 15, paragraph (1))

(2) Cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent (in relation to Article 5, Paragraph 3, Item (2)):

Article 5, Paragraph 1 or 2 shall not apply to cases in which there is a need to protect specific rights and interests such as a life, body or fortune of a person (including an entity), and when it is difficult to obtain a principal's consent, and in such cases, without obtaining the principal's consent in advance, his/her/its personal information may be handled beyond the extent necessary in order to achieve the specified utilization purpose.

Case 1) When a medical emergency or such other situation occurs, and a principal's blood type, his/her family contact, etc. are provided to a medical doctor or nurse.
Case 2) When an emergency situation such as a large-scale disaster or accident occurs, and information concerning disaster victims and injured persons is provided to families, administrative agencies, municipal governments, etc.
Case 3) When a telecommunications carrier and another personal information handling business operator shares information concerning anti-social forces such as an organized crime

group, information concerning accounts used for bank transfer fraud, and information concerning a person who intentionally engages in an obstruction of business.

Case 4) In an emergency situation where a human life, body or fortune needs to be protected from a serious defect in a product, when the manufacturer asks for customer information, and such information needs to be furnished.

Case 5) When information concerning the occurrence of a financial crime such as fraudulent transfer of funds is provided to other business operators in order to prevent damage from a related crime.

(3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent (in relation to Article 5, Paragraph 3, Item (3)):

Article 5, Paragraph 1 or 2 shall not apply to cases in which there is a special need to enhance public hygiene or promote fostering healthy children in the process of developing mind and body, and when it is difficult to obtain a principal's consent, and in such cases, without obtaining the principal's consent in advance, his/her personal information may be handled beyond the extent necessary in order to achieve the specified utilization purpose.

(4) Cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs (in relation to Article 5, Paragraph 3, Item (4)):

Article 5, Paragraph 1 or 2 shall not apply to a private-sector corporation in cases where there is a need to cooperate in regard to a central government organization, etc. (including a local government or a person entrusted by them) performing affairs prescribed by laws and regulations, and when it is recognized that there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs, and in such cases, without obtaining the principal's consent in advance, his/her personal information may be handled by such private-sector corporation beyond the extent necessary in order to achieve the specified utilization purpose.

Case 1) When a telecommunications carrier submits personal information at the discretionary request of an officer, etc., of a tax office or a custom.

Case 2) When a telecommunications carrier submits personal information at the discretionary request of the police.

Case 3) When a telecommunications carrier responds to a general statistical survey or a statistical survey conducted by a municipal government.

(For Reference)

Article 16 of the Act (paragraph (3))

(3) The provisions under the preceding two paragraphs shall not apply to those cases set forth in the following.

(i) cases based on laws and regulations

(ii) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent

(iii) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent

(iv) cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs

3-1-7 Exceptions to Personal Information Protected under the Secrecy of Communications in Relation to Restriction due to a Utilization Purpose (in Relation to Article 5, Paragraph 4)

Article 5 (Paragraph 4)

4. Notwithstanding the provisions of the preceding three paragraphs, a telecommunications carrier shall not use personal information protected under the secrecy of communications except if there is consent of the users or other justifiable cause for noncompliance with the law.

Acquisition, storage, use or provision to third parties of any matter protected under the secrecy of communications is not permitted except where the corresponding party's consent has been obtained, any of the foregoing is carried out in accordance with a warrant issued by a judge, self-defense or necessity applies, or if there is other justifiable cause for noncompliance with the law (in relation to Articles 4 of the Telecommunications Business Act).

Accordingly, even if any of the provisions in Article 5, Paragraphs 1 through 3 applies, if any personal information is protected under the secrecy of communications, then the use of such information is not permitted except where the corresponding party's consent has been obtained or if there is justifiable cause for noncompliance with the law. Additionally, this also applies where the use is within the scope of utilization purpose.

(*) With regard to the consent relating to the handling of personal information protected under

the secrecy of communications, see 2-13 (Principal's Consent).

3-2 Acquisition of Personal Information (in Relation to Articles 6 through 8)

3-2-1 Restriction on Acquisition (in Relation to Article 6)

> Article 6
>
> A telecommunications carrier shall strive to limit its acquisition of personal information to cases where such information is required in order to provide telecommunications services and incidental services.

In order to prevent unnecessary acquisition of personal information, a telecommunications carrier must strive to acquire personal information only in cases where it is required in order to provide telecommunications services. However, "cases where it is required in order to provide telecommunications services" are not limited to cases where such information is directly necessary for telecommunications services currently provided, but also include those relevant to such services (for instance, a survey by questionnaire for the provision of a new service).

3-2-2 Proper Acquisition (in Relation to Article 7, Paragraph 1)

> Article 7 (Paragraph 1)
>
> 1. A telecommunications carrier shall not acquire personal information by deceit or other improper means.

A telecommunications carrier must not acquire (*1) personal information by deceit or other improper means (*2).

<Cases of Acquisition of Personal Information by a Telecommunications Carrier by Improper Means>

Case 1) Where personal information concerning a family, such as the family's income and other unrelated affairs in view of the situation for acquiring such information, is acquired from a child or disabled person who do not have a sufficient capacity for judgment, without the family's consent.

Case 2) Where personal information is acquired by coercing a violation of restriction on third-party provision prescribed in Article 15, Paragraph 1.

Case 3) Where personal information is acquired from a principal by intentionally indicating false information about an acquirer of personal information, utilization purpose, etc.

Case 4) Where personal information is acquired from another business operator by instructing such business operator to acquire such personal information through improper means.

Case 5) Where personal information is acquired while knowing or being able to easily recognize that a violation of restriction of third-party provision prescribed in Article 15, Paragraph 1, is likely to occur.

Case 6) Where personal information is acquired while knowing or being able to easily recognize that such personal information has been acquired through improper means.

(*1) Where information containing personal information is in the public domain through the Internet, etc., then merely viewing the same will not be interpreted as acquiring such personal information if it is not transferred, etc.

(*2) If a telecommunications carrier or a person engaging in such business or those who were in such business in the past provide or misappropriate a personal information database, etc. handled by such person in connection with such business (including those reproduced or processed in whole or in part) for the purpose of making for its/his/her own benefit or for a third party's benefit improperly, then such act is subject to criminal punishment (imprisonment with work for not more than one year or a fine of not more than 500,000 yen) under Article 83 of the Act.

(For Reference)

Article 17 of the Act (paragraph (1))
(1) A personal information handling business operator shall not acquire personal information by deceit or other improper means.

3-2-3 Acquisition of Special Care-Required Personal Information (in Relation to Article 7, Paragraph 2)

Article 7 (Paragraph 2)
2. A telecommunications carrier shall, except in those cases set forth in the following, not acquire special care-required personal information without obtaining in advance a principal's consent: (1) cases based on laws and regulations; (2) cased in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent; (3) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent; (4) cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a

principal's consent would interfere with the performance of the said affairs;

(5) cases in which the said special care-required personal information is being open to the public by a principal, a government organization, a local government, a person set forth in each item of Article 76, paragraph (1) of the Act, a foreign government, a foreign government agency, a local government in a foreign country, an international organization, or a person equivalent to the person set forth in each item of Article 76, paragraph (1) of the Act;

(6) cases in which seemingly-clear special care-required personal information is acquired by visual observation, filming or photographing of a principal;

(7) when receiving the provision of special care-required personal information organized as personal data in those cases set forth in each item of Article 15, Paragraph 10.

When acquiring special care-required personal information (*1), the principal's consent (*2) must be obtained in advance. However, the principal's consent is not required in the cases of (1) through (7) below.

Incidentally, where a telecommunications carrier acquires special care-required personal information, such telecommunications carrier must not engage in unfair and discriminatory treatment for certain users based on such information in executing a contract for provision of telecommunications services and providing such services (in relation to Article 6 of the Telecommunications Business Act).

(1) Cases based on laws and regulations (in relation to Article 7, Paragraph 2, Item (1)):

In cases based on laws and regulations, special care-required personal information may be acquired without obtaining the principal's consent in advance.

(2) Cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent (in relation to Article 7, Paragraph 2, Item (2)):

In cases in which there is a need to protect specific rights and interests such as a life, body or fortune of a person (including an entity), and when it is difficult to obtain a principal's consent, special care-required personal information may be acquired without obtaining the principal's consent in advance.

Case 1) When, for measures against improper acts, etc., a telecommunications carrier and another personal information handling business operator share information concerning anti-social forces such as an organized crime group or information concerning a person who intentionally engages in an obstruction of business where such information relates

to previous arrests, etc. for such obstruction of business.

Case 2) When information concerning the occurrence of a financial crime such as fraudulent transfer of funds is acquired from other business operators in order to prevent damage from a related crime.

(3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent (in relation to Article 7, Paragraph 2, Item (3)):

In cases in which there is a special need to enhance public hygiene or promote fostering healthy children in the process of developing mind and body, and when it is difficult to obtain a principal's consent, special care-required personal information may be acquired without obtaining the principal's consent in advance.

(4) Cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs (in relation to Article 7, Paragraph 2, Item (4)):

Where a private-sector corporation's cooperation is necessary in order for a central government organization, etc. (including a local government or a person entrusted by them) to perform affairs prescribed by laws and regulations, and when it is recognized that there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs, such private-sector corporation may acquire special care-required personal information without obtaining the principal's consent in advance.

Case) When a telecommunications carrier acquires special care-required personal information to submit such personal information at the discretionary request of the police.

(5) Cases in which the said special care-required personal information is open to the public by a principal, a government organization, a local government, a person set forth in each item of Article 76, paragraph (1) of the Act, or other persons specified by the Rules of the Personal Information Protection Committee (in relation to Article 7, Paragraph 2, Item (5)):

If special care-required personal information is open to the public by the following person, then such special care-required personal information may be acquired without obtaining the principal's consent in advance:

(i) a principal;
(ii) a government organization;
(iii) a local government;
(iv) a broadcasting institution, newspaper publisher, communication agency and other press organization (including an individual engaged in the press as his or her business);
(v) a person who practices writing as a profession;
(vi) a university and other organization or group aimed at academic studies, or a person belonging thereto;
(vii) a religious body;
(viii) a political body;
(ix) a foreign government, a foreign government agency, a local government in a foreign country, an international organization;
(x) a person equivalent to the person set forth in each item of Article 76, paragraph (1) of the Act.

(6) Cases in which seemingly-clear special care-required personal information is acquired by visual observation, filming or photographing of a principal (in relation to Article 7, Paragraph 2, Item (6)):

Regardless of a principal's intentions, any matter regarded as special care-required personal information is clear from the principal's physical characteristics (e.g. a physical disability, etc.), then such special care-required personal information may be acquired without obtaining the principal's consent in advance.

Case) When a physically handicapped person visits a store, and a clerk attending such person makes an entry in customer records to that effect (acquisition by eye sight) or such person's physical disability is caught in a security camera installed in such store (acquisition by video recording).

(7) When receiving the provision of special care-required personal information organized as personal data in those cases set forth in each item of Article 15, Paragraph 10 (in relation to Article 7, Paragraph 2, Item (7)):

When special care-required personal information is acquired due to an entrustment, business succession, or joint utilization as set forth in the respective items of Article 15, Paragraph 10, then such special care-required personal information may be acquired without obtaining the principal's consent in advance.

<Example of Violation of Article 7, Paragraph 2>

Acquisition of information concerning a principal's creed, criminal records, etc. from information made public on the Internet by a person other than those persons set forth in Article 7, Paragraph 2, Item (5), without obtaining the principal's consent, and registering the information so acquired in the database, etc. as part of information already held with regard to the principal.

(*1) For "special care-required personal information", see 2-4 (Special Care-Required Personal Information). Incidentally, for the third-party provision of special care-required personal information, the principal's consent is required as a general rule, and it should be kept in mind that the third-party provision through opt-out is not permitted (see 3-5-1 (Principle of Restrictions on Third-Party Provision) and 3-5-2 (Third-Party Provision through Opt-Out)).

(*2) For the "principal's consent", see 2-13 (Principal's Consent). Incidentally, where a telecommunications carrier appropriately acquires special care-required personal information directly from a principal in writing, orally, or otherwise, the provision of such information by the principal is interpreted as the principal's consent to the acquisition of such information by such telecommunications carrier. Furthermore, if a telecommunications carrier acquires special care-required personal information through the third-party provision, such acquisition is conditioned on such provider's acquisition of the principal's consent required pursuant to Article 7, Paragraph 2 and Article 15, Paragraph 1 (consent to the acquisition of special care-required personal information and the third-party provision), and accordingly, it is interpreted to mean that the personal information handling business operator which received such provision is not required to acquire the principal's consent under Article 7, Paragraph 2 again.

(For Reference)

Article 17 of the Act (paragraph (2))

(2) A personal information handling business operator shall, except in those cases set forth in the following, not acquire special care-required personal information without obtaining in advance a principal's consent.

(i) cases based on laws and regulations

(ii) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent

(iii) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent

(iv) cases in which there is a need to cooperate in regard to a central government organization

or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs

(v) cases in which the said special care-required personal information is being open to the public by a principal, a government organization, a local government, a person set forth in each item of Article 76, paragraph (1) or other persons prescribed by rules of the Personal Information Protection Commission

(vi) other cases prescribed by cabinet order as equivalent to those cases set forth in each preceding item

Article 6 of the Rules

A person prescribed by rules of the Personal Information Protection Commission under Article 17, paragraph (2), item (v) shall be a person falling under any of each following item.

(i) a foreign government, a foreign governmental organization, a local government in a foreign country, or an international organization

(ii) a person who is equivalent to a person set forth in each item of Article 76, paragraph (1) of the Act in a foreign country

Article 7 of the Cabinet Order

Those cases prescribed by cabinet order under Article 17, paragraph (2), item (vi) of the Act shall be those cases set forth in the following.

(i) cases in which seemingly-clear special care-required personal information is acquired by visual observation, filming or photographing of a principal;

(ii) when receiving the provision of special care-required personal information organized as personal data in those cases set forth in each item of Article 23, paragraph (5) of the Act.

3-2-4 Acquisition of Personal Information Protected under the Secrecy of Communications (in Relation to Article 7, Paragraph 3)

Article 7 (Paragraph 3)

3. Notwithstanding the provisions of the preceding paragraph, a telecommunications carrier shall not acquire personal information protected under the secrecy of communications except where the user’s consent has been obtained or where there is other justifiable cause for noncompliance with the law.

Notwithstanding the provisions of Article 7, Paragraph 2, if personal information is protected under the secrecy of communications, acquisition of such information is not allowed except where such corresponding person’s consent has been obtained or if there is justifiable cause for

noncompliance with the law.

(*) With regard to the consent concerning the handling of personal information protected under the secrecy of communications, see 2-13 (Principal's Consent).

3-2-5 Notification or Disclosure to the Public of Utilization Purpose (in Relation to Article 8, Paragraph 1)

Article 8 (Paragraph 1)
1. A telecommunications carrier shall, in case of having acquired personal information except in cases where a utilization purpose has been disclosed in advance to the public, promptly inform a principal of, or disclose to the public, the utilization purpose.

When a telecommunications carrier acquires personal information, it is desirable that the utilization purpose thereof is disclosed to the public (*1) in advance. If it is not disclosed to the public, the principal must be informed of the utilization purpose (*2) or the utilization purpose must be disclosed to the public promptly after the acquisition.

<Examples where Notice to the Principal or Disclosure to the Public is Required>

Case 1) Where personal information voluntary made public by the principal on the Internet is acquired (except where such information is merely viewed).

Case 2) Where personal information is acquired from the Internet, an Official Gazette, employee directory, etc. (except where such information is merely viewed).

Case 3) Where personal information is acquired through the third-party provision.

(*1) For "disclosure to the public", see 2-12 (Disclosure to the Public).

(*2) For "informing the principal", see 2-11 (Informing a Principal).

(For Reference)

Article 18 of the Act (paragraph (1))
(1) A personal information handling business operator shall, in case of having acquired personal information except in cases where a utilization purpose has been disclosed in advance to the public, promptly inform a principal of, or disclose to the public, the utilization purpose.

3-2-6 Direct Acquisition in Writing, etc. (in Relation to Article 8, Paragraph 2)

Article 8 (Paragraph 2)
2. A telecommunications carrier shall, notwithstanding the provisions under the preceding paragraph, in cases where it acquires, accompanied by concluding a contract with a principal, the principal's personal information stated in a written contract or other document (including an electromagnetic record; hereinafter the same in this paragraph) or other similar cases where it acquires directly from a principal his or her personal information stated in a written document, state a utilization purpose explicitly to the said principal. This, however, shall not apply in cases where there is an urgent need to protect a human life, body or fortune.

When a telecommunications carrier acquires personal information directly from a principal by way of an indication in a contract, prize entry postcard, or other document, electromagnetic records entered by a user on a computer screen, or otherwise, the telecommunications carrier must explicitly state (*) the utilization purpose of such personal information in advance.

Incidentally, in general practice, a business card, etc. presents a principal's personal information to the other party on the principal's volition in an arbitrary brief form, and unlike an application form, questionnaire, prize entry postcard, etc. by which a principal provides personal information as requested by a telecommunications carrier in a certain document or form prepared by it, and thus the obligations under this paragraph are not imposed with regard to a business card; however, the utilization purpose must be disclosed to the public in advance, or promptly after the acquisition, the principal must be informed of the utilization purpose thereof or the utilization purpose must be disclosed to the public (however, see 3-2-7 (Where Notification, etc. of Utilization Purpose is Not Required)). The foregoing also applies when such personal information is acquired orally.

Furthermore, in cases where there is an urgent need to protect a life, body or fortune of a person (including an entity), then the utilization purpose of personal information does not have to be clearly indicated to the principal in advance, but promptly after the acquisition, the principal must be informed of the utilization purpose thereof or the utilization purpose must be disclosed to the public (3-2-5 (Notification or Disclosure to the Public of Utilization Purpose)).

<Cases Where a Principal Must be Explicitly Stated of Utilization Purpose in Advance>

Case 1) Where an application form, contract, etc. containing a principal's personal information is acquired directly from the principal.

Case 2) Where personal information contained in a questionnaire is acquired directly from the principal.

Case 3) Where a person who wishes to participate in a campaign hosted by a company enters his/her personal information on a computer screen in the company's web page for the

participation, and the company acquires such personal information directly from the principal.

<Examples of Explicit Statements of Utilization Purpose>

Case 1) Where a contract or other document explicitly setting forth the utilization purpose is personally delivered or sent to the principal as a party to such contract.
Additionally, if the provisions regarding the utilization purpose are contained in a document (containing an electromagnetic record) such as contractual terms and conditions or terms of use, it is desirable to ensure that the principal will be able to actually recognize the utilization purpose, for instance, noting that the utilization purpose is set forth in contractual terms and conditions on the backside, or the utilization purpose set forth on the backside contractual terms and conditions being also set forth on the front, and such provisions being indicated at such location and in such character size as the principal can recognize it under social norms.

Case 2) Where on the network, the utilization purpose is explicitly stated on a company's webpages accessed by a principal or shown on a principal's terminal device.
Additionally, when personal information is acquired on the network, it is desirable to pay attention to the placement of the utilization purpose is so that the utilization purpose is noticed by the principal before clicking on the send button, etc. (including by creating a link or button so that the screen explicitly stating a description of the utilization purpose may be viewed in one action or so).

(*) An explicit statement of the utilization purpose to a principal" means explicitly stating the utilization purpose to a principal, and depending on the nature of business and how personal information is handled, such statement must be made in such reasonable and appropriate manner that the principal may recognize specifics.

(For Reference)

Article 18 of the Act (paragraph (2)) (2) A personal information handling business operator shall, notwithstanding the provisions under the preceding paragraph, in cases where it acquires, accompanied by concluding a contract with a principal, the principal's personal information stated in a written contract or other document (including an electromagnetic record; hereinafter the same in this paragraph) or other similar cases where it acquires directly from a principal his or her personal information stated in a written document, state a utilization purpose explicitly to the said principal. This, however, shall not apply in cases where there is an urgent need to protect a human life, body or fortune.

3-2-7 Where Notification, etc. of Utilization Purpose is Not Required (in Relation to Article 8, Paragraph 4)

Article 8 (Paragraph 4)

4. The provisions of the preceding three paragraphs shall not apply in those cases set forth in the following:
   (1) cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm a principal or third party's life, body, fortune or other rights and interests;
   (2) cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm the rights or legitimate interests of the said telecommunications carrier;
   (3) cases in which there is a need to cooperate in regard to a central government organization or a local government performing affairs prescribed by laws and regulations, and when there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would interfere with the performance of the said affairs;
   (4) cases in which it can be recognized, judging from the acquisitional circumstances, that a utilization purpose is clear.

In the cases set forth below, notification of the utilization purpose is not required even if notification of the utilization purpose by informing a principal (*1), disclosure to the public (*2), or explicit statement (*3) is required (hereinafter in this paragraph referred to as "Notification, etc. of the Utilization Purpose").

(1) Cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm a principal or third party's life, body, fortune or other rights and interests (in relation to Article 8, Paragraph 4, Item (1)):

If there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm a principal or third party's life, body, fortune or other rights and interests, Article 8, Paragraphs 1 through 3 shall not apply, and such Notification, etc., of the Utilization Purpose is not required.

(2) Cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm the rights or legitimate interests of the said telecommunications carrier (in relation to Article 8, Paragraph 4, Item (2)):

If there is a possibility that informing a principal of, or disclosing to the public, a utilization

purpose would harm the rights or legitimate interests of the said telecommunications carrier, Article 8, Paragraphs 1 through 3 shall not apply, and such Notification, etc., of the Utilization Purpose is not required.

Case) Where a company acquired information concerning an organized crime group or other anti-social forces, information concerning the subject of a report of a suspicious transaction, information concerning a rogue person who engages in an obstruction of business, etc., if the company acquiring such information may suffer damage if it becomes clear that such information has been obtained from the principal or other business operators.

(3) Cases in which there is a need to cooperate in regard to a central government organization or a local government performing affairs prescribed by laws and regulations, and when there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would interfere with the performance of the said affairs (in relation to Article 8, Paragraph 4, Item (3)):

If there is a need to cooperate in regard to a central government organization (including a local government or a person delegated by it) performing affairs prescribed by laws and regulations, and when there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would interfere with the performance of the said affairs, Article 8, Paragraphs 1 through 3 shall not apply, and such Notification, etc., of the Utilization Purpose is not required.

Case) Where without a public search, the police provide personal information concerning a suspect only to a telecommunications carrier with which the suspect may be involved, and if the telecommunications carrier which received such personal information notifies the principal of, or discloses to the public, the utilization purpose, the police's investigative activities may be obstructed.

(4) Cases in which it can be recognized, judging from the acquisitional circumstances, that a utilization purpose is clear (in relation to Article 8, Paragraph 4, Item (4)):

If it can be recognized, judging from the acquisitional circumstances, that a utilization purpose is clear, Article 8, Paragraphs 1 through 3 shall not apply, and such Notification, etc., of the Utilization Purpose is not required.

Case 1) Where personal information such as an address, telephone number, etc. is acquired in selling or providing products, services, etc., if the utilization purpose is just to sell or

provide such products, services, etc. surely.

Case 2) When business cards are exchanged in general practice, personal information such as a principal's name, affiliation, title, contact information, etc. is acquired directly from the principal, but the utilization purpose is for future contacts or to send brochures or emails for promotion and advertise of the affiliated company.

(*1) For "informing a principal", see 2-11 (Informing a Principal).

(*2) For "disclosure to the public", see 2-12 (Disclosure to the Public).

(*3) For "clear indication", see 3-2-6 (Direct Acquisition in Writing, etc.).

(For Reference)

Article 18 of the Act (paragraph (4))

(4) The provisions of the preceding three paragraphs shall not apply in those cases set forth in the following.

(i) cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm a principal or third party's life, body, fortune or other rights and interests

(ii) cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm the rights or legitimate interests of the said personal information handling business operator

(iii) cases in which there is a need to cooperate in regard to a central government organization or a local government performing affairs prescribed by laws and regulations, and when there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would interfere with the performance of the said affairs

(iv) cases in which it can be recognized, judging from the acquisitional circumstances, that a utilization purpose is clear

3-3 Management of Personal Data, etc. (in Relation to Articles 9 through 13)

3-3-1 Assurance, etc. about the Accuracy of Data Contents (in Relation to Article 9)

Article 9

A telecommunications carrier shall strive to keep personal data accurate and up to date within the scope necessary to achieve a utilization purpose.

A telecommunications carrier must strive to keep personal data accurate and up to date within the scope necessary to achieve a utilization purpose, *inter alia* by establishing procedures for collation and check in entering personal information into personal information data base, etc., establishing procedures for correction, etc. upon detecting an error, etc., and updating recorded

matters, etc.

Incidentally, it is not necessary to update retained personal data uniformly or at all times, and it is sufficient to ensure the accuracy and currentness to the extent necessary for each utilization purpose.

(For Reference)

Article 19 of the Act
A personal information handling business operator shall strive to keep personal data accurate and up to date within the scope necessary to achieve a utilization purpose, and to delete the personal data without delay when such utilization has become unnecessary.

3-3-2 Retention Period, etc. (in Relation to Article 10, Paragraph 1)

Article 10 (Paragraph 1)
1. A telecommunications carrier shall, in handling personal data (excluding those protected under the secrecy of communications; the same shall apply hereinafter in this Article), determine a retention period to the extent necessary for the utilization purpose and strive to delete such personal data without delay after the expiration of such retention period or after such utilization has become unnecessary. This, however, shall not apply to the following cases: (1) when the retention is required under the provisions of laws and regulations; (2) when a principal's consent has been obtained; (3) where personal data is retained by a telecommunications carrier to the extent necessary for the execution of its business, when there is a reasonable ground for not deleting such personal data; (4) other than the cases set forth in the preceding three items, when there is a special reason for not deleting such personal data.

When it becomes unnecessary to use retained personal data, i.e., when the utilization purpose has been achieved and there no longer exist reasonable grounds to retain the personal data in relation to such utilization purpose, or when the operation itself as the basis of such purpose is suspended even though such utilization purpose has not been achieved, then it is appropriate to delete such personal data without delay (*). From the perspective of ensuring such intent, a telecommunications carrier must strive to set a retention period based on the utilization purpose. Furthermore, if it becomes no longer necessary to use such retained personal data during the retention period, such telecommunications carrier must strive to delete such personal data at such point in time.

On the other hand, because there may be personal data as to which it is difficult to set a

retention period, setting a retention period for all kinds of personal data is not required; however, even in such situation, the telecommunications carrier must strive to delete the personal data without delay after the utilization purpose is achieved.

However, this provision shall not apply to the cases set forth in the respective items of Article 10, Paragraph 1 or to personal data protected under the secrecy of communications.

<Cases where it is deemed that it has become no longer necessary to use personal data>

Case) Where personal data of applicants for a campaign are retained in order to send prizes in such campaign, when all such prizes are sent out, and a reasonable period for handling of non-delivery, etc. has elapsed.

(*) "Deletion of personal data" means an action of making such personal data unusable as personal data and includes not only deletion of such personal data but also deidentification of such personal data.

On the other hand, in the following cases, personal data may be kept undeleted even after the expiration of the retention period or after the utilization purpose is achieved.

(1) When the retention is required under the provisions of laws and regulations (in relation to Article 10, Paragraph 1, Item (1)):

When the retention is required under the provisions of laws and regulations, such as Article 126 of the Corporation Tax Act (Act No. 34 of 1965), Article 59 of the Regulation for Enforcement of the Corporation Tax Act (Order of the Ministry of Finance No. 12 of 1965), and Article 4 of the Regulation of Enforcement of the Act on Temporary Special Measures for Telephone Subscriber's Right (Order of the Ministry of Posts and Communications No. 18 of 1958), personal data may be kept undeleted even after the expiration of the retention period or after the utilization purpose is achieved.

(2) When a principal's consent has been obtained (in relation to Article 10, Paragraph 1, Item (2)):

When a principal's consent has been obtained (*), such as where the principal makes a particular request, his/her personal data may be kept undeleted even after the expiration of the retention period or after it becomes no longer necessary to use such personal data.

(*) For the "principal's consent", see 2-13 (Principal's Consent).

(3) Where personal data is retained by a telecommunications carrier to the extent necessary for

the execution of its business, when there is a reasonable ground for not deleting such personal data (in relation to Article 10, Paragraph 1, Item (3)):

Where personal data is retained by a telecommunications carrier to the extent necessary for the execution of its business, when there is a reasonable ground for not deleting such personal data (for instance, when information concerning a person whose use of a service was suspended due to delinquency of fees in the past is retained even after his/her contract is terminated), such personal data may be kept undeleted even after the expiration of the retention period or after it becomes no longer necessary to use such personal data.

(4) Other than the cases set forth in the preceding three items, when there is a special reason for not deleting such personal data (in relation to Article 10, Paragraph 1, Item (4)):

When there is a special reason for not deleting personal data (for instance, when an investigative authority requests for preservation of certain personal data which may be used as evidence in a criminal case), such personal data may be kept undeleted even after the expiration of the retention period or after the utilization purpose is achieved.

(For Reference)

Article 19 of the Act
A personal information handling business operator shall strive to keep personal data accurate and up to date within the scope necessary to achieve a utilization purpose, and to delete the personal data without delay when such utilization has become unnecessary.

3-3-3 Exception to Personal Information Protected the Secrecy of Communications during the Retention Period, etc. (in Relation to Article 10, Paragraph 2)

Article 10 (Paragraph 2)
2. Except where the user's consent has been obtained or if there is other justifiable cause for noncompliance with the law, a telecommunications carrier shall not retain personal information protected under the secrecy of communications, and even if such retention is permitted, a telecommunications carrier shall delete such personal information promptly after the utilization purpose is achieved.

Except where the user's consent has been obtained or if there is other justifiable cause for noncompliance with the law, a telecommunications carrier must not retain personal information protected under the secrecy of communications, as a general rule, because the recording of such information needs to be minimized, and even if such retention is permitted, a telecommunications

carrier must not store such information beyond the extent of the corresponding person's consent or the extent necessary for the purpose of such storage and must delete such personal information promptly (including deletion of information protected by the secrecy of communications as well as deidentification of personal information not covered by the secrecy of communications) after the utilization purpose is achieved.

(*) With respect to the consent concerning the handling of personal information protected under the secrecy of communications, see 2-13 (Principal's Consent). For the preservation of communications history, see 5-1 (Recording of Communications History).

3-3-4 Security Control Action (in Relation to Article 11)

Article 11

A telecommunications carrier shall take necessary and appropriate action for the security control (hereinafter referred to as "security control action") of personal data or personal information protected under the secrecy of communications (hereinafter referred to as "personal data, etc.") including preventing the leakage, loss or damage of its handled personal data, etc.

A telecommunications carrier must take necessary and appropriate action for the security control (hereinafter referred to as "security control action") of personal data or personal information protected under the secrecy of communications (hereinafter referred to as "personal data, etc.") including preventing the leakage, loss or damage (hereinafter referred to as "leakage, etc.") of its handled personal data, etc., and such action must be determined with necessary and appropriate specifics, taking into consideration the scale of potential damage to be inflicted on the rights and interests of the principal in the event of leakage, etc., of personal data, etc. and depending on risks associated with the size and nature of business, the way personal data, etc. are handled (including the nature and quantity of personal data, etc. handled), and the nature, etc. of a medium in which personal data, etc. are recorded. For specifics of the action required to be taken and illustrations of methods to implement such items, see "7 (Attachment) Specifics of Security Control Action Required to be Taken".

Additionally, it is desirable to take such security control action with respect to personal information which is not part of personal data, etc. (so-called scattered information) because such information can be recognized as information associated with the secrecy of communications.

Furthermore, in taking such security control action, the Standards for Safety and Reliability of Information and Telecommunications Networks (Ministry of Posts and Communications Public Notice No. 73 of 1987) shall be utilized. Additionally, it is also necessary to note that, with respect to technical protection measures for telecommunications facilities for telecommunications

business (telecommunications facilities for telecommunications business of providing telecommunications line facilities and universal telecommunications services), a telecommunications carrier which runs such telecommunications facilities for telecommunications business has the duty to maintain such facilities to conform to the technical standards set forth in the Regulations for Telecommunications Facilities for Telecommunications Business (Order of the Ministry of Posts and Communications No. 30 of 1985) (Article 41 of the Telecommunications Business Act).

(For Reference)

Article 20 of the Act A personal information handling business operator shall take necessary and appropriate action for the security control of personal data including preventing the leakage, loss or damage of its handled personal data.

3-3-5 Supervision over Employees (in Relation to Article 12, Paragraphs 1 and 2)

Article 12 (Paragraphs 1 and 2) 1. A telecommunications carrier shall, in having its employees (including dispatched workers; the same shall apply hereinafter) handle personal data, etc., exercise necessary and appropriate supervision over the employees so as to seek the security control of the personal data, etc. 2. A telecommunications carrier shall strive to provide necessary education and training to its employees for the purpose of taking security control action and otherwise ensuring proper handling of personal data, etc.

A telecommunications carrier shall, in having its employees handle personal data, etc., exercise necessary and appropriate supervision over its employees so as to make them comply with the security control action under Article 11. In that respect, necessary and appropriate measures, such as satisfactory substance and frequency of education and training of its employees handling personal data, etc., must be taken, taking into consideration the scale of potential damage to be inflicted on the rights and interests of a principal in the event of leakage, etc., of personal data, etc. and depending on risks associated with the size and nature of business and the way personal data, etc. are handled (including the nature and quantity of personal data, etc. handled).

The term “employees” refers to those who engage in a telecommunications carrier’s operations as directed and supervised by the telecommunications carrier, directly or indirectly, within the organization of the telecommunications carrier, and such term includes not only employees in an employment relationship (such as full-time employees, contractual employees, commissioned employees, part-time workers, and temporary employees) but also directors,

executive officers, board members, statutory auditors, auditors, and dispatched workers.

<Examples of cases where necessary and appropriate supervision is not being exercised over employees>

Case 1) When a leakage of personal data, etc. occurs as a result of the failure to ensure that the employees are conducting business activities in accordance with the regulations, etc. setting forth security control actions for personal data, etc.

Case 2) When a leakage of personal data, etc. occurs where a notebook PC or external storage unit containing personal data, etc. is removed out of a workplace repeatedly in violation of internal regulations, etc., and as a result of overlooking such actions, such PC or storage unit is lost.

(For Reference)

Article 21 of the Act A personal information handling business operator shall, in having its employees handle personal data, exercise necessary and appropriate supervision over the employees so as to seek the security control of the personal data.

3-3-6 Supervision over Contractors (in Relation to Article 12, Paragraph 3)

Article 12 (Paragraph 3) 3. A telecommunications carrier shall, in case of entrusting a whole or part of the handling of personal data, etc., exercise necessary and appropriate supervision over an entrusted person so as to seek the security control of the personal data, etc., of which the handling has been entrusted.

A telecommunications carrier must, in case of entrusting (*1) a whole or part of the handling of personal data, etc., exercise necessary and appropriate supervision over an entrusted person (hereinafter referred to as "contractor") so as to seek appropriate security control of such personal data, etc. Specifically, a telecommunications carrier shall exercise supervision to ensure that its contractors will take security control actions equivalent to those required to be taken by such telecommunications carrier under Article 11 (*2).

In that respect, obviously, a telecommunications carrier must try not to provide to a contractor personal data, etc. that are not necessary for services entrusted to such contractor, and the telecommunications carrier must also take necessary and appropriate actions described in (1) through (3) below, taking into consideration the scale of potential damage to be inflicted on the rights and interests of a principal in the event of leakage, etc., of personal data, etc. in light of the substance of personal data, etc. of which the handling is entrusted, and depending on risks

associated with the size and nature of entrusted business, and the way personal data, etc. are handled (including the nature and quantity of personal data, etc. handled) (*3).

(1) Selection of an appropriate contractor:

In selecting a contractor, a telecommunications carrier must confirm in advance that, in order to ensure that the security control actions of the contractor are at least equivalent to those the telecommunications carrier are expected to take under Article 20 of the Act and the Guidelines, the respective items set forth in "7 (Attachment) Specifics of Security Control Action Required to be Taken" will be taken in line with the services to be entrusted, and must check the contractor's system, regulations, etc. in that regard by visiting a place at which personal data, etc. are handled or otherwise using reasonable means, as necessary.

(2) Execution of an entrustment agreement:

It is appropriate that an entrustment agreement duly sets forth the following matters: security control actions (clear indication as to who handles personal data, etc. at the contractor (including those who are not workers of the contractor), and specifics of security control actions required to be taken at the contractor, among other matters); confidentiality; terms of subcontracting (matters such as whether subcontracting is permitted, and if permitted, selection by the subcontractor of those who are regarded as properly handling personal data, etc., prior notification to, or approval by, the telecommunications carrier with regard to such subcontracting, and supervision over the subcontractor; it is noted that if any further subcontracting is allowed, terms for selecting and supervising any such further contractor must be prescribed); handling of personal data, etc. at the end of the entrustment agreement (return, deletion, etc., of personal data, etc.); actions to be taken in the event of failure to comply with the contractual terms (for instance, matters concerning damages in the event of failure to comply with security control matters and any resulting leakage of personal data, etc., and termination upon discovery of any deficiency in the security control actions); and other matters relating to the handling of personal data, etc. In addition, it is desirable that an entrustment agreement contains a provision to the effect that the entrusting party reasonably keeps track of how the contractor handles personal date, etc. entrusted.

(3) Keeping track of the way the contractor handles personal data, etc.:

In order to keep track of the way the contractor handles personal data, etc., it is desirable that the entrusting party conducts an audit on a regular basis or otherwise examines the extent of implementation of the terms of the entrustment agreement, and makes an appropriate evaluation, including reexamination of the terms of the entrustment.

Additionally, when the contractor intends to carry out subcontracting, it is desirable that, as with the initial entrustment, the entrusting party will be notified in advance by the contractor of, or approve, the subcontractor, specifics of the services to be further entrusted, and how such subcontractor will handle personal data, etc.; that the entrusting party will supervise, as necessary, or have the contractor supervise, such subcontractor by conducting an audit on a regular basis, and the contractor will otherwise appropriately supervise the subcontractor, appropriately fulfilling the contractor's supervision over the subcontractor; and that the entrusting party will sufficiently confirm that security control actions under Article 11 are taken (*4). When the subcontractor makes even further entrustment, the foregoing shall apply.

<Examples of cases where necessary and appropriate supervision is not being exercised over the contractor>

Case 1) Where the entrusting party entrusts any service to an outside vendor without checking its security control actions for personal data, etc. at the time of executing a contract or thereafter, as appropriate, and the contractor consequently leaks personal data, etc.

Case 2) Where the entrusting party fails to give the contractor instructions as to specifics of necessary security control actions relating to the handling of personal data, etc., and the contractor consequently leaks personal data, etc.

Case 3) Where the entrusting party fails to give the contractor instructions relating to conditions of subcontracting and to check how the contractor handles personal data, etc., and the contractor further entrusts the processing of personal data, etc., and such subcontractor consequently leaks personal data, etc.

Case 4) Where, despite the fact that a contract sets forth that the entrusting party shall keep track of how the contractor checks the subcontracting, the entrusting party fails to take necessary measures such as asking the contractor to give notice of subcontracting, and subcontracting is carried out without the entrusting party's knowledge, and such subcontractor consequently leaks personal data, etc.

(*1) "Entrustment of the handling of personal data, etc." refers to a personal information handling business operator's having another person handle personal data, etc., regardless of the form and type of such contract. Specifically, it is anticipated that entry (including acquisition from a principal), editing, analysis, and other processing of personal data, etc. will be entrusted.

(*2) It is not intended that, if the entrusting party takes security control actions at a high level exceeding the level sought in Article 11, it is not expected that the contractor is also required to take security control actions at the same level, and it means that it is sufficient if the contractor takes security control actions sought in Article 11.

(*3) In selecting a contractor or keeping track of how the contractor handles personal data, etc., it is necessary to adopt an appropriate method, depending on the substance or size of personal data, etc. of which the handling is entrusted. For instance, such confirmation may be made by visiting a place at which personal data, etc. are handled or otherwise using reasonable means (including verbal confirmation), as necessary.

(*4) Where the entrusting party fails to exercise "necessary and appropriate supervision" on the contractor, if the contractor carries out subcontracting and the subcontractor makes inappropriate handling, then the initial entrusting party will be held liable for a violation of laws. Accordingly, subcontracting requires attention.

(For Reference)

Article 22 of the Act

A personal information handling business operator shall, in case of entrusting a whole or part of the handling of personal data, exercise necessary and appropriate supervision over an entrusted person so as to seek the security control of the personal data of which the handling has been entrusted.

3-3-7 Personal Information Protection Manager (in Relation to Article 13)

Article 13

A telecommunications carrier shall strive to appoint a personal information protection officer (which refers to a person who is in charge of the handling of personal data, etc. for such telecommunications carrier), and to have such officer implement internal regulations, establish an audit system, and oversee such telecommunications carrier's handling of personal data, etc. for compliance with these Guidelines.

In order to clarify who is responsible for executing protection measures for personal data, etc. and establish the telecommunications carrier's internal responsibility structure regarding the implementation of security control actions under Article 11 and other appropriate handling of personal data, etc., the telecommunications carrier must strive to appoint a person who is able to oversee the handling of personal data, etc. for such telecommunications carrier throughout the organization, such as an officer who has the necessary authority (personal information protection manager), and to have such manager take responsibility for necessary supervision, etc. over the handling of personal data, etc.

Additionally, the appointment of a personal information protection manager is important in clarifying who is responsible, especially for the purpose of preventing a leakage, etc., of personal

data, etc. due to misconduct inside and outside the telecommunications carrier. Furthermore, it is desirable that the personal information protection manager includes actions prescribed in "7 (Attachment) Specifics of Security Control Actions Required to be Taken" in drawing up internal regulations and establishing an audit system.

3-4 Privacy Policy (in Relation to Article 14)

3-4-1 Disclosure of Privacy Policy to the Public (in Relation to Article 14, Paragraph 1)

Article 14 (Paragraph 1)
1. It is appropriate for a telecommunications carrier to disclose to the public a privacy policy (which refers to a concept or policy under which such telecommunications carrier promotes the protection of personal information).

In order for a telecommunications carrier to gain social trust in respect of the protection of personal information, it is appropriate for the telecommunications carrier to disclose and declare to the public its concept or policy under which it promotes the protection of personal information, as a privacy policy.

Each telecommunications carrier is expected to present a privacy policy in expressions that easy to understand, and the matters that are required to be included in such privacy policy may include the following:

(1) Compliance with the Act, and the provisions of the Telecommunications Business Act relating to the secrecy of communications as well as other relevant laws and regulations
(2) Compliance with the Guidelines
(3) Matters required to be disclosed to the public as set forth in the respective items in Article 19, Paragraph 1
    (i) Name or appellation of the said telecommunications carrier
    (ii) Utilization purpose of retained personal data
    (iii) Notification or disclosure of the utilization purpose or procedures for responding to a principal's request for correction, etc.
    (iv) Where to lodge a complaint
    (v) Appellation of an accredited personal information protection organization and where to lodge a petition for resolving a complaint
(4) Policy relating to the security control actions under Article 11
(5) Matters concerning the protection of rights and interests of users
    (i) Upon a principal's request with regard to retained personal data, the telecommunications carrier will suspend sending direct mail or otherwise suspend the use of such information on its own volition.

(ii) The telecommunications carrier will clearly indicate whether any service is outsourced and what service is outsourced, and otherwise enhance transparency with regard to outsourcing.
(iii) The telecommunications carrier will indicate the utilization purpose separately for each type of users in view of its operations, make efforts on its own volition to limit the utilization purpose at a principal's choice, or otherwise make the utilization purpose clearer for a principal.
(iv) The telecommunications carrier will clearly indicate the source of personal information and how it is acquired (such as the type of the source) as specifically as possible.

In addition to the above, it must be noted that the following matters are required to be announced or disclosed to the public in a privacy policy or put into a state where a principal can know in a privacy policy, etc.: utilization purpose for acquisition (Article 1, Paragraphs 1 and 3); items of personal data when personal data is provided to third parties through opt-out (Article 15, Paragraphs 2, 3 and 9); items of personal data to be shared in joint utilization (Article 15, Paragraph 10, Item (3), and Paragraph 11); items of information included in anonymously processed information (Article 28, Paragraphs 3, 4, 5 and 7, and Article 29); and security control actions, etc. for anonymously processed information at an anonymously processed information handling business operators (Article 31).

(For Reference)

Basic Policy on the Protection of Personal Information (Cabinet Decision of April 2, 2004)

6 Basic matters concerning actions for protection of personal information to be taken by personal information handling business operator etc.

(1) Matters concerning personal information handled by personal information handling business operator etc.

Personal information handling business operators are expected to voluntarily make efforts, in line with the Personal Information Protection Commission's Guidelines and Accredited Personal Information Protection Organizations' Personal Information Protection Guidelines mentioned 2 (2) (i), for protection of personal information, and appropriate and effective utilization of personal information, such as externally clarifying ideas or policies on facilitating protection of personal information (so-called privacy policies, privacy statements) from the viewpoint of further protection of consumers' rights, in addition to complying with the law, and they are required to proactively establish a system. In so doing, it is important for each business operator to take appropriate actions according to the volume and nature of the business, the handling status of the personal data, and etc.

3-4-2 Privacy Policy for Application Software (in Relation to Article 14, Paragraphs 2 and 3)

Article 14 (Paragraphs 2 and 3)

2. Where a telecommunications carrier makes available application software (hereinafter referred to as an "application"), it is appropriate to disclose to the public a privacy policy which clearly and appropriately provides for collection, etc. of information through such application.
3. Where a telecommunications carrier operates a site at which an application is made available, it is appropriate to encourage the party making such application available at such site to disclose to the public a privacy policy which clearly and appropriately provides for collection, etc. of information through such application.

Application software (hereinafter referred to as "application") refers to software which executes various functions such as calls, communications, and other communication tools, photographs, and games. In a smart device such as a smartphone, it is possible to expand or customize functions by installing an application.

Because some applications collect various types of information and send the same to the outside, when a telecommunications carrier makes such application available, it is appropriate, from the perspective of protecting users' privacy by ensuring transparency and opportunities for users' involvement, to disclose to the public a privacy policy which clearly and appropriately provides for collection, etc. of information through such application (in relation to Article 14, Paragraph 2).

Furthermore, when a telecommunications carrier operates a site at which an application is made available, it is appropriate to encourage the party making such application available at such site (other than the telecommunications carrier itself) to disclose to the public a privacy policy which clearly and appropriately provides for collection, etc. of information through such application (in relation to Article 14, Paragraph 3).

Matters required to be indicated in a privacy policy for an application may include the matters set forth below.

(i) Name or appellation of the party making available an application that collects information
(ii) Items of information to be collected
(iii) How the information is collected
(iv) Specification and explicit statements of the utilization purpose
(v) How to notify or disclose to the public, how to obtain a consent, and how to involve a user
(vi) Whether information may be sent to the outside, whether information may be provided to third parties, or whether any information collection module is used
(vii) Contact information

(v) Procedures for amendment to the privacy policy

Furthermore, in order to ensure that the substance of such privacy policy appropriately sets forth matters such as collection of information by such application, it is desirable for a telecommunications carrier to verify the appropriateness by using a third-party verification, etc.

Other details concerning a privacy policy for an application shall conform *inter alia* to the Smartphone Privacy Initiative (by the Study Group on Examining Issues around ICT Services from the User Perspective in August 2012).

Additionally, the Guidelines are intended for telecommunications carriers and accordingly describe the efforts on the part of telecommunications carriers, but the efforts to disclose to the public a privacy policy which clearly and appropriately provides for collection, etc. of information through such application shall also apply to concerned parties such as application providers, information collection module providers, application provision site operators, and OS providers, respectively. It is expected that the initiatives described in this Article as those on the part of telecommunications carriers will contribute to the promotion of such efforts on the part of such respective concerned parties.

3-5 Provision of Personal Data to Third Parties (in Relation to Articles 15 through 18)

3-5-1 Principle of Restrictions on Third-Party Provision (in Relation to Article 15, Paragraph 1)

Article 15 (Paragraph 1)

1. A telecommunications carrier shall, except in those cases set forth in the following, not provide personal data to a third party without obtaining in advance a principal's consent:
   (1) cases based on laws and regulations;
   (2) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent;
   (3) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent;
   (4) cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs.

A telecommunications carrier must not provide personal data to a third party without obtaining a principal's consent (*1) in advance (*2) (*3). In obtaining such consent, details of such provision must be clearly indicated to the principal to the extent reasonable and appropriate for the principal to make a decision to give the consent, depending on the scale and nature of

business and how personal data are handled (including the nature and quantity of personal data handled) among other things.

Additionally, if it is anticipated in advance that personal information will be provided to a third party, such provision must be specified in a description of the utilization purpose (see 3-1-1 (Specifying a Utilization Purpose)).

<Examples of third-party provision> (except for the cases under the respective items of Article 15, Paragraph 10)

Case 1) When personal data are exchanged among parent companies, subsidiaries, sister companies, or group companies.

Case 2) When personal data are exchanged between the headquarters of a franchising organization and franchisees.

Case 3) When specific personal data are exchanged between telecommunications carriers.

<Examples of a case which is not recognized as a third-party provision> (Provided that this is subject to a limitation by the utilization purpose.)

Case) When, within the same telecommunications carrier, personal data are provided by one department to another department.

However, a principal's consent is not required for a third-party provision of personal data in the cases described in following (1) through (4). Incidentally, for specific examples, see 3-1-6 (Exceptions to Restrictions by Utilization Purpose).

(1) Cases based on laws and regulations (in relation to Article 15, Paragraph 1, Item (1)):

With regard to the "cases based on laws and regulations", when a search, seizure, etc. is made as a compulsory disposition based on a warrant issued by a judge, the provision of the relevant information may not be refused so long as such information is provided to the extent specified by the warrant.

On the other hand, when an inquiry is made by a person who has the legal authority to make such inquiry (for instance, pursuant to Article 197, paragraph (2) of the Code of Criminal Procedure, Article 6-4 of the Juvenile Act, Article 23-2, paragraph (2) of the Attorney Act, and Article 29 of the Act on Regulation of Transmission of Specified Electronic Mail (Act No. 26 of 2002); hereinafter referred to as the "Specified Electronic Mail Act")), the telecommunications carrier should respond to such inquiry as a general rule, but because the telecommunications carrier is also obligated to protect the secrecy of communications, it is not appropriate, as a general rule, to provide information regarding matters protected by the secrecy of communications (including not only the contents of communications, but also the elements of communications

such as the corresponding person's name and address, location of transmission or receipt, date of transmission as well as the number of transmissions and whether there was any transmission). Additionally, because the name, address, etc. of subscribers which are not related to individual transmissions are outside the scope of protection under the secrecy of communications, a telecommunications carrier may basically respond to an inquiry made by a person who has the legal authority to make such inquiry. However, because a determination of whether or not any individual transmission is unrelated may depend on the way such inquiry is made, and for that reason, if it appears in the process of an inquiry that any item of the inquiry closely relates to any individual transmission, then it is appropriate to treat such transmission as protected under the secrecy of communications (*4).

In either case, so that the rights and interests of a principal, etc. would not be unreasonably infringed, such provision, etc. should be limited to a portion specified in a warrant, inquiry, etc., or otherwise limited to the minimum necessity in line with the intent of such provision, and it is not appropriate to make a general and comprehensive provision.

(2) Cases in which the provision of personal data is necessary given a threat of infringement on specific rights and interests such as a life, body or fortune of a person (including an entity), and when it is difficult to obtain a principal's consent (in relation to Article 15, Paragraph 1, Item (2))

(3) Cases in which there is a special need to enhance public hygiene or promote fostering healthy children in the process of developing mind and body, and when it is difficult to obtain a principal's consent (in relation to Article 15, Paragraph 1, Item (3))

(4) Cases in which there is a need to obtain a private-sector corporation's cooperation where a central government organization, etc. performs affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent to such cooperating private-sector corporation's provision of personal data to such central government organization, etc. would interfere with the performance of the said affairs (in relation to Article 15, Paragraph 1, Item (4))

(*1) For the "principal's consent", see 2-13 (Principal's Consent).

(*2) With regard to information containing personal data posted on a blog or other SNS, such information is published for a large number of unspecified persons or a limited target with a clear intention of the person who posted such information, and because the person who posted such information designates who may view such content and because there is no discretion as to the scope of such publication on the part of the service provider of the Internet connection service or the

operator of a blog or other SNS, such business operator is not interpreted as providing personal data to a third party.

(*3) If any person who is or was a telecommunications carrier or its employee provides or misappropriates a personal information database, etc. (including those reproduced or processed in whole or in part) which such person handles or handled in relation to its/his/her business activities, for the purpose of making for its/his/her own benefit or for a third party's benefit improperly, then such act is subject to a criminal punishment (imprisonment with work for not more than one year or a fine of not more than 500,000 yen) under Article 83 of the Act.

(*4) There may be a case where, pursuant to a sender information disclosure request under Article 4 of the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Act No. 137 of 2001), a telephone number held by a business operator (content provider (CP)) which provided a site or service in which infringing information was posted is disclosed to the person who requested such telephone number (i.e., the person who alleges that its/his/her right was infringed due to the distribution of such information through a specified telecommunications service), and then for the purpose of specifying a sender of such infringing information, an attorney-at-law representing such person makes a request to the relevant telecommunications carrier which provides telephone services (hereinafter referred to as the "telephone company") based on such telephone number, asking for submission of the address and name of the subscriber associated with such telephone number through an inquiry pursuant to Article 23-2, paragraph (2) of the Attorney Act (hereinafter referred to as the "bar association inquiry").

In such event, for such telephone company, the posting of such infringing information is not an individual transmission in the telephone service provided by it, and such bar association inquiry is not intended to reveal senders of individual transmissions in the telephone service provided by such telephone company, and accordingly, the telephone company is not regarded as breaching the secrecy of communications in responding to such inquiry.

(For Reference)

Article 23 of the Act (paragraph (1))
(1) A personal information handling business operator shall, except in those cases set forth in the following, not provide personal data to a third party without obtaining in advance a principal's consent.

(i) cases based on laws and regulations
(ii) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent
(iii) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent
(iv) cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs

3-5-2 Third-Party Provision through Opt-Out (in Relation to Article 15, paragraphs (2) through (7) and (9) of the Act)

3-5-2-1 Principles Regarding Opt-Out (in Relation to Article 15, Paragraphs 2, 4 through 7, and 9)

Article 15 (Paragraphs 2, 4, 5, 6, 7 and 9)

2. A telecommunications carrier, in regard to personal data provided to a third party (excluding special care-required personal information; hereinafter the same in this paragraph), may, in cases where it is set to cease in response to a principal's request a third-party provision of personal data that can identify the principal and when it has in advance informed a principal of those matters set forth in the following or put them into a state where a principal can easily know, and notified them to the Personal Information Protection Commission pursuant to the provisions of Article 23, paragraph (2) of the Act, provide the said personal data to a third party notwithstanding the provisions of the preceding paragraph:
   (1) to set a third-party provision as a utilization purpose;
   (2) the categories of personal data provided to a third party;
   (3) a method of a third-party provision;
   (4) to cease, in response to a principal's request, a third-party provision of personal data that can identify the principal;
   (5) a method of receiving a principal's request.
4. Action for informing or putting into a state where a principal can easily know pursuant to the provisions of the preceding two paragraphs shall be carried out as set forth in the following:
   (1) setting a necessary period for a principal identifiable by the provided personal data (referred to as the "principal" in the next following item) to request the provision to be ceased;

(2) adopting an appropriate and reasonable method to enable the principal to recognize without fail a matter set forth in each item of Paragraph 2.

5. A notification pursuant to the provisions of Paragraph 2 or 3 shall be given by any of each method set forth in the following:
   (1) a method using an electronic data processing system (meaning an electronic data processing system connecting a computer relating to use by the Personal Information Protection Commission and a computer relating to use by a notifying person via electronic telecommunication line) as prescribed by the Personal Information Protection Commission;
   (2) a method submitting a written notification in Form No. 1 appended to the Enforcement Rules for the Act on the Protection of Personal Information (Personal Information Protection Commission Rules No. 3 of 2016; hereinafter referred to as the "Rules") and an optical disc (including an object that can assuredly keep a record of certain matters by an equivalent method to such an optical disc; hereinafter referred to as an "optical disc, etc.") that has kept a record of a matter to be stated in the written notification.
6. A telecommunications carrier shall, in case of giving a notification pursuant to the provisions of Paragraph 2 or 3 by an agent, submit to the Personal Information Protection Commission a document verifying the power of agency in Form No. 2 appended to the Rules.
7. A telecommunications carrier in a foreign county (meaning a country or region located outside the territory of Japan; hereinafter the same) shall, in case of giving a notification pursuant to the provisions of Paragraph 2 or 3, appoint a person domiciled in Japan who has the authorization to act for the telecommunications carrier on any action relating to the notification. In this case, the said telecommunications carrier shall submit a document (including texts translated into Japanese) verifying that it has conferred the power of agency on the person domiciled in Japan to the Personal Information Protection Commission at the same time of giving the said notification.
9. A telecommunications carrier shall, promptly after public disclosure pursuant to the provisions of Article 23, paragraph (4) of the Act has been made, disclose to the public those matters set forth in Paragraph 2 (when a matter set forth in Item (2), (3) or (5) has been modified, a post-modified matter set forth in each said item) by utilizing the Internet or other appropriate method.

In providing personal data to a third party, when a telecommunications carrier has in advance (*1) informed a principal of those matters set forth in following (1) through (5) or put them into a state where a principal can easily know (*2), and notified them to the Personal Information Protection Commission pursuant to the provisions of Article 23, paragraph (2) of the Act (*3),

then notwithstanding the provisions of Article 15, Paragraph 1, such telecommunications carrier may provide the said personal data to a third party (*5) without obtaining the principal's consent (*4) in advance (third-party provision through opt-out). On the other hand, when a telecommunications carrier provides its subscriber's personal data to a third party, it is generally possible to obtain the principal's consent under contractual terms and conditions, and basically, it is desirable that such provision is made upon obtaining the principal's consent. However, even where the principal's consent has been obtained under contractual terms and conditions for such purpose, with regard to the inclusion in a telephone directory and such other matters as to which the principal's intention should be respected, it is desirable to have an arrangement that any such provision shall be ceased upon the principal's request.

Pursuant to Article 15, Paragraph 2, when a telecommunications carrier notifies necessary matters to the Personal Information Protection Commission, it shall also disclose such matters to the public (*6) by using the Internet or such other appropriate method.

Incidentally, it must be kept in mind that special care-required personal information may not be provided to a third party by opting out, and in providing such information to a third party, a principal's consent must be obtained in advance without fail unless any of the respective items of Article 15, Paragraph 1 or the respective items of Article 15, Paragraph 5 applies.

(1) To set a third-party provision as a utilization purpose:

The utilization purpose must be described in specific terms. Use of vague expressions such as "etc." or "... and any other ..." is undesirable.

Case 1) Provision of personal data to a third party by creating and selling a residential map, residential map database, and products relating to residential map (including a delivery service thereof).

Case 2) Provision of personal data to a third party by creating and selling a list of people in a certain age group, wealthy individuals, healthy food purchasers, alumni association, attorneys-at-law, real estate investors, or condominium owners.

(2) Categories of personal data provided to a third party:

It is necessary to cover all items of personal data to be provided to a third party by opting out. It must be kept in mind that items of personal data not so covered may not be provided to a third party by opting out.

Case 1) Name, address, telephone number, age

Case 2) Name, history of product purchase

(3) Method of a third-party provision:

Case 1) Publication as a book (including an electronic book)

Case 2) Posting on the Internet
Case 3) Delivery in printed form
Case 4) Distribution by various means of communication
Case 5) Delivery in the form of other external storage units

(4) To cease a third-party provision in response to a principal's request.

(5) Method of receiving a principal's request (*7):
Case 1) Mail
Case 2) Emailing
Case 3) Entry into a designated form on a webpage
Case 4) In-person acceptance through a window service at a business office
Case 5) Telephone

(*1) When carrying out a third-party provision through opt-out, in order to ensure that a principal who may be identified by personal data to be provided to a third party would have a sufficient period in order to request the provision to be ceased, the principal must be notified of the matters set forth in (1) through (5) above in advance, or such matters must be put into a state where the principal can easily know them (Article 15, Paragraph 4, Item (1)), and for this purpose, if the third-party provision is carried out in an extremely short period after the principal is so notified or such matters are put into a state where the principal can easily know them, then it can be interpreted that "a period required in order to request the provision to be ceased" has not been given.
A specific length of such period is required to be determined on a case-by-case basis because such length may vary depending *inter alia* on the type of business, form of business, how notification is given or how the principal can easily know such matters, the proximity between the principal and the personal information handling business operator, and the system for accepting the principal's request for cessation, and the nature of personal data to be provided.
Additionally, the time at which "the principal must be notified ..., or such matters must be put into a state where the principal can easily know them" and the time at which "notification is made to the Personal Information Protection Commission" do not have to be the same, but it is desirable to give notification to the Personal Information Protection Committee promptly after the principal is so notified or such matters are put into a state where the principal can easily know them.

(*2) As for "Informing a Principal", see 2-11 (Informing a Principal).

A “state where a principal can easily know” refers to a state where the principal can know easily in terms of both timing and means if the principal intends to know, by displaying or making available a document at the window, etc. of a business office, a posting on web pages, or such other continuing method, and an appropriate and reasonable method to enable the principal to recognize without fail must be adopted, depending on the nature of business and how personal information is handled (Article 15, Paragraph 4, Item (2)).

<Examples of a state where the principal can easily know>

Case 1) Where a web page of the telecommunications carrier which the principal is reasonably expected to view continuously post legal required matters in an easy-to-understand manner at an easy-to-find location (for instance, at a site which can be reached by one action or so from the home page).

Case 2) Where the relevant matters are displayed, made available, or otherwise continuously provided at the window, etc. of a business office which the principal is reasonably expected to visit.

Case 3) Where the relevant matters are provided on a regular basis in a periodical publication distributed to the principal.

Case 4) Where, in an electronic commerce transaction, a link is continuously provided on a web page that introduces the product.

(*3) Notification must be given in the method prescribed by the Personal Information Protection Committee (Article 15, Paragraph 5). Additionally, when an attorney-in-fact gives such notification, a document verifying the power of agency must be submitted in the form prescribed by the Personal Information Protection Committee (Article 15, Paragraph 6). Furthermore, a telecommunications carrier in a foreign county must, in case of giving the notification, appoint a person domiciled in Japan who has the authorization to act for the telecommunications carrier on any action relating to the notification, and the said telecommunications carrier must submit a document verifying such power of agency to the Personal Information Protection Commission (Article 15, Paragraph 7).

(*4) For the “principal’s consent”, see 2-13 (Principal’s Consent).

(*5) If the initial utilization purpose specified pursuant to Article 4, Paragraph 1 does not include any matter relating to a third-party provision of personal information, the third-party provision through opt-out cannot be made because such third-party provision would be regarded as unintended use.

(*6) Basically, “disclosure to the public” “through the Internet” is desirable, but in

view of the characteristics of the telecommunications carrier and the proximity with the principal, disclosure to the public can be made by an appropriate method other than the aforementioned method. For “disclosure to the public”, see 2-12 (Disclosure to the Public).

(*7) The method of “receiving a principal’s request” includes a contact by which the principal makes a request (such as the name of a business operator, window service description, mailing address, and receiving email address; and if such personal information handling business operator is based in a foreign country, the name, contact information, etc., of an attorney-in-fact in Japan).

(For Reference)

Article 23 of the Act (paragraph (2))

(2) A personal information handling business operator, in regard to personal data provided to a third party (excluding special care-required personal information; hereinafter the same in this paragraph), may, in cases where it is set to cease in response to a principal’s request a third-party provision of personal data that can identify the principal and when pursuant to rules of the Personal Information Protection Commission it has in advance informed a principal of those matters set forth in the following or put them into a state where a principal can easily know, and notified them to the Personal Information Protection Commission, provide the said personal data to a third party notwithstanding the provisions of the preceding paragraph.

(i) to set a third-party provision as a utilization purpose

(ii) the categories of personal data provided to a third party

(iii) a method of a third-party provision

(iv) to cease, in response to a principal’s request, a third-party provision of personal data that can identify the principal

(v) a method of receiving a principal’s request

Article 7 of the Rules

(1) Action for informing or putting into a state where a principal can easily know pursuant to the provisions of Article 23, paragraph (2) and paragraph (3) is to be carried out as set forth in the following.

(i) setting a necessary period for a principal identifiable by the provided personal data (referred to as "the principal" in the succeeding item) to request the provision to be ceased.

(ii) adopting an appropriate and reasonable method to enable the principal to recognize without fail a matter set forth in each item of Article 23, paragraph (2) of the Act.

(2) A notification pursuant to the provisions of Article 23, paragraph (2) or paragraph (3) shall

be given by any of each method set forth in the following.

(i) a method using an electronic data processing system (meaning an electronic data processing system connecting a computer relating to use by the Personal Information Protection Commission and a computer relating to use by a notifying person via electronic telecommunication line) as prescribed by the Personal Information Protection Commission.

(ii) a method submitting a written notification in an appended form No. 1 and an optical disc (including, an object that can assuredly keep a record of certain matters by an equivalent method to such an optical disc; hereinafter referred to as an "optical disc etc.") that has kept a record of a matter to be stated in the written notification.

(3) A personal information handling business operator shall, in case of giving a notification pursuant to the provisions of Article 23, paragraph (2) or paragraph (3) of the Act by an agent, submit to the Personal Information Protection Commission a document (including an electromagnetic record; hereinafter the same.) verifying the power of agency in an appended form No. 2.

Article 8 of the Rules

A personal information handling business operator in a foreign county shall, in case of giving a notification pursuant to the provisions of Article 23, paragraph (2) or paragraph (3) of the Act, appoint a person domiciled in Japan who has the authorization to act for the personal information handling business operator on any action relating to the notification. In this case, the said personal information handling business operator shall submit a document (including texts translated into Japanese) verifying that it has conferred the power of agency on the person domiciled in Japan to the Personal Information Protection Commission at the same time of giving the said notification.

Article 10 of the Rules

A personal information handling business operator shall, promptly after public disclosure pursuant to the provisions of Article 23, paragraph (4) of the Act has been made, disclose to the public those matters set forth in paragraph (2) of the said Article (when a matter set forth in item (ii), item (iii) or item (v) has been modified, a post-modified matter set forth in each said item) by utilizing the Internet or other appropriate method.

3-5-2-2 Altering to Matters Relating to Opt-out (in Relation to Article 15, Paragraph 3)

Article 15 (Paragraph 3)
3. A telecommunications carrier shall, in case of altering those matters set forth in Item (2), (3) or (5) of the preceding paragraph, in advance inform a principal of the contents to be altered or put them into a state where a principal can easily know and notify them to the Personal Information Protection Commission.

Where a telecommunications carrier provides personal data to a third party through opt-out pursuant to Article 15, Paragraph 2, when it alters items of persona data provided, method of provision, or method for accepting a principal's request for cessation of such third-party provision, it must inform in advance (*1) the principal of the contents to be altered or put them into a state where a principal can easily know (*2) and notify them to the Personal Information Protection Commission (*3).

Additionally, where a telecommunications carrier has notified the Personal Information Protection Committee of necessary matters pursuant to Article 15, Paragraph 9, the telecommunications carrier itself shall also disclose such contents to the public (*4).

(*1) For a specific period of "in advance", see 3-5-2-1 (Principles Regarding Opt-Out).

(*2) For "informing a principal", see 2-11 (Informing a Principal).
For a "state where a principal can easily know", see 3-5-2-1 (Principles Regarding Opt-Out). Additionally, methods such as those described below are regarded as appropriate and reasonable methods.

- Notifying a principal of the altered contents in a document which clearly indicates the same, for instance, by using a comparison chart of new and old contents.
- Clearly indicating the altered contents, for instance, by using a comparison chart of new and old contents, at an easy-to-find location for the principal on a web page of the telecommunications carrier which the principal is reasonably expected to view.

(*3) For the method, etc. of notification, see 3-5-2-1 (Principles Regarding Opt-Out).

(*4) For "disclosure to the public", see 2-12 (Disclosure to the Public).

(For Reference)

Article 23 of the Act (paragraph (3))
(3) A personal information handling business operator shall, in case of altering those matters set forth in item (ii), item (iii) or item (v) of the preceding paragraph, in advance inform a principal of the contents to be altered or put them into a state where a principal can easily

know and notify them to the Personal Information Protection Commission pursuant to rules of the Personal Information Protection Commission.

Articles 7, 8 and 10 of the Rules
(omitted) (see 3-5-2-1 (Principles Regarding Opt-out))

3-5-3 Exceptions to Personal Information Protected under the Secrecy of Communications in Limiting Third-Party Provision (in Relation to Article 15, Paragraph 8)

Article 15 (Paragraph 8)
8. Notwithstanding the provisions of the respective preceding paragraphs, a telecommunications carrier shall not provide to a third party personal information protected under the secrecy of communications except where the user's consent has been obtained or if there is other justifiable cause for noncompliance with the law.

Where certain personal information is protected under the secrecy of communications, a third-party provision of such personal information is permitted only in cases where the corresponding party's consent has been obtained, such provision is carried out in accordance with a warrant issued by a judge, the requirements of necessity are met, or if there is other justifiable cause for noncompliance with the law.

(*) With regard to the consent to the handling of personal information protected under the secrecy of communications, see 2-13 (Principal's Consent).

3-5-4 Where a Person is Not Deemed a Third Party (in Relation to Article 15, Paragraph 10)

Article 15 (Paragraph 10)
10. In those cases set forth in the following, a person receiving the provision of the said personal data shall not fall under a third party in regard to applying the provisions of Paragraphs 1 through 7 and the preceding paragraph:
(1) cases in which personal data is provided accompanied by a telecommunications carrier entrusting a whole or part of the handling of the personal data within the necessary scope to achieve a utilization purpose;
(2) cases in which personal data is provided accompanied with business succession caused by a merger or other reason;
(3) cases in which personal data to be jointly utilized by a specified person is provided to the specified person, and when a principal has in advance been informed or a state

has been in place where a principal can easily know to that effect as well as of the categories of the jointly utilized personal data, the scope of a jointly utilizing person, the utilization purpose for the utilizing person and the name or appellation of a person responsible for controlling the said personal data.

In the cases set forth in (1) through (3) below, the recipient of personal data is regarded as a third party in formality given that it is a separate entity form the telecommunications carrier; however, because it is reasonable to treat such recipient as one unit with the telecommunications carrier in terms of the relationship with the principal, such recipient shall not be regarded as a third party.

When such requirement is satisfied, notwithstanding the provisions of Article 15, Paragraphs 1 through 7 and 9, personal data may be provided without obtaining the principal's consent in advance or in the absence of an opt-out for the third-party provision.

Incidentally, this paragraph does not apply to personal information protected under the secrecy of communications, and even where the entrustment, business succession, or joint utilization is involved, such personal information must not be provided except where the corresponding party's consent has been obtained, or if there is justifiable cause for noncompliance with the law. However, this does not apply where the holder of information remains substantially the same as in the case of a merger or company split.

(1) Entrustment (in Relation to Article 15, Paragraph 10, Item (1)):

Where personal data are provided accompanied by a telecommunications carrier entrusting a whole or part of the handling of the personal data within the necessary scope to achieve a utilization purpose, the recipient of such personal data is not regarded as a third party.

Incidentally, the telecommunications carrier will be held responsible for supervision over the contractor pursuant to Article 12, Paragraph 3 (see 3-3-6 (Supervision over Contractors)).

Case 1) Where personal data are provided in order to entrust processing of information such as typing in of data entry.

Case 2) Where personal data are provided to a package delivery company for the purpose of delivery of ordered products.

(2) Business Succession (in Relation to Article 15, Paragraph 10, Item (2)):

Where personal data pertaining to a business is provided accompanied with business succession caused by a merger, company split, business transfer, or other reason, the recipient of such personal data shall not be regarded as a third party.

Additionally, after the business succession, personal data must be used within the scope of utilization purpose prescribed before such personal data are provided due to such business succession (see 3-1-5 (Succession of Business)).

Furthermore, this item also applies where, at a negotiation process for the execution of an agreement for business succession, a company is examined by the other party and provides personal data to the other party, and such personal data may be provided without obtaining the principal's consent in advance or without taking an opt-out procedure; however, an agreement must be executed as needed to ensure the other company's compliance with security control actions, by providing for the utilization purpose and method of handling of such data, measures to be taken in the event of a leakage, etc., and measures, etc. in the event that the negotiation for the business succession is unsuccessful.

Case 1) Where personal data are provided to a new company due to a merger or company split.
Case 2) Where personal data are provided to a transferee company due to a business transfer.

(3) Joint Utilization (in Relation to Article 15, Paragraph 10, Item (3)):

Cases in which personal data to be jointly utilized by a specified person is provided to the specified person (*1), and when a principal has in advance been informed (*3) or a state has been put in place where a principal can easily know (*4) with regard to the matters set forth in (i) through (v) below (*2), then the recipient of such personal data shall not be regarded as a third party because it can be recognized as reasonable from the principal's perspective to treat such recipient as one unit with the business operator to which the principal initially provided such personal data (*5). On the other hand, when a telecommunications carrier jointly utilizes personal data of subscribers, it is generally possible to obtain the principal's consent under contractual terms and conditions, and basically it is desirable to do so upon obtaining the principal's consent. However, even where the principal's consent is obtained for joint utilization under contractual terms and conditions, if any information which may have a material impact on the principal's rights and interests, such as non-paying person information, is to be exchanged, then it is appropriate to ensure that the principal is notified of the information set forth in Article 15, Paragraph 10, Item (3) or such information is put into a state where the principal can easily know such information so as not to unreasonably infringe the principal's rights and interests.

Furthermore, where personal data which a specific business operator has already acquired are jointly used with another business operator, such personal data must be jointly utilized within the scope of utilization purpose specified pursuant to the provisions of Article 4, Paragraph 1.

(i) Manifestation of joint utilization

(ii) Categories of the jointly utilized personal data

Case 1) Name, address, telephone number, age

Case 2) Name, history of product purchase

(iii) Scope of a jointly utilizing person

The "purpose of joint utilization" is to jointly utilize personal data with another business operator to the extent that it is reasonable from the principal' perspective that such business operator may be treated as one unit with the business operator providing such personal data.

Accordingly, the scope of a jointly utilizing person needs to be clarified so that the principal is able to determine to what extent the business operators will utilize his/her personal data in the future.

Incidentally, so long as such scope is clear, it is not always necessary to list the names of such business operators individually, but the principal should be able to determine to what extent the business operators will utilize his/her personal data.

(iv) Utilization purpose for the utilizing person

The principal must be notified of all utilization purposes of personal data to be utilized jointly, or such purposes must be put into a state where the principal can easily know them.

Additionally, if the utilization purpose is different for each item of personal data, it is desirable that the utilization purpose is specified separately for each such item of personal data.

(v) Name or appellation of a person responsible for controlling such personal data

A "person responsible for controlling such personal data" refers to a person who accepts requests for disclosure and complaints, endeavors to process the same, has the authority to disclose, correct, suspend the utilization of, and otherwise deal with the contents, etc. of personal data, and is responsible for security control and other administration of personal data.

Additionally, the "responsible person" for this purpose refers to, within all business operators which jointly utilize personal data, a person who is primarily authorized to accept and process complaints and make disclosure, correction, etc., and does not refer to an internal person in charge within one business operator of all jointly utilizing persons.

Furthermore, the person responsible for controlling such personal data must strive to keep the accuracy and currentness of personal data utilized among the jointly utilizing persons to the extent necessary in order to achieve the utilization purpose (see 3-3-1 (Assurance, etc. about the Accuracy of Data Contents)).

<Examples of Joint Utilization>

Case 1) Where information is jointly utilized within the scope of utilization purpose at the time when such information is acquired for group companies to provide general services (including the utilization purpose altered in accordance with the provisions of Article 4, Paragraph 2; the same shall apply hereinafter).

Case 2) Where personal data are jointly utilized within the scope of utilization purpose at the time when such data are acquired among subsidiaries and sister companies.

(*1) With regard to the provision of personal data to be jointly utilized, such provision does not have to be mutual among all jointly utilizing persons, and one joint user may provide such data to another unilaterally.

(*2) Where a telecommunications carrier implements joint utilization, with a view to clarifying responsibilities, etc. of jointly utilizing persons and smoothly implementing the same, it is desirable to agree on the matters in (a) through (f) below in advance in addition to the matters set forth in (i) through (v) above.

(a) Requirements of a jointly utilizing person (being a group company, being a member of a specific campaign project, or a certain framework in executing a project through joint utilization)

(b) Personal information protection manager, person in charge of inquiries, and contact information at each jointly utilizing person

(c) Matters concerning the handling of personal data jointly utilized

- Matters concerning prevention of leakage, etc. of personal data
- Prohibition of unintended processing, utilization, copying, reproduction, etc.
- Matters concerning return, deletion, and disposal of data after the joint utilization ends

(d) Measures to be taken in the event of a violation of any arrangement concerning the handling of personal data jointly utilized

(e) Matters concerning reporting and notification upon the occurrence of an incident or accident involving personal data jointly utilized

(f) Procedures for ending joint utilization

(*3) For “informing a principal”, see 2-11 (Informing a Principal).

(*4) For a “state in which a principal can easily know”, see 3-5-2 (Third-Party Provision through Opt Out).

(*5) Whether joint utilization or entrustment is applicable is determined based on the form of handling of personal data, and even where a contractor is included in jointly utilizing persons, the relationship with the contractor is not that of joint utilization, and the entrusting party shall not be excused from the duty to

supervise the contractor.

(For Reference)

Article 23 of the Act (paragraph (5))

(5) In those cases set forth in the following, a person receiving the provision of the said personal data shall not fall under a third party in regard to applying the provisions of each preceding paragraph.

(i) cases in which personal data is provided accompanied by a personal information handling business operator entrusting a whole or part of the handling of the personal data within the necessary scope to achieve a utilization purpose

(ii) cases in which personal data is provided accompanied with business succession caused by a merger or other reason

(iii) cases in which personal data to be jointly utilized by a specified person is provided to the specified person, and when a principal has in advance been informed or a state has been in place where a principal can easily know to that effect as well as of the categories of the jointly utilized personal data, the scope of a jointly utilizing person, the utilization purpose for the utilizing person and the name or appellation of a person responsible for controlling the said personal data

<Altering matters relating to joint utilization (in Relation to Article 15, Paragraph 11)>

Article 15 (Paragraph 11)

11. A telecommunications carrier shall, in case of altering a utilization purpose for a utilizing person or the name or appellation of a person responsible for controlling personal data prescribed in Item (3) of the preceding paragraph, in advance inform a principal of the contents to be altered or put them into a state where a principal can easily know.

Where personal data are jointly utilized, a telecommunications carrier may alter a "utilization purpose for a utilizing person" to the extent that may be objectively recognized as the extent that a principal can normally expect under social norms (*1), and the "name or appellation of a person responsible for controlling personal data" may also be altered, but in either case, the telecommunications carrier must in advance inform a principal (*2) or put them into a state where a principal can easily know (*3).

Incidentally, as a general rule, it is not permitted to alter the "categories of the jointly utilized personal data" and the "scope of a jointly utilizing person"; however, the joint utilization may be continued, for instance, in the cases illustrated below.

Case 1) Where the principal's consent has been obtained in advance with respect to any alteration to the categories of the jointly utilized personal data or to the jointly utilizing

person.

Case 2) Where the appellation of the jointly utilizing business operator has been changed, but the categories of the jointly utilized personal data remain unchanged.

Case 3) Where a business succession (*4) has occurred in respect of the jointly utilizing business operator (on condition that there is no alteration to the categories of the jointly utilized personal data).

(*1) For the scope of "the extent that may be objectively recognized as the extent that a principal can normally expect under social norms", see 3-1-2 (Altering a Utilization Purpose).

(*2) For "informing a principal", see 2-11 (Informing a Principal).

(*3) For a "state in which a principal can easily know", see 3-5-2 (Third-Party Provision Through Opt-Out).

(*4) For a "business succession", see 3-1-5 (Succession of Business).

(For Reference)

Article 23 of the Act (paragraph (6))

(6) A personal information handling business operator shall, in case of altering a utilization purpose for a utilizing person or the name or appellation of a person responsible for controlling personal data prescribed in item (iii) of the preceding paragraph, in advance inform a principal of the contents to be altered or put them into a state where a principal can easily know.

3-5-5 Restriction on Provision to a Third Party in a Foreign Country (in Relation to Article 16)

Article 16

1. A telecommunications carrier, except in those cases set forth in each item of the preceding Article, Paragraph 1, shall, in case of providing personal data to a third party (excluding a person establishing a system conforming to standards prescribed by the next following paragraph as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data pursuant to the provisions of Chapter IV, Section 1 of the Act; hereinafter the same in this Article) in a foreign country, in advance obtain a principal's consent to the effect that he or she approves the provision to a third party in a foreign country. In this case, the provisions of the preceding Article (except for Paragraph 8 of the said Article) shall not apply.
2. Standards prescribed as necessary measures for continuously taking measures equivalent

to those which shall be taken by a personal information handling business operator pursuant to the provisions of Chapter IV, Section 1 of the Act with regard to the handling of personal data shall fall under any of each following item:

(1) a telecommunications carrier and a person who receives the provision of personal data have ensured, in relation to the handling of personal data by the person who receives the provision, the implementation of measures in line with the purport of the provisions under Chapter IV, Section 1 of the Act by an appropriate and reasonable method;

(2) a person who receives the provision of personal data has obtained a recognition based on an international framework concerning the handling of personal information.

With regard to the restriction on provision to a third party in a foreign country, the "*Guidelines for the Act on the Protection of Personal Information (for Provision to a Third Party in a Foreign Company)*" (Personal Information Protection Commission Public Notice No. 7 of 2016) prescribed by the Personal Information Protection Commission shall apply *mutatis mutandis*.

(For Reference)

Article 24 of the Act

A personal information handling business operator, except in those cases set forth in each item of the preceding Article, paragraph (1), shall, in case of providing personal data to a third party (excluding a person establishing a system conforming to standards prescribed by rules of the Personal Information Protection Commission as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data pursuant to the provisions of this Section; hereinafter the same in this Article) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same) (excluding those prescribed by rules of the Personal Information Protection Commission as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests; hereinafter the same in this Article), in advance obtain a principal's consent to the effect that he or she approves the provision to a third party in a foreign country. In this case, the provisions of the preceding Article shall not apply.

Article 11 of the Rules

1. Foreign countries prescribed by rules of the Personal Information Protection Commission under Article 24 of the Act as having systems for protection of personal information are to be prescribed by the Personal Information Protection Commission as falling under all

of the following items.

(i) there is a law or other regulations corresponding to provisions of the Act for personal information handling business operators, and the circumstances are sufficient to consider enforcement of them is ensured

(ii) an independent foreign enforcement authority corresponding to the Personal Information Protection Commission exists, and such foreign enforcement authority ensures a system to exercise necessary and appropriate supervision

(iii) it is considered possible to collaborate and cooperate with Japan based on mutual understanding concerning the proper and effective application of personal information and protection of individual's rights and interests

(iv) it is considered possible to attempt mutual and smooth transfer of personal data with Japan, protecting personal information, without limiting international transfer of personal data beyond the extent necessary to protect of personal information

(v) in addition to those prescribed in the preceding four items, deciding the foreign country as a foreign country under Article 24 of the Act is considered to contribute 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

2. When deciding a foreign country under the preceding paragraph, the Personal Information Protection Commission may set necessary conditions including limiting the scope of personal data which may be provided without a principal's consent to provision to a third party in the foreign country, if considering it necessary to protect individual's rights and interest.

3. After deciding the foreign country under the first paragraph, if considering it necessary to confirm that the foreign country falls under each item of paragraph (1) or that the condition set under the preceding paragraph concerning the foreign country is met, the Personal Information Commission shall conduct necessary research on the personal information protection system or the status of attempt regarding the condition in the foreign country.

4. After deciding the foreign country under the first paragraph, if considering the foreign country no longer falls under each paragraph of paragraph 1 or the condition set under the paragraph (2) concerning the foreign country is no longer met in light of the research result under the preceding paragraph and other circumstances, the Personal Information Protection Commission shall rescind the decision under paragraph (1).

Article 11-2 of the Rules

Standards prescribed by rules of the Personal Information Protection Commission under Article 24 of the Act are to be falling under any of each following item.

(i) a personal information handling business operator and a person who receives the provision of personal data have ensured in relation to the handling of personal data by the person who receives the provision the implementation of measures in line with the purport of the provisions under Chapter IV, Section 1 of the Act by an appropriate and reasonable method

(ii) a person who receives the provision of personal data has obtained a recognition based on an international framework concerning the handling of personal information

3-5-6 Keeping, etc. of a Record on a Third-Party Provision (in Relation to Article 17)

Article 17

1. A telecommunications carrier shall, when having provided personal data to a third party (excluding a person set forth in each item of Article 2, paragraph (5) of the Act; hereinafter the same in this Article and the next following Article), keep a record of the following matters, for each of the categories set forth in the following items by a method of keeping such record in writing, an electromagnetic form, or a microfilm. This, however, shall not apply in cases where the personal data provision falls under any of each item of Article 15, Paragraph 1 or 10 (this means, in case of a personal data provision pursuant to the provisions of the preceding Article, any of each item of Article 15, Paragraph 1):
   (1) cases in which personal data has been provided to a third party pursuant to the provisions of Article 15, Paragraph 2: a matter set forth in (a) to (d) below.
      (a) the date on which the personal data was provided;
      (b) the name or appellation of the third party or other matter sufficient to identify the said third party (when provided to a large number of unspecified persons, the fact to that effect);
      (c) the name of a principal identifiable by the personal data and other matter sufficient to specify the principal;
      (d) the category of the personal data.
   (2) cases in which personal data has been provided to a third party pursuant to Article 15, Paragraph 1, or the provisions of the preceding Article: a matter set forth in (a) and (b) below.
      (a) the fact to the effect that a principal's consent has been obtained under Article 15, Paragraph 1, or the preceding Article;
      (b) a matter set forth in (b) to (d) in the preceding item.
2. Regarding those matters prescribed in each item of the preceding paragraph which are identical in contents to those matters contained in a record already kept by using a method prescribed in Paragraphs 1, 3 and 4 (limited to those in the case of such a record having

been maintained), a record on the said matters may be omitted.

3. A record under Paragraph 1 shall be kept promptly at each time of personal data having been provided to a third party. Such a record, however, may be kept at one time for a series of provisions if personal data has been provided (excluding a provision pursuant to the provisions of Article 15, Paragraph 2; the same shall apply in this paragraph) continuously or repeatedly to the third party, or if it is certainly expected that personal data will be provided continuously or repeatedly to the said third party.
4. Notwithstanding the provisions of the preceding paragraph, in cases where personal data relating to a principal, pursuant to the provisions of Article 15, Paragraph 1, or the preceding Article, has been provided to a third party in connection with supplying goods or services to the principal and when a matter prescribed in each item of Paragraph 1 is stated in a contract or other document prepared in connection with the said supply, such a document may substitute for a record relating to the said matter.
5. A telecommunications carrier shall keep the record under Paragraph 1 for a period of time prescribed in each following item in accordance with the categories of those cases set forth in each following item:
   (1) cases in which a record was kept by using a method prescribed in the provisions of the preceding paragraph: a period of time up to the day on which one year has passed from the last date of personal data relating to the record having been provided;
   (2) cases in which a record was kept by using a method prescribed in the proviso to Paragraph 3: a period of time up to the day on which three years have passed from the last date of personal data relating to the record having been provided;
   (3) cases other than the preceding two items; three years.

With regard to keeping, etc. of a record on a third-party provision, the "*Guidelines for the Act on the Protection of Personal Information (for Duties of Confirmation and Recordkeeping for Third-Party Provision)*" (Personal Information Protection Commission Public Notice No. 8 of 2016) prescribed by the Personal Information Protection Commission shall apply *mutatis mutandis*.

Incidentally, even where the provision appears to be a third-party provision in formality, if there is substantially only small necessity to impose the duties of confirmation and recordkeeping in respect of such third-party provision in view of the purpose of confirmation and recordkeeping, then such third-party provision is not subject to such duties. For instance, where a telecommunications carrier displays a caller's telephone number at the principal's choice in a caller telephone number display service, or where a telecommunications carrier notifies a CGM (Consumer Generated Media) operator, etc. specified in advance of a user's age threshold information (whether or not the user has reached a certain age) based on information registered by a subscriber with regard to users as a part of a user registration service subscribed by such

subscriber, such telecommunications carrier provides personal data “on behalf of the principal”, and for the third-party provision in such cases, the duties of confirmation and record keeping are not imposed on either the provider or the recipient.

(For Reference)

Article 25 of the Act

(1) A personal information handling business operator shall, when having provided personal data to a third party (excluding a person set forth in each item of Article 2, paragraph (5); hereinafter the same in this Article and the succeeding Article), keep a record pursuant to rules of the Personal Information Protection Commission on the date of the personal data provision, the name or appellation of the third party, and other matters prescribed by rules of the Personal Information Protection Commission. This, however, shall not apply in cases where the personal data provision falls under any of each item of Article 23, paragraph (1) or paragraph (5) (this means, in case of a personal data provision pursuant to the provisions of the preceding Article, any of each item of Article 23, paragraph (1)).

(2) A personal information handling business operator shall maintain a record under the preceding paragraph for a period of time prescribed by rules of the Personal Information Protection Commission from the date when it kept the record.

Article 12 of the Rules

(1) A method of keeping a record under Article 25, paragraph (1) of the Act pursuant to the said paragraph shall be a method to keep it by using a written document, electromagnetic record or microfilm.

(2) A record under Article 25, paragraph (1) of the Act shall be kept promptly at each time of personal data having been provided to a third party (meaning a third party set forth in the said paragraph; the same shall apply in this Article, the succeeding Article, and from Articles 15 to 17.). Such a record, however, may not be kept at each time of provision if personal data has been provided (excluding a provision pursuant to the provisions of Article 23, paragraph (2) of the Act; the same shall apply in this paragraph.) continuously or repeatedly to the third party, or if a certainty has been anticipated that personal data will be provided continuously or repeatedly to the said third party.

(3) Notwithstanding the provisions of the preceding paragraph, in cases where personal data relating to a principal, pursuant to the provisions of Article 23, paragraph (1) or Article 24 of the Act, has been provided to a third party in connection with supplying goods or services to the principal with having his or her consent obtained and when a matter prescribed in each item of paragraph (1) of the succeeding Article is stated in a contract or other document produced in connection with the said supply, such a document may substitute for a record

relating to the said matter.1

Article 13 of the Rules

(1) Matters prescribed by rules of the Personal Information Protection Commission under Article 25, paragraph (1) of the Act shall be, in accordance with the categories of those cases set forth in each following item, those matters prescribed in each said item respectively.

(i) cases in which personal data has been provided to a third party pursuant to the provisions of Article 23, paragraph (2) of the Act; a matter set forth in the following (a) to (d)

(a) the date on which the personal data was provided

(b) the name or appellation of the third party or other matter sufficient to identify the said third party (when provided to a large number of unspecified persons, the fact to that effect)

(c) the name of a principal identifiable by the personal data and other matter sufficient to specify the principal

(d) the categories of the personal data

(ii) cases in which personal data has been provided to a third party pursuant to the provisions of Article 23, paragraph (1) or Article 24 of the Act; a matter set forth in the following (a) and (b)

(a) the fact to the effect that a principal's consent has been obtained under Article 23, paragraph (1) or Article 24 of the Act

(b) a matter set forth in (b) to (d) under the preceding item.

(2) Regarding those matters prescribed in each item of the preceding paragraph which are identical in contents to those matters contained in a record already kept by using a method prescribed in the preceding Article (limited to those in the case of such a record having been maintained), a record on the said matters may be omitted.

Article 14 of the Rules

A period of time prescribed by rules of the Personal Information Protection Commission under Article 25, paragraph (2) of the Act shall be, in accordance with the categories of those cases set forth in each following item, a period of time prescribed in each said item respectively.

(i) cases in which a record was kept by using a method prescribed in the provisions of Article 12, paragraph (3); a period of time up to the day on which one year has passed from the last date of personal data relating to the record having been provided

(ii) cases in which a record was kept by using a method prescribed in the provisions of the proviso under Article 12, paragraph (2); a period of time up to the day on which three years have passed from the last date of personal data relating to the record having been provided

(iii) cases other than the preceding two items; three years

3-5-7 Confirmation, etc. when Receiving a Third-Party Provision (in Relation to Article 18)

<Confirmation when Receiving a Third-Party Provision (in Relation to Article 18, Paragraphs 1 and 2)>

Article 18 (Paragraphs 1 and 2)

1. A telecommunications carrier shall, when receiving the provision of personal data from a third party, confirm those matters set forth in the following in the manner set forth in the following, respectively. This, however, shall not apply in cases where the said personal data provision falls under any of each item of Article 15, Paragraph 1 or 10.
   (1) the name or appellation and address of the third party and, for a corporate body, the name of its representative (for a non-corporate body having appointed a representative or administrator, the said representative or administrator) (except for the matters set forth in item (3)): by a method of reporting by the third party providing such personal data or in another appropriate manner;
   (2) circumstances under which the said personal data was acquired by the said third party (except for the matters set forth in the next following item): by a reasonable method such as having the said third party present a contract or other document showing those circumstances under which the said third party acquired the personal data ;
   (3) matters which have already been confirmed when receiving the provision of other personal data from a third party (limited to those in cases where a record has been kept and maintained by using a method prescribed in Paragraphs 3, 5 and 6 relating to the confirmation): by a method to confirm that the said matters are identical in contents to those matters set forth in the preceding two items relating to the said provision.
2. A third party under the preceding paragraph shall, in cases where a telecommunications carrier confirms pursuant to the provisions of the preceding paragraph, not deceive the telecommunications carrier on a matter relating to the confirmation.

<Keeping a Record when Receiving a Third-Party Provision (in Relation to Article 18, Paragraphs 3 through 7)>

Article 18 (Paragraphs 3 through 7)

3. A telecommunications carrier shall, when having confirmed pursuant to the provisions of Paragraph 1, keep a record of each of the following matters for the respective categories in the following items, by a method of preparing such record in writing, an electromagnetic form, or a microfilm:

(1) cases in which the provision of personal data has been received from a personal information handling business operator pursuant to the provisions of Article 23, paragraph (2) of the Act: a matter set forth in (a) to (e) below.
  (a) the date on which the provision of personal data was received;
  (b) a matter set forth in each item of Paragraph 1;
  (c) the name of a principal identifiable by the personal data and other matters sufficient to specify the principal;
  (d) the categories of the personal data;
  (e) the fact to the effect that disclosure to the public has been made pursuant to the provisions of Article 23, paragraph (4) of the Act.

(2) cases in which the provision of personal data has been received from a personal information handling business operator pursuant to the portions listed in the respective items of Article 23, paragraph (1) or Article 24 of the Act: a matter set forth in (a) and (b) below.
  (a) the fact to the effect that a principal's consent has been obtained under Article 23, paragraph (1) or Article 24 of the Act;
  (b) a matter set forth in (b) to (d) under the preceding item.

(3) cases in which the provision of personal data has been received from a third party (excluding a person falling within the purview of a personal information handling business operator): a matter set forth in (b) to (d) under Item (1).

4. Regarding those matters prescribed in each item of the preceding paragraph which are identical in contents to matters contained in a record already kept by using a method prescribed in the preceding paragraph, the next following paragraph, and Paragraph 6 (limited to those in the case of such a record having been maintained), a record on the said matters may be omitted.

5. A record under Paragraph 3 shall be kept promptly at each time when the provision of personal data has been received from a third party. Such a record, however, may be kept at one time for a series of receipts if the provision of personal data has been received continuously or repeatedly from the third party (excluding a provision pursuant to the provisions of Article 15, Paragraph 2; hereinafter the same in this Article), or when it is certainly expected that the provision of personal data will be received continuously or repeatedly from the said third party.

6. Notwithstanding the provisions of the preceding paragraph, in cases where the provision of personal data relating to a principal has been received from a third party in connection with supplying the principal with goods or services and when a matter prescribed in each item of Paragraph 3 is stated in a contract or other document prepared in connection with the supply, such a document may substitute for a record relating to the matter.

7. A telecommunications carrier shall maintain a record under Paragraph 3 for a period of time prescribed in the following items for the categories set forth in the following items, respectively:
   (1) cases in which a record was kept by using a method prescribed in the preceding paragraph: a period of time up to the day on which one year has passed from the last date on which the provision of personal data relating to the record was received;
   (2) cases in which a record was kept by using a method prescribed in the proviso to Paragraph 5: a period of time up to the day on which three years have passed from the last date on which the provision of personal data relating to the record was received;
   (3) cases other than the preceding two items: three years.

For confirmation, etc. in accepting a third-party provision, the "*Guidelines for the Act on the Protection of Personal Information (for Duties of Confirmation and Recordkeeping for Third-Party Provision)*" shall apply *mutatis mutandis*.

(For Reference)

<Confirmation when Receiving a Third-Party Provision (in Relation to Article 26, paragraphs (1) and (2))>

Article 26 (Paragraphs 1 and 2) of the Act

(1) A personal information handling business operator shall, when receiving the provision of personal data from a third party, confirm those matters set forth in the following pursuant to rules of the Personal Information Protection Commission. This, however, shall not apply in cases where the said personal data provision falls under any of each item of Article 23, paragraph (1) or paragraph (5).
   (i) the name or appellation and address of the third party and, for a corporate body, the name of its representative (for a non-corporate body having appointed a representative or administrator, the said representative or administrator)
   (ii) circumstances under which the said personal data was acquired by the said third party

(2) A third party under the preceding paragraph shall, in cases where a personal information handling business operator confirms pursuant to the provisions of the preceding paragraph, not deceive the personal information handling business operator on a matter relating to the confirmation.

Article 15 of the Rules

(1) A method of confirming those matters set forth in Article 26, paragraph (1), item (i) of the Act pursuant to the provisions of the said paragraph shall be a reasonable method such as

receiving a declaration from a third party who provides personal data.

(2) A method of confirming those matters set forth in Article 26, paragraph (1), item (ii) of the Act pursuant to the provisions of the said paragraph shall be a reasonable method such as receiving from a third party the production of a contract or other document showing those circumstances under which the personal data was acquired by the third party.

(3) Notwithstanding the provisions of the preceding two paragraphs, a method of confirming those matters which have already been confirmed when receiving the provision of other personal data from a third party (limited to those in cases where a record has been kept and maintained by using a method prescribed in the succeeding Article relating to the confirmation) shall be a method to confirm that the said matters are identical in contents to those matters set forth in each item of Article 26, paragraph (1) relating to the said provision.

<Keeping a Record Regarding a Confirmation when Receiving a Third-Party Provision (in Relation to Article 26, paragraphs (3) and (4))>

Article 26 of the Act (paragraphs (3) and (4))

(3) A personal information handling business operator shall, when having confirmed pursuant to the provisions of paragraph (1), keep a record pursuant to rules of the Personal Information Protection Commission on the date when it received the provision of personal data, a matter concerning the said confirmation, and other matters prescribed by rules of the Personal Information Protection Commission.

(4) A personal information handling business operator shall maintain a record under the preceding paragraph for a period of time prescribed by rules of the Personal Information Protection Commission from the date when it kept the record.

Article 16 of the Rules

(1) A method of keeping a record under Article 26, paragraph (3) of the Act pursuant to the said paragraph shall be a method to keep it by using a written document, electromagnetic record or microfilm.

(2) A record under Article 26, paragraph (3) of the Act shall be kept promptly at each time when the provision of personal data has been received from a third party. Such a record, however, may not be kept at each time of receipt if the provision of personal data has been received continuously or repeatedly from the third party (excluding a provision pursuant to the provisions of Article 23, paragraph (2) of the Act; hereinafter the same in this Article.), or when a certainty has been anticipated that the provision of personal data will be received continuously or repeatedly from the said third party.

(3) Notwithstanding the provisions of the preceding paragraph, in cases where the provision of personal data relating to a principal has been received from a third party in connection with

supplying the principal with goods or services and when a matter prescribed in each item of the succeeding Article, paragraph (1) is stated in a contract or other document produced in connection with the supply, such a document may substitute for a record relating to the matter.

Article 17 of the Rules

(1) Matters prescribed by rules of the Personal Information Protection Commission under Article 26, paragraph (3) of the Act shall be, in accordance with the categories of those cases set forth in each following item, those matters prescribed in each said item respectively.

(i) cases in which a personal information handling business operator has received the provision of personal data pursuant to the provisions of Article 23, paragraph (2) of the Act; a matter set forth in the following (a) to (e)

(a) the date on which the provision of personal data was received

(b) a matter set forth in each item of Article 26, paragraph (1) of the Act

(c) the name of a principal identifiable by the personal data and other matters sufficient to specify the principal

(d) the categories of the personal data

(e) the fact to the effect that disclosure has been made pursuant to the provisions of Article 23, paragraph (4) of the Act.

(ii) cases in which a personal information handling business operator has received the provision of personal data pursuant to the provisions of Article 23, paragraph (1) or Article 24 of the Act; a matter set forth in the following (a) and (b)

(a) the fact to the effect that a principal's consent has been obtained under Article 23, paragraph (1) or Article 24 of the Act

(b) a matter set forth in (b) to (d) under the preceding item

(iii) cases in which the provision of personal data has been received from a third party (excluding a person falling within the purview of a personal information handling business operator)

(a) a matter set forth in (b) to (d) under item (i).

(2) Regarding those matters prescribed in each item of the preceding paragraph which are identical in contents to matters contained in a record already kept by using a method prescribed in the preceding Article (limited to those in the case of such a record having been maintained), a record on the said matters may be omitted.

Article 18 of the Rules

A period of time prescribed by rules of the Personal Information Protection Commission under Article 26, paragraph (4) of the Act shall be, in accordance with the categories of those

cases set forth in each following item, a period of time prescribed in each said item respectively.

(i) cases in which a record was kept by using a method prescribed in Article 16, paragraph (3); a period of time up to the day on which one year has passed from the last date on which the provision of personal data relating to the record was received

(ii) cases in which a record was kept by using a method prescribed in the proviso under Article 16, paragraph (2); a period of time up to the day on which three years have passed from the last date on which the provision of personal data relating to the record was received

(iii) cases other than the preceding two items; three years

3-6 Disclosure to the Public of Matters Relating to Retained Personal Data; Disclosure, Alteration, etc. and Utilization Cease, etc. (in Relation to Articles 19 through 26)

3-6-1 Public Disclosure, etc. of Matters Relating to Retained Personal Data (in Relation to Article 19)

(1) Ensuring a Principal's Awareness of Matters Relating to Retained Personal Data (in Relation to Article 19, Paragraph 1)

Article 19 (Paragraph 1)

1. A telecommunications carrier shall, concerning its retained personal information, put those matters set forth in the following into a state where a principal can know (including those cases in which it, at the request of a principal, responds without delay):
   (1) the name or appellation of the said telecommunications carrier;
   (2) the utilization purpose of all retained personal data (excluding those cases falling under Items (1) through (3) of Article 8, Paragraph 4);
   (3) the procedures for responding to a request pursuant to the provisions of the next following paragraph or a demand pursuant to the provisions of Paragraph 1 of the next following Article, Article 21, Paragraph 1, or Article 22, Paragraph 1 or 3 (including, when the amount of a fee has been decided pursuant to the provisions of Article 25, Paragraph 2, the amount of the fee);
   (4) where to lodge a complaint about the handling of retained personal data by the said telecommunications carrier;
   (5) in those cases where the telecommunications carrier is a covered business operator of an accredited personal information protection organization, the appellation of the accredited personal information protection organization and where to lodge a petition for resolving a complaint.

A telecommunications carrier must, concerning its retained personal data, put those matters set forth in (i) through (iv) below into a state where a principal can know (including those cases

in which it, at the request of a principal, responds without delay) (*1).

(i) Name or appellation of the telecommunications carrier

(ii) Utilization purpose of all retained personal data (*2) (excluding certain cases (*3))

(iii) Procedures for responding to a request for notification or disclosure, etc. of the utilization purpose of retained personal data (*4) and the amount of a fee (if prescribed) for responding to a request for notification or disclosure, etc. of the utilization purpose of retained personal data (*5)

(iv) Where to lodge a complaint about the handling of retained personal data
(Example) Name of a service window or department which accepts a complaint, mailing address, telephone number, or other contact for lodging a complaint (if the telecommunications carrier is a covered business operator of an accredited personal information protection organization, then such organization's name and contact for resolution of complaints shall be included).

(*1) A "state where a principal can know (including those cases in which it, at the request of a principal, responds without delay)" refers to actions such as a posting in a web page, distribution of a brochure, and response without delay at the request of a principal, and otherwise putting into a state where the principal can know easily as the principal wishes to know, and at all times, current and accurate details must be put into a state where the principal can know such details. This does not necessarily require a posting on a home page or a display at the window in an office, etc. on an ongoing basis, but depending on the nature of business and how personal information is handled, such indication must be made in such reasonable and appropriate manner that the principal may recognize such details. Additionally, if a telecommunications carrier responds to many inquiries on a routine basis and posts such details on a home page on an ongoing basis, then such method meets both of the requirements of the "state where a principal can know" (see 3-5-2 (Third-Party Provision Through Opt-Out)) and the "state where a principal can know (including those cases in which it, at the request of a principal, responds without delay)".
<Examples of a state where a principal can know>
Case 1) Where a service window is set up, and a system is established so that an inquiry may be handled orally or in writing.
Case 2) Where a brochure is made available at a store.

Case 3) In electronic commerce, where a web page that introduces a product indicates an email address for inquiries.

(*2) If the utilization purpose includes third-party provision, then it must be so clearly indicated.

(*3) "Certain cases" refers to the cases below as set forth in Article 8, Paragraph 4, Items (1) through (3) (see 3-2-7 (Where Notification, etc. of Utilization Purpose is Not Required)).

a) Cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm a principal or third party's life, body, fortune or other rights and interests.

b) Cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm the rights or legitimate interests of the relevant telecommunications carrier.

c) Cases in which a private-sector corporation's cooperation is necessary in order for a central government organization, etc. to perform affairs prescribed by laws and regulations, and when there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would interfere with the performance of such affairs.

(*4) A "demand for disclosure, etc." refers to a demand for disclosure of retained personal data (see 3-6-2 (Disclosure of Retained Personal Data)), correction, addition or deletion of retained personal data (see 3-6-3 (Correction, etc. of Retained Personal Data), or utilization cease, deletion or cease of third-party provision of retained personal data (see 3-6-4 (Utilization Cease, etc. of Retained Personal Data)).

(*5) When the amount of a fee is to be determined, such amount must be set within such range as considered reasonable in view of actual costs (see 3-6-7 (Fee)).

(For Reference)

Article 27 of the Act (paragraphs (1) through (3))

(1) A personal information handling business operator shall, concerning its retained personal information, put those matters set forth in the following into a state where a principal can know (including those cases in which it, at the request of a principal, responds without delay).

(i) the name or appellation of the said personal information handling business operator

(ii) the utilization purpose of all retained personal data (excluding those cases falling under item (i) through item (iii) of Article 18, paragraph (4))

(iii) the procedures for responding to a request pursuant to the provisions of the succeeding

paragraph or a demand pursuant to the provisions of the succeeding Article, paragraph (i); Article 29, paragraph (1); or Article 30, paragraph (1) or paragraph (3) (including, when the amount of a fee has been decided pursuant to the provisions of Article 33, paragraph (2), the amount of the fee)

(iv) besides those set forth under the preceding three items, those prescribed by cabinet order as a necessary matter to ensure the proper handling of retained personal data

(2) A personal information handling business operator shall, when requested by a principal to get informed of a utilization purpose of retained personal data that can identify the principal, inform the said principal thereof without delay. This, however, shall not apply in those cases falling under any of each following item.

(i) cases in which the utilization purpose of retained personal data that can identify the said principal is clear pursuant to the provisions of the preceding paragraph

(ii) cases falling under item (i) through item (iii) of Article 18, paragraph (4)

(3) A personal information handling business operator shall, when having been requested based on the provisions of the preceding paragraph but decided not to inform a principal of the utilization purpose of retained personal data, inform the principal to that effect without delay.

Article 8 of the Cabinet Order

Article 8 Those prescribed by cabinet order under Article 27, paragraph (1), item (iv) of the Act shall be those set forth in the following;

(i) where to lodge a complaint about the handling of retained personal data by the said personal information handling business operator;

(ii) In those cases where the said personal information handling business operator is a covered business operator of an accredited personal information protection organization, the appellation of the accredited personal information protection organization and where to lodge a petition for resolving a complaint.

Article 47 of the Act

(1) A corporation (including a non-corporate body which has appointed a representative or administrator; the same shall apply in the succeeding Article, item (iii), (b)) which intends to render the following services in order to ensure the proper handling of personal information etc. by a personal information handling business operator etc. may receive an accreditation from the Personal Information Protection Commission.

(i) dealing with a complaint under the provisions of Article 52 about the handling of personal information etc. by a personal information handling business operator covered by the services (hereinafter referred to as a “covered business operator”)

(ii) providing a covered business operator with information concerning a matter contributory

to ensuring the proper handling of personal information etc.

(iii) besides those set forth in the preceding two items, rendering necessary services related to ensuring the proper handling of personal information etc. by a covered business operator

(2) A person who intends to receive an accreditation under the preceding paragraph shall, as prescribed by cabinet order, apply to the Personal Information Protection Commission.

(3) The Personal Information Protection Commission shall, when having granted an accreditation under the paragraph (1), announce to the public to that effect.

Article 52 of the Act

(1) An accredited personal information protection organization shall, when petitioned by a principal or other concerned person to resolve a complaint about its covered business operator's handling of personal information etc., hold consultation, give necessary advice to the petitioner and investigate circumstances surrounding the complaint, as well as inform the covered business operator of the complaint contents and request its expeditious resolution.

(2) An accredited personal information protection organization may, when recognizing that there is a need in regard to the resolution of a complaint in connection with a petition under the preceding paragraph, request the covered business operator to provide a written or oral explanation or submit a referential material.

(3) A covered business operator shall, when requested by an accredited personal information protection organization pursuant to the provisions of the preceding paragraph, not refuse the request without a justifiable reason.

(2) Informing Matters relating to Retained Personal Data (Article 19, Paragraphs 2 and 3)

Article 19 (Paragraphs 2 and 3)

2. A telecommunications carrier shall, when requested by a principal to get informed of a utilization purpose of retained personal data that can identify the principal, inform the said principal thereof without delay. This, however, shall not apply in those cases falling under any of each following item:
   (1) cases in which the utilization purpose of retained personal data that can identify the said principal is clear pursuant to the provisions of the preceding paragraph;
   (2) cases falling under Items (1) through (3) of Article 8, Paragraph 4.
3. A telecommunications carrier shall, when having been requested based on the provisions of the preceding paragraph but deciding not to inform a principal of the utilization purpose of retained personal data, inform the principal to that effect without delay.

A telecommunications carrier must, when requested by a principal to be informed (*) of a utilization purpose of retained personal data that can identify the principal, inform the said

principal thereof without delay, except in the cases of (i) through (iv) below.

Additionally, when the telecommunications carrier decides to refrain from informing the principal as requested, it must inform the principal to that effect without delay.

(i) Cases in which, the utilization purpose of retained personal data that can identify the principal is clear because of the measures in (1) above (Article 19, Paragraph 1).

(ii) Cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm a principal or third party's life, body, fortune or other rights and interests (Article 8, Paragraph 4, Item (1)) (see 3-2-7 (Where Notification, etc. of Publication Use is Not Required)).

(iii) Cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm the rights or legitimate interests of the relevant telecommunications carrier (Article 8, Paragraph 4, Item (2)) (see 3-2-7 (Where Notification, etc. of Publication Use is Not Required)).

(iv) Cases in which a private-sector corporation's cooperation is necessary in order for a central government organization, etc. to perform affairs prescribed by laws and regulations, and when there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would interfere with the performance of such affairs (Article 8, Paragraph 4, Item (3)) (see 3-2-7 (Where Notification, etc. of Publication Use is Not Required)).

(*) For "informing a principal", see 2-11 (Informing a Principal).

(For Reference)

Article 27 of the Act (paragraphs (2) and (3))

(2) A personal information handling business operator shall, when requested by a principal to get informed of a utilization purpose of retained personal data that can identify the principal, inform the said principal thereof without delay. This, however, shall not apply in those cases falling under any of each following item.

(i) cases in which the utilization purpose of retained personal data that can identify the said principal is clear pursuant to the provisions of the preceding paragraph

(ii) cases falling under item (i) through item (iii) of Article 18, paragraph (4)

(3) A personal information handling business operator shall, when having been requested based on the provisions of the preceding paragraph but decided not to inform a principal of the

utilization purpose of retained personal data, inform the principal to that effect without delay.

3-6-2 Disclosure of Retained Personal Data (in Relation to Article 20)

Article 20

1. A principal may demand of a telecommunications carrier the disclosing of retained personal data that can identify him or herself.
2. A telecommunications carrier shall, when having received a demand pursuant to the provisions of the preceding paragraph, disclose retained personal data to a principal without delay by delivery of a document to the principal (or by such method as agreed to by the person making the demand). However, in cases where disclosing such data falls under any of each following item, a whole or part thereof may not be disclosed:
   (1) cases in which there is a possibility of harming a principal or third party's life, body, fortune or other rights and interests;
   (2) cases in which there is a possibility of interfering seriously with the said telecommunications carrier implementing its business properly;
   (3) cases of violating other laws or regulations (excluding the Act, the Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003), and the Rules; the same in Paragraph 4 of this Article and Paragraph 2 in the next following Article).
3. A telecommunications carrier shall, when having decided not to disclose a whole or part of retained personal data in connection with a demand pursuant to the provisions of Paragraph 1 or when the retained personal data does not exist, inform a principal thereof without delay.
4. In cases where a whole or part of retained personal data that can identify a principal is to be disclosed to the principal pursuant to the provisions of other laws or regulations using a method equivalent to that prescribed in the main clause of Paragraph 2, the provisions of Paragraphs 1 and 2 shall not apply in regard to the said whole or part of retained personal data.

When a telecommunications carrier receives from a principal a demand for disclosure of retained personal data that can identify the principal (including notification of the absence of such retained personal data), the telecommunications carrier must disclose such retained personal data to the principal without delay by delivery of a document to the principal (or by such method as agreed to by the person making the demand (*1)) (*2).

However, in cases where disclosing such data falls under any of the cases set forth in (1) through (3) below, a whole or part thereof may not be disclosed, but when the telecommunications carrier decided to refrain from making such disclosure as a result, or when the retained personal

data so demanded does not exist, the telecommunications carrier must so inform the principal (*3) without delay.

(1) Cases in which there is a possibility of harming a principal or third party's life, body, fortune or other rights and interests:

If disclosing retained personal data to a principal may harm the principal's or a third party's life, body, fortune or other rights and interests, the telecommunications carrier may refrain from disclosing such retained personal data in whole or in part.

(2) Cases in which there is a possibility of interfering seriously with the relevant telecommunications carrier's implementing its business properly:

If disclosing retained personal data to a principal may interfere seriously with the relevant telecommunications carrier's implementing its business properly, the telecommunications carrier may refrain from disclosing such retained personal data in whole or in part.

Case 1) Where a single principal repetitiously makes a demand for disclosure of the same matter which necessitates a complicated response, and such situation is likely to result in a substantial operational interference due to the service window's being effectively occupied with such demand and being unable to respond to other inquiries.

Case 2) Where a telecommunications carrier is likely to experience a substantial operational interference due to a principal's request for disclosure of credit assessment, etc. which has been given by the telecommunications carrier independently.

(3) Cases of violating laws or regulations (excluding the Act, the Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003), and the Rules; the same in Paragraph 4 and Article 21, Paragraph 2).

Where disclosing retained personal data to a principal may violate laws and regulations (excluding the personal information protection laws and regulations), the telecommunications carrier may refrain from disclosing such retained personal data in whole or in part.

Case) Where such disclosure may violate Article 134 (Unlawful Disclosure of Confidential Information) of the Penal Code (Act No. 45 of 1907) or Article 4 (Protection of Secrecy of Communications) of the Telecommunications Business Act.

Furthermore, if any provision of laws and regulations (excluding the personal information protection laws and regulations) sets forth that retained personal information that can identify the principal shall be disclosed by a method equivalent to that under Article 20, Paragraph 2 (by delivery of a document to the principal (or by such method as agreed to by the person making the demand)), then the provisions of Article 20, Paragraph 1 and 2 shall not apply, and such provision of laws and regulations shall apply.

Additionally, with regard to the relationship between this Article and the case in which a principal demands, by filing a lawsuit in court, disclosure of retained personal date that can identify the principal, see 3-6-8 (Advance Demand Before Filing a Lawsuit).

(*1) "Such method as agreed to by the person making the demand" may be email, telephone, or other various methods as agreed to by the person making the demand as the method of disclosure, and it means that the method by delivery of a document is possible in the absence of such person's consent.
Additionally, if the person making the demand does not specify the method of disclosure and does not raise an objection to the method indicated by the telecommunications carrier (including where a demand for disclosure is made by telephone and a response is given by telephone in the same call after necessary confirmation of the identity), it may be deemed that the principal has given the consent to such method. As an alternative method of obtaining the consent of the person making a demand for disclosure, the telecommunications carrier may indicate several methods of disclosure to such person, and such person may select one of such methods as he/she wishes.

(*2) From the perspective of protecting the rights and interests of a principal such as a consumer, it is desirable to make further efforts to accommodate the principal's demand by clearly indicating from where and how personal information is acquired (the type, etc. of source) as specifically as possible, taking into account the characteristics, scale and actual situation of business activities.

(*3) For "informing a principal", see 2-11 (Informing a Principal).

(For Reference)

Article 28 of the Act (paragraphs (1) through (4))
(1) A principal may demand of a personal information handling business operator disclosing retained personal data that can identify him or herself.
(2) A personal information handling business operator shall, when having received a demand pursuant to the provisions of the preceding paragraph, disclose retained personal data to a principal without delay pursuant to a method prescribed by cabinet order. However, in cases

where disclosing such data falls under any of each following item, a whole or part thereof may not be disclosed.

(i) cases in which there is a possibility of harming a principal or third party's life, body, fortune or other rights and interests

(ii) cases in which there is a possibility of interfering seriously with the said personal information handling business operator implementing its business properly

(iii) cases of violating other laws or regulations

(3) A personal information handling business operator shall, when having decided not to disclose a whole or part of retained personal data in connection with a demand pursuant to the provisions of paragraph (1) or when the retained personal data does not exist, inform a principal thereof without delay.

(4) In cases where a whole or part of retained personal data that can identify a principal is to be disclosed to the principal pursuant to the provisions of other laws or regulations using a method equivalent to that prescribed in the main clause of paragraph (2), the provisions of paragraph (1) and paragraph (2) shall not apply in regard to the said whole or part of retained personal data.

Article 9 of the Cabinet Order

A method prescribed by cabinet order under Article 28, paragraph (2) of the Act shall be the one by delivering a written document (when there is a method agreed on by a person having requested disclosure, that method).

3-6-3 Correction, etc. of Retained Personal Data (in Relation to Article 21)

Article 21

1. A principal may, when the contents of retained personal data that can identify the principal are not factual, demand of a telecommunications carrier the making of a correction, addition or deletion (hereinafter referred to as a "correction etc." in this Article) in regard to the contents of the retained personal data.
2. A telecommunications carrier shall, in case of having received a demand pursuant to the provisions of the preceding paragraph except in cases where special procedure concerning a correction etc. of the contents is prescribed by the provisions of laws or regulations, conduct a necessary investigation without delay to the extent necessary to achieve a utilization purpose and, based on the result thereof, make a correction etc. of the contents of the retained personal data.
3. A telecommunications carrier shall, when having made a correction etc. on a whole or part of the contents of the retained personal data in connection with a demand pursuant to the

provisions under Paragraph 1 or when having made a decision not to make a correction etc., inform a principal without delay to that effect (including, when having made a correction etc., the contents thereof).

When a telecommunications carrier receives a principal's demand for the making of a correction, addition or deletion (*1) (hereinafter referred to as a "correction, etc.") on the ground that the contents of retained personal data that can identify the principal are erroneous and incorrect, then the telecommunications carrier must conduct a necessary investigation without delay to the extent necessary to achieve a utilization purpose and make a correction, etc. based on the result thereof, as a general rule (*2).

Additionally, when a telecommunications carrier makes a correction, etc. of the contents of the retained personal data, in whole or in part, in response to a demand under the provisions of Article 21, Paragraph 2, or decides to refrain from making such correction, etc., the telecommunications carrier must inform the principal (*3) without delay to that effect (including the contents of such correction, etc. if such correction, etc. is made).

Furthermore, if a special procedure is prescribed in the provisions of laws and regulations (excluding the personal information protection laws and regulations) with regard to a correction, etc. of the contents of retained personal data, the provisions of Article 21, Paragraph 1 and 2 shall not apply, and such provision of laws and regulations shall apply.

Incidentally, with regard to the relationship between this Article and the case in which a principal demands, by filing a lawsuit in court, a correction, etc. of retained personal date that can identify the principal, see 3-6-8 (Advance Demand Before Filing a Lawsuit).

<Examples where no correction is required>

Case) Where the subject of a correction, etc. is not about a fact but is information relating to an evaluation.

(*1) "Deletion" means removal of unnecessary information.

(*2) Where a correction, etc. is unnecessary in view of the utilization purpose, or where an allegation that retained personal data contains an error is made incorrectly, then it is unnecessary to make the correction, etc.; provided that, in such case, the principal must be informed without delay to the effect that such correction, etc. will not be made.

(*3) For "informing a principal", see 2-11 (Informing a Principal).

(For Reference)

Article 29 of the Act

(1) A principal may, when the contents of retained personal data that can identify the principal are not factual, demand of a personal information handling business operator making a correction, addition or deletion (hereinafter referred to as a "correction etc." in this Article) in regard to the contents of the retained personal data.

(2) A personal information handling business operator shall, in case of having received a demand pursuant to the provisions of the preceding paragraph except in cases where special procedure concerning a correction etc. of the contents is prescribed by the provisions of other laws or regulations, conduct a necessary investigation without delay to the extent necessary to achieve a utilization purpose and, based on the result thereof, make a correction etc. of the contents of the retained personal data.

(3) A personal information handling business operator shall, when having made a correction etc. on a whole or part of the contents of the retained personal data in connection with a demand pursuant to the provisions under paragraph (1) or when having made a decision not to make a correction etc., inform a principal without delay to that effect (including, when having made a correction etc., the contents thereof).

3-6-4 Utilization Cease, etc. of Retained Personal Data (in Relation to Article 22)

Article 22

1. A principal may, when retained personal data that can identify the principal is being handled in violation of the provisions of Article 5 or has been acquired in violation of the provisions of Article 7, demand of a telecommunications carrier a utilization cease or deletion (hereinafter referred to as a "utilization cease etc." in this Article) of the retained personal data.
2. A telecommunications carrier shall, in case of having received a demand pursuant to the provisions of the preceding paragraph and when it has become clear that there is a reason in the demand, fulfill a utilization cease etc. of the said retained personal data to the extent necessary to redress a violation without delay. This, however, shall not apply in cases where a utilization cease etc. of the said retained personal data requires a large amount of expenses or other cases where it is difficult to fulfil a utilization cease etc. and when necessary alternative action is taken to protect a principal's rights and interests.
3. A principal may, when retained personal data that can identify the principal is being provided to a third party in violation of the provisions of Article 15, Paragraph 1 or Article 16, demand of a telecommunications carrier the ceasing of a third-party provision of the retained personal data.

4. A telecommunications carrier shall, in case of having received a demand pursuant to the provisions of the preceding paragraph and when it has become clear that there is a reason in the demand, cease a third-party provision of the retained personal data without delay. This, however, shall not apply in cases where ceasing a third-party provision of the said retained personal data requires a large amount of expenses or other cases where it is difficult to cease a third-party provision and when necessary alternative action is taken to protect a principal's rights and interests.
5. A telecommunications carrier shall, when having fulfilled a utilization cease etc. or decided not to fulfill a utilization cease etc. of a whole or part of retained personal data in connection with a demand pursuant to the provisions of Paragraph 1, or when having ceased a third-party provision or decided not to cease a third-party provision of a whole or part of retained personal data in connection with a demand pursuant to the provisions of Paragraph 3, inform a principal to that effect without delay.

When a telecommunications carrier receives a principal's demand for a utilization cease or deletion (*1) (hereinafter referred to as a "utilization cease, etc.") of retained personal data that can identify the principal on the ground that such retained personal data is used for unintended purpose without the principal's consent in violation of the provisions of Article 5, or that personal information has been acquired by deceit or other improper means or special care-required personal information has been acquired without the principal's consent in violation of the provisions of Article 7, and if it turns out that such demand has reason, the telecommunications carrier must fulfill such utilization cease, etc. without delay, as a general rule (*2).

Furthermore, when a telecommunications carrier receives a principal's demand for a cessation of third-party provision of retained personal data that can identify the principal on the ground that such retained personal data has been provided to a third party without the principal's consent in violation of Article 15, Paragraph 1 or Article 16, and if it turns out that such demand has reason, the telecommunications carrier must cease such third-party provision without delay, as a general rule (*3).

Additionally, when a telecommunications carrier fulfills a utilization cease, etc. or decides to refrain from fulfilling a utilization cease, etc., or ceases such third-party provision or decides to refrain from ceasing such third-party provision, the telecommunications carrier must inform the principal (*4) without delay to that effect.

Furthermore, with regard to the relationship between this Article and the case in which a principal demands, by filing a lawsuit in court, a utilization cease, etc. or a cease of third-party provision of retained personal date that can identify the principal, see 3-6-8 (Advance Demand Before Filing a Lawsuit).

Incidentally, from the perspective of protecting the rights and interests of a principal such as a consumer, it is desirable to make further efforts to accommodate the principal's demand with

respect to retained personal data, for instance, by suspending delivery of direct mail or fulfilling a utilization cease on its own volition, taking into account the characteristics, scale and actual situation of business activities.

(*1) "Deletion" means an action of making such retained personal data unusable as retained personal data and includes not only deletion of such data but also deidentification of such data (see 3-3-1 (Assurance, etc. about the Accuracy of Data Contents)).

(*2) For instance, even where a demand for deletion of the entire retained personal data is made, if a breach of procedure may be cured by a utilization cease, then by taking such action, it will be deemed that the obligation has been fulfilled, and it is not always necessary to take an exact action as demanded.
Additionally, if the allegation of a breach of procedure is made incorrectly, it is unnecessary to fulfill a utilization cease, etc.

(*3) If the allegation of a breach of procedure is made incorrectly, it is unnecessary to cease the third-party provision.

(*4) For "informing a principal", see 2-11 (Informing a Principal).

(For Reference)

Article 30 of the Act

(1) A principal may, when retained personal data that can identify the principal is being handled in violation of the provisions of Article 16 or has been acquired in violation of the provisions of Article 17, demand of a personal information handling business operator a utilization cease or deletion (hereinafter referred to as a "utilization cease etc." in this Article) of the retained personal data.

(2) A personal information handling business operator shall, in case of having received a demand pursuant to the provisions of the preceding paragraph and when it has become clear that there is a reason in the demand, fulfill a utilization cease etc. of the said retained personal data to the extent necessary to redress a violation without delay. This, however, shall not apply in cases where a utilization cease etc. of the said retained personal data requires a large amount of expenses or other cases where it is difficult to fulfil a utilization cease etc. and when necessary alternative action is taken to protect a principal's rights and interests.

(3) A principal may, when retained personal data that can identify the principal is being provided to a third party in violation of the provisions of Article 23, paragraph (1) or Article 24, demand of a personal information handling business operator ceasing a third-party provision of the retained personal data.

(4) A personal information handling business operator shall, in case of having received a

demand pursuant to the provisions of the preceding paragraph and when it has become clear that there is a reason in the demand, cease a third-party provision of the retained personal data without delay. This, however, shall not apply in cases where ceasing a third-party provision of the said retained personal data requires a large amount of expenses or other cases where it is difficult to cease a third-party provision and when necessary alternative action is taken to protect a principal's rights and interests.

(5) A personal information handling business operator shall, when having fulfilled a utilization cease etc. or decided not to fulfill a utilization cease etc. of a whole or part of retained personal data in connection with a demand pursuant to the provisions of paragraph (1), or when having ceased a third-party provision or decided not to cease a third-party provision of a whole or part of retained personal data in connection with a demand pursuant to the provisions of paragraph (3), inform a principal to that effect without delay.

3-6-5 Explanation of Reason (in Relation to Article 23)

Article 23

A telecommunications carrier shall, in case of informing a principal to the effect that, as regards a whole or part of action requested or demanded by the principal pursuant to the provisions of Article 19, Paragraph 3; Article 20, Paragraph 3; Article 21, Paragraph 3; or Paragraph 5 of the preceding Article, the action will not be taken, or to the effect that different action from the said action will be taken, strive to explain a reason therefor to the said principal.

When a telecommunications carrier informs a principal (*) to the effect that, as regards a whole or part of action of the principal requesting or demanding notification of the utilization purpose of retained personal data, or disclosure, correction, etc., utilization cease, etc. of retained personal data, or cease of third-party provision (hereinafter referred to as a "demand, etc. for disclosure, etc."), the action will not be taken, or to the effect that a different action from the said action will be taken, the telecommunications carrier must strive to also explain a reason therefor to the principal.

(*) For "informing a principal", see 2-11 (Informing a Principal).

(For Reference)

Article 31 of the Act

A personal information handling business operator shall, in case of informing a principal to the effect that, as regards a whole or part of action requested or demanded by the principal

pursuant to the provisions of Article 27, paragraph (3); Article 28, paragraph (3); Article 29, paragraph (3); or the preceding Article, paragraph (5), the action will not be taken, or to the effect that different action from the said action will be taken, strive to explain a reason therefor to the said principal.

3-6-6 Procedure for Responding to a Demand, etc. for Disclosure, etc. (in Relation to Article 24)

Article 24

1. A telecommunications carrier may, as regards a request pursuant to the provisions of Article 19, Paragraph 2 or a demand pursuant to the provisions of Article 20, Paragraph 1; Article 21, Paragraph 1; or Article 22, Paragraph 1 or 3 (hereinafter referred to as a "demand etc. for disclosure etc." in this Article), decide on a method of receiving a request or demand pursuant to those prescribed in each of the following items. In this case, a principal shall make a demand etc. for disclosure etc. in accordance with the method.
   (1) where to file a demand etc. for disclosure etc.;
   (2) a format of a document to be submitted at the time of making a demand etc. for disclosure etc. and other forms wherein a demand etc. for disclosure etc. may be made;
   (3) a method of confirming that a person making a demand etc. for disclosure etc. is a principal or an agent prescribed in Paragraph 3;
   (4) a method of collecting a fee under Paragraph 1 of the next following Article.
2. A telecommunications carrier may, as regards a demand etc. for disclosure etc., request a principal to present a matter sufficient to specify retained personal data subject to the demand etc. In this case, a telecommunications carrier shall take appropriate action in consideration of a principal's convenience such as providing information conducive to specify the retained personal data so that the principal would be able to easily and precisely make a demand etc. for disclosure etc.
3. A demand etc. for disclosure etc. may be made through an agent pursuant to those prescribed in the following. This, however, shall not apply if the secrecy of communications of a principal may be violated or any item of Article 20, Paragraph 2 is otherwise applicable.
   (1) a statutory agent of a minor or adult ward;
   (2) an agent entrusted by a principal with making a demand etc. for disclosure etc.
4. A telecommunications carrier shall, in establishing a procedure for responding to a demand etc. for disclosure etc. based on the provisions of the preceding three paragraphs, give consideration so as not to impose excessive burden on a principal.

A telecommunications carrier may, as regards a demand, etc. for disclosure, etc. (*1), decide on a method of receiving the same by setting forth the matters in (1) through (4) below (*2).

Where the telecommunications carrier decides on the method of receiving a demand, etc. for disclosure, etc., it must put that into a state where a principal can know (including those cases in which it, at the request of a principal, responds without delay) (*3) (see 3-6-1 (Public Disclosure, etc. of Matters Relating to Retained Personal Data)).

Additionally, when a telecommunications carrier decides on a reasonable method of receiving a demand, etc. for disclosure, etc., a principal must make such demand, etc. for disclosure, etc. in accordance with such method, and if the principal does not comply with such method, the telecommunications carrier may reject such demand, etc. for disclosure, etc. (*4)

With regard to a demand, etc. for disclosure, etc., if a principal is in a remote location or ill or injured, or for such other reasons, then because the principal needs to be allowed to make such demand through his/her agent for the convenience of the principal, the principal may demand such disclosure, etc. through his/her agent specified in the respective items of Paragraph 3. Incidentally, if the secrecy of communications in respect of a principal may be violated by disclosing usage details, etc. to his/her agent, or if any of the respective items of Article 20, Paragraph 2 is applicable, the making of a demand through an agent will not be permitted.

Furthermore, for smooth operation of procedures for disclosure, etc., a telecommunications carrier may request that a principal provide necessary matters (such as an address, ID, password, and membership number) to specify retained personal data that can identify such principal as the subject of a demand, etc. for disclosure, etc. For instance, where a telecommunications carrier holds retained personal data at its respective business units or offices, or holds retained personal data by assorting them based on the date of acquisition thereof, the telecommunications carrier may, with regard to such demand for disclosure, etc., ask the principal to specify the category of retained personal data as the subject of such demand. In so asking, the telecommunications carrier must take the principal's convenience into consideration and provide information that is helpful for the specification of such retained personal data so that the principal can make a demand, etc. for disclosure, etc. easily and appropriately.

(1) Where to file a demand, etc. for disclosure, etc.
(Examples) Service window or department name, mailing address, telephone number, FAX number and email address for contact, etc.

(2) Format of a document to be submitted at the time of making a demand, etc. for disclosure, etc. and other forms wherein a demand, etc. for disclosure, etc. may be made
(Examples) To the effect that such demand, etc. may be made by mail, FAX, or email.

(3) Method of confirming that a person making a demand, etc. for disclosure, etc. is a principal

or an agent ((i) a statutory agent of a minor or adult ward; (ii) an agent entrusted by a principal with making a demand, etc. for disclosure, etc.) (*5)

(4) Method of collecting a fee in notifying the utilization purpose of retained personal data or disclosing retained personal data

(*1) "Demand, etc. for Disclosure, etc." refers to a request for notification of the utilization purpose of retained personal data (see 3-6-1 (Public Disclosure, etc. of Matters Relating to Retained Personal Data)), or a demand for disclosure of retained personal data (see 3-6-2 (Disclosure of Retained Personal Data)), correction, etc. (see 3-6-3 (Correction, etc. of Retained Personal Data), or utilization cease, etc. or cease of third-party provision of retained personal data (see 3-6-4 (Utilization Cease, etc. of Retained Personal Data)).

(*2) In deciding on a procedure for accommodating a demand, etc. for disclosure, etc., a telecommunications carrier must give considerations so that such procedure will be appropriate in view of the nature of business, how retained personal data are handled, how a demand, etc. for disclosure, etc. is accepted, etc., and must also give considerations to avoid putting an excessive burden on a principal: requesting to prepare a complex document more than necessary, limiting a service window for accepting such demand, etc. to extremely inconvenient locations separately from the site that conducts other services, for example.

(*3) For a "state where a principal can know (including those cases in which it, at the request of a principal, responds without delay)", see 3-6-1 (Public Disclosure, etc. of Matters Relating to Retained Personal Data).

(*4) It must be kept in mind that, if a telecommunications carrier does not provide for the method for accepting a demand, etc. for disclosure, etc., it means that a principal is allowed to make a request freely.

(*5) The method of confirmation must be appropriate in view of the nature of business, how retained personal data are handled, how a demand, etc. for disclosure, etc. is accepted, etc., and the telecommunications carrier must give considerations to avoid putting an excessive burden on a principal: requesting, for the purpose of verifying the identity, many items of information more than necessary compared to personal data held by the telecommunications carrier, for example.

Case 1) In the case of a principal: a driver's license; health insurance certificate; the front side of personal identification number card (My Number Card); passport; residence card; special permanent resident certificate; pension handbook; certificate of seal impression and registered seal.

Case 2) In the case of an agent: for each of the principal and his/her agent, a driver's license; health insurance certificate; the front side of personal identification number card (My Number Card); passport; residence card; special permanent resident certificate; pension handbook. In addition to the foregoing, for the agent, a power of attorney evidencing the authority (where a person who has parental authority shows that he/she is a statutory agent of a minor, a certified copy or abridged copy of family register or a copy of residence certificate that indicates both the principal and his/her agent and their relationship).

(For Reference)

Article 32 of the Act

(1) A personal information handling business operator may, as regards a request pursuant to the provisions of Article 27, paragraph (2) or a demand pursuant to the provisions of Article 28, paragraph (1); Article 29, paragraph (1); Article 30, paragraph (1) or paragraph (3) (hereinafter referred to as a "demand etc. for disclosure etc." in this Article and Article 53, paragraph (1)), decide on a method of receiving a request or demand pursuant to those prescribed by cabinet order. In this case, a principal shall make a demand etc. for disclosure etc. in accordance with the method.

(2) A personal information handling business operator may, as regards a demand etc. for disclosure etc., request a principal to present a matter sufficient to specify retained personal data subject to the demand etc. In this case, a personal information handling business operator shall take appropriate action in consideration of a principal's convenience such as providing information conducive to specify the retained personal data so that the principal would be able to easily and precisely make a demand etc. for disclosure etc.

(3) A demand etc. for disclosure etc. may be made through an agent pursuant to those prescribed by cabinet order.

(4) A personal information handling business operator shall, in establishing a procedure for responding to a demand etc. for disclosure etc. based on the provisions of the preceding three paragraphs, give consideration so as not to impose excessive burden on a principal.

Article 10 of the Cabinet Order

Those matters which a personal information handling business operator may prescribe as a method of receiving a demand etc. for disclosure etc. pursuant to the provisions of Article 32, paragraph (1) of the Act, shall be as set forth in the following:

(i) where to file a demand etc. for disclosure etc.;

(ii) a format of a document (including an electromagnetic record; the same shall apply in

Article 14, paragraph (1) and Article 21, paragraph (3)) to be submitted at the time of making a demand etc. for disclosure etc. and other forms wherein a demand etc. for disclosure etc. may be made;

(iii) a method of confirming that a person making a demand etc. for disclosure etc. is a principal or an agent prescribed in the following Article;

(iv) a method of collecting a fee under Article 33, paragraph (1) of the Act.

Article 11 of the Cabinet Order

An agent who may make a demand etc. for disclosure etc. pursuant to the provisions of Article 32, paragraph (3) of the Act shall be an agent set forth in the following:

(i) a statutory agent of a minor or adult ward;

(ii) an agent entrusted by a principal with making a demand etc. for disclosure etc.

3-6-7 Fee (in Relation to Article 25)

Article 25

1. A telecommunications carrier may, when having been requested to inform of a utilization purpose pursuant to the provisions of Article 19, Paragraph 2 or when having received a demand for disclosure pursuant to the provisions of Article 20, Paragraph 1, collect a fee in relation to taking such action.
2. A telecommunications carrier shall, in case of collecting a fee pursuant to the provisions of the preceding paragraph, decide on the amount of the fee within a range recognized as reasonable considering actual expenses.

When a telecommunications carrier receives a request for notification of a utilization purpose of retained personal data (Article 19, Paragraph 2) or receives a demand for disclosure of retained personal data (Article 20, Paragraph 1), the telecommunications carrier may set a fee for taking such action and collect the same.

Additionally, when the amount of such fee is set, such amount must be put into a state where a principal can know (including those cases in which it, at the request of a principal, responds without delay) (*) (Article 19, Paragraph 1, Item (3)).

Furthermore, when a fee is to be collected, the amount of such fee must be set within such range as considered reasonable in view of actual costs.

(*) For a “state where a principal can know (including those cases in which it, at the request of a principal, responds without delay)”, see 3-6-1 (Public Disclosure, etc. of Matters Relating to Retained Personal Data).

(For Reference)

Article 33 of the Act

(1) A personal information handling business operator may, when having been requested to inform of a utilization purpose pursuant to the provisions of Article 27, paragraph (2) or when having received a demand for disclosure pursuant to the provisions of Article 28, paragraph (1), collect a fee in relation to taking such action.

(2) A personal information handling business operator shall, in case of collecting a fee pursuant to the provisions of the preceding paragraph, decide on the amount of the fee within a range recognized as reasonable considering actual expenses.

3-6-8 Advance Demand before Filing a Lawsuit (in Relation to Article 26)

Article 26

1. A principal may, when intending to file a lawsuit in connection with a demand pursuant to the provisions of Article 20, Paragraph 1; Article 21, Paragraph 1; or Article 22, Paragraph 1 or 3, not file the lawsuit unless the principal had issued the demand in advance against a person who should become a defendant in the lawsuit and two weeks have passed from the delivery day of the issued demand. This, however, shall not apply when the person who should become a defendant in the lawsuit has rejected the demand.
2. A demand under the preceding paragraph is deemed as having been delivered at the time when such a demand should have normally been delivered.
3. The provisions of the preceding two paragraphs shall apply *mutatis mutandis* to a petition for a provisional disposition order in connection with a demand pursuant to the provisions of Article 20, Paragraph 1; Article 21, Paragraph 1; or Article 22, Paragraph 1 or 3.

When a principal intends to file a lawsuit against a telecommunications carrier in connection with a demand for disclosure of retained personal data that can identify the principal (*1), correction, etc. (*2), or utilization cease, etc. (*3) or cease of third-party provision (*4), the principal may not file the lawsuit unless the principal had issued in advance the demand against such telecommunications carrier out of court and two weeks have passed from the delivery day of the issued demand to such telecommunications carrier. (*5) (*6)

However, if the telecommunications carrier rejects the demand made out of court (*7), a lawsuit in court in connection with such demand may be filed before such two-week period has passed.

(*1) With regard to disclosure of retained personal data, see 3-6-2 (Disclosure of Retained Personal Data).

(*2) Correction, etc. of retained personal data refers to a correction, addition, or deletion of retained personal data (see 3-6-3 (Correction, etc. of Retained Personal Data)).

(*3) Utilization cease, etc. of retained personal data refers to a utilization cease or deletion of retained personal data (see 3-6-4 (Utilization Cease, etc. of Retained Personal Data)).

(*4) With regard to a cease of third-party provision of retained personal date, see 3-6-4 (Utilization Cease, etc. of Retained Personal Data).

(*5) For instance, if a principal's demand for disclosure of retained personal data against a telecommunications carrier is delivered on April 1, the principal may file a lawsuit in court in connection with such demand after two weeks have passed since such delivery data (namely, on and after April 16).

(*6) Likewise, when a principal intends to file a petition for order of provisional disposition in connection with disclosure of retained personal data that can identify the principal, correction, etc., or utilization cease, etc. or cease of third-party provision, the principal may not file the petition for order of provisional disposition unless the principal had issued the demand in advance against such telecommunications carrier in advance and two weeks have passed from the delivery day of the issued demand to such telecommunications carrier.

(*7) The phrase "if the [telecommunications carrier] rejects the demand made outside a court" includes cases set forth in Article 20, Paragraph 3, Article 21, Paragraph 3, and Article 22, Paragraph 5 as well as cases in which, for instance, a personal information handling business operator merely notifies the person making such demand of a rejection of such demand without giving any particular reason.

(For Reference)

Article 34 of the Act

(1) A principal may, when intending to file a lawsuit in connection with a demand pursuant to the provisions of Article 28, paragraph (1); Article 29, paragraph (1); or Article 30, paragraph (1) or paragraph (3), not file the lawsuit unless the principal had previously issued the demand against a person who should become a defendant in the lawsuit and two weeks have passed from the delivery day of the issued demand. This, however, shall not apply when the person who should become a defendant in the lawsuit has rejected the demand.

(2) A demand under the preceding paragraph is deemed as having been delivered at the time when such a demand should have normally been delivered.

(3) The provisions of the preceding two paragraphs shall apply mutatis mutandis to a petition for a provisional disposition order in connection with a demand pursuant to the provisions

of Article 28, paragraph (1); Article 29, paragraph (1); or Article 30, paragraph (1) or paragraph (3).

3-7 Dealing with a Complaint about the Handling of Personal Information (in Relation to Article 27)

Article 27

1. A telecommunications carrier shall deal appropriately and promptly with a complaint about the handling of personal information.
2. A telecommunications carrier shall establish a system necessary to achieve a purpose under the preceding paragraph.

A telecommunications carrier must deal appropriately and promptly with a complaint relating to the utilization, provision, disclosure, or correction, etc. of personal information or any other complaint about the handling of personal information.

Furthermore, in dealing with a complaint appropriately and promptly, the telecommunications carrier must set up a service window for handling of complaints, provide for the steps for handling complaints, or otherwise establish a necessary system (*1). Because it is difficult to provide for specific details of "appropriate and prompt dealing" uniformly for all telecommunications carrier, etc., and the telecommunications carrier is required to decide on specifics individually, but in the cases set forth below, the telecommunications carrier will not be regarded as taking appropriate and prompt actions at a minimum.

(i) Where a service window is not set up to accept complaints.
(ii) Where a service window for accepting complaints exists, but contact information or operating hours of such service window is not made clear to the public.
(iii) Where contact information or operating hours of a service window for accepting complaints is made clear to the public, such service window is scarcely available in fact (for instance, where a telephone contact cannot be reached despite numerous attempts to reach such contact by telephone, or where there is no response from an email contact service despite repeated attempts by emailing such contact).

However, this does not mean that a telecommunications carrier is required to accommodate unreasonable requests.

Additionally, with regard to where to file a complaint relating to the handling of retained personal data (if a telecommunications carrier is a covered business operator of an accredited personal information protection organization, including the name of such organization and where to make a request for resolution of a complaint), the telecommunications carrier must put such information to a state where a principal can know (including those cases in which it, at the request of a principal, responds without delay) (*2) (see 3-6-1 (Public Disclosure, etc. of Matters Relating

to Retained Personal Data)).

Furthermore, Article 27 of the Telecommunications Business Act sets forth that a telecommunications carrier must appropriately and promptly deal with complaints and inquiries from consumers, etc. with regard to telecommunications services and the method of operations relating to such services as set forth in the respective items of Article 26, paragraph (1), of such Act.

(*1) In order to establish a relationship of trust with a principal such as a consumer and ensure social trust in business activities, it is also important to draw up a "concept and policy in promoting the protection of personal information (so-called privacy policy, privacy statement, etc.)", disclose the same to the public by *inter alia* posting it on a web page or displaying at a conspicuous location in a store, and providing an easy-to-understand explanation in advance to the outside, indicating whether any subcontracting is made and the contents of administrative matters subject to subcontracting, and otherwise enhancing transparency with respect to subcontracting.

(*2) For a "state where a principal can know (including those cases in which it, at the request of a principal, responds without delay)", see 3-6-1 (Public Disclosure, etc. of Matters Relating to Retained Personal Data).

(For Reference)

Article 35 of the Act (1) A personal information handling business operator shall strive to deal appropriately and promptly with a complaint about the handling of personal information. (2) A personal information handling business operator shall strive to establish a system necessary to achieve a purpose under the preceding paragraph.

3-8 Duties of Anonymously Processed Information Handling Business Operators, etc. (in Relation to Articles 28 through 31)

<Production etc. of Anonymously Processed Information (in Relation to Article 28, Paragraph 1)> Article 28 (Paragraph 1) 1. A telecommunications carrier shall, when producing anonymously processed information (limited to those constituting anonymously processed information databases etc.; hereinafter the same), process personal information in accordance with standards set forth below as those necessary to make it impossible to identify a specific individual and restore

the personal information used for the production.

(1) deleting a whole or part of those descriptions etc. which can identify a specific individual contained in personal information (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the whole or part of descriptions etc.)

(2) deleting all individual identification codes contained in personal information (including replacing such codes with other descriptions etc. using a method with no regularity that can restore the individual identification codes)

(3) deleting those codes (limited to those codes linking mutually plural information being actually handled by a telecommunications carrier) which link personal information and information obtained by having taken measures against the personal information (including replacing the said codes with those other codes which cannot link the said personal information and information obtained by having taken measures against the said personal information using a method with no regularity that can restore the said codes)

(4) deleting idiosyncratic descriptions etc. (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the idiosyncratic descriptions etc.)

(5) besides action set forth in each preceding item, taking appropriate action based on the results from considering the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information and descriptions etc. contained in other personal information constituting the personal information database etc. that encompass the said personal information

<Security Control Actions, etc. for Anonymously Processed Information (in Relation to Article 28, Paragraphs 2 through 4, Article 28, Paragraph 7, and Article 31)>

Article 28 (Paragraphs 2 through 4 and 7)

2. A telecommunications carrier, when having produced anonymously processed information, shall, in accordance with standards set forth below as those necessary to prevent the leakage of information relating to those descriptions etc. and individual identification codes deleted from personal information used to produce the anonymously processed information, and information relating to a processing method carried out pursuant to the provisions of the preceding paragraph, take action for the security control of such information.

(1) defining clearly the authority and responsibility of a person handling processing method etc. related information (which refers to information relating to those descriptions etc. and individual identification codes which were deleted from

personal information used to produce anonymously processed information and information relating to a processing method carried out pursuant to the provisions of the preceding paragraph (limited to those which can restore the personal information by use of such relating information); the same shall apply hereinafter in this Article)

(2) establishing rules and procedures on the handling of processing method etc. related information, handling appropriately processing method etc. related information in accordance with the rules and procedures, evaluating the handling situation, and based on such evaluation results, taking necessary action to seek improvement

(3) taking necessary and appropriate action to prevent a person with no legitimate authority to handle processing method etc. related information from handling the processing method etc. related information

3. A telecommunications carrier, when having produced anonymously processed information, shall, without delay by utilizing the Internet or other appropriate method, disclose to the public the categories of information relating to an individual contained in the anonymously processed information.

4. In cases where a telecommunications carrier entrusted by another personal information handling business operator has produced anonymously processed information, the said other personal information handling business operator shall disclose the categories of information relating to an individual contained in the anonymously processed information by a method prescribed in the preceding paragraph. In such cases, it shall be deemed that the public disclosure of the said categories has been made by such telecommunications carrier.

7. A telecommunications carrier shall, when having produced anonymously processed information, strive to take itself necessary and appropriate action for the security control of the anonymously processed information and necessary action for ensuring the proper handling of the anonymously processed information such as dealing with a complaint about the handling, including producing, of the said anonymously processed information, and strive to disclose to the public the contents of such action taken.

Article 31

A telecommunications carrier as an anonymously processed information handling business operator shall strive to take itself necessary and appropriate action for the security control of anonymously processed information and necessary action to ensure the proper handling of anonymously processed information such as dealing with a complaint about the handling of anonymously processed information, and shall strive to disclose to the public the contents of such action taken.

<Third-Party Provision of Anonymously Processed Information (in Relation to Article 28, Paragraph 5 and Article 29)>

Article 28 (Paragraph 5)

5. A telecommunications carrier, when having produced anonymously processed information and providing the anonymously processed information to a third party, shall, by utilizing the Internet or other appropriate method, in advance disclose to the public the categories of information concerning an individual contained in anonymously processed information to be provided to a third party and its providing method, and state to the third party explicitly by emailing, in writing, or in other appropriate manner, to the effect that the information being provided is anonymously processed information.

Article 29

A telecommunications carrier as an anonymously processed information handling business operator, when providing anonymously processed information (excluding those which it produced itself by processing personal information; hereinafter the same in this Chapter) to a third party, shall, by utilizing the Internet or other appropriate method, in advance disclose to the public the categories of personal information contained in anonymously processed information to be provided to a third party and state to the third party explicitly by emailing, in writing, or in other appropriate manner, to the effect that the provided information is anonymously processed information.

<Prohibition against the Act of Identifying (in Relation to Article 28, Paragraph 6 and Article 30)>

Article 28 (Paragraph 6)

6. A telecommunications carrier shall, when having produced anonymously processed information and itself handling the anonymously processed information, not collate the said anonymously processed information with other information in order to identify a principal concerned with personal information used to produce the said anonymously processed information.

Article 30

A telecommunications carrier as an anonymously processed information handling business operator, shall, in handling anonymously processed information, neither acquire information relating to those descriptions etc. or individual identification codes deleted from the personal information and information relating to a processing method carried out pursuant to the provisions of Article 28, Paragraph 1; Article 44-10, paragraph (1) of the Act on the Protection of Personal Information Held by Administrative Organs (Act No.

58 of 2003) (including cases to which paragraph (2) of the said Article applies *mutatis mutandis*), or Article 44-10, paragraph (1) of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003) (including cases to which paragraph (2) of the said Article applies *mutatis mutandis*), nor collate the said anonymously processed information with other information in order to identify a principal concerned with personal information used to produce the anonymously processed information.

With regard to the duties of anonymously processed information handling business operators, the "*Guidelines for the Act on the Protection of Personal Information (for Anonymously Processed Personal Information)*" prescribed by the Personal Information Protection Commission shall apply *mutatis mutandis*.

Additionally, while location information handled by a telecommunications carrier includes location information relating to a base station, GPS location information, Wi-Fi location information, such information may include personal information covered by the secrecy of communications and is required to be protected from the perspective of privacy, and it is anticipated that such information will require an increased level of privacy protection due to further technological developments in the future. For that reason, in processing location information for deidentification, a telecommunications carrier is required to have an appropriate processing method and control and operational system. Because it is desirable to provide for a specific processing method, etc., depending on actual situations of the handling of location information, 5-4 (Location Information) addresses this matter, and the policy on the protection of personal information and other self-regulatory rules prepared by the relevant accredited personal information protection organization must be referenced as well.

(For Reference)

<Production etc. of Anonymously Processed Information (in Relation to Article 36, paragraph (1) of the Act)>

Article 36 of the Act (paragraph (1))

(1) A personal information handling business operator shall, when producing anonymously processed information (limited to those constituting anonymously processed information database etc.; hereinafter the same), process personal information in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to make it impossible to identify a specific individual and restore the personal information used for the production.

Article 19 of the Rules

Standards prescribed by rules of the Personal Information Protection Commission under Article 36, paragraph (1) of the Act shall be as follows.

(i) deleting a whole or part of those descriptions etc. which can identify a specific individual contained in personal information (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the whole or part of descriptions etc.)

(ii) deleting all individual identification codes contained in personal information (including replacing such codes with other descriptions etc. using a method with no regularity that can restore the individual identification codes)

(iii) deleting those codes (limited to those codes linking mutually plural information being actually handled by a personal information handling business operator) which link personal information and information obtained by having taken measures against the personal information (including replacing the said codes with those other codes which cannot link the said personal information and information obtained by having taken measures against the said personal information using a method with no regularity that can restore the said codes)

(iv) deleting idiosyncratic descriptions etc. (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the idiosyncratic descriptions etc.)

(v) besides action set forth in each preceding item, taking appropriate action based on the results from considering the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information and descriptions etc. contained in other personal information constituting the personal information database etc. that encompass the said personal information

<Security Control Actions, etc. of Anonymously Processed Information (in Relation to Article 36, paragraphs (2), (3) and (6) and Article 39 of the Act)>

Article 36 of the Act (Paragraphs 2, 3 and 6)

(2) A personal information handling business operator, when having produced anonymously processed information, shall, in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to prevent the leakage of information relating to those descriptions etc. and individual identification codes deleted from personal information used to produce the anonymously processed information, and information relating to a processing method carried out pursuant to the provisions of the preceding paragraph, take action for the security control of such information.

(3) A personal information handling business operator, when having produced anonymously

processed information, shall, pursuant to rules of the Personal Information Protection Commission, disclose to the public the categories of information relating to an individual contained in the anonymously processed information.

(6) A personal information handling business operator shall, when having produced anonymously processed information, strive to take itself necessary and appropriate action for the security control of the anonymously processed information and necessary action for ensuring the proper handling of the anonymously processed information such as dealing with a complaint about the handling, including producing, of the said anonymously processed information, and strive to disclose to the public the contents of such action taken.

Article 39 of the Act

An anonymously processed information handling business operator shall strive to take itself necessary and appropriate action for the security control of anonymously processed information and necessary action to ensure the proper handling of anonymously processed information such as dealing with a complaint about the handling of anonymously processed information, and shall strive to disclose to the public the contents of such action taken.

Article 20 of the Rules

Standards prescribed by rules of the Personal Information Protection Commission under Article 36, paragraph (2) of the Act shall be as follows.

(i) defining clearly the authority and responsibility of a person handling information relating to those descriptions etc. and individual identification codes which were deleted from personal information used to produce anonymously processed information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph (1) (limited to those which can restore the personal information by use of such relating information) (hereinafter referred to as "processing method etc. related information" in this Article.)

(ii) establishing rules and procedures on the handling of processing method etc. related information, handling appropriately processing method etc. related information in accordance with the rules and procedures, evaluating the handling situation, and based on such evaluation results, taking necessary action to seek improvement

(iii) taking necessary and appropriate action to prevent a person with no legitimate authority to handle processing method etc. related information from handling the processing method etc. related information

Article 21 of the Rules

(1) Public disclosure pursuant to the provisions of Article 36, paragraph (3) of the Act shall,

without delay after anonymously processed information has been produced, be made by utilizing the Internet or other appropriate method.

(2) In cases where a personal information handling business operator entrusted by another personal information handling business operator has produced anonymously processed information, the said other personal information handling business operator shall disclose the categories of information relating to an individual contained in the anonymously processed information by a method prescribed in the preceding paragraph. In such cases, it shall be deemed that the public disclosure of the said categories has been made by the said entrusted personal information handling business operator.

<Third-Party Provision of Anonymously Processed Information (in Relation to Article 36, paragraph (4) and Article 37 of the Act)>

Article 36 of the Act (paragraph (4))

(4) A personal information handling business operator, when having produced anonymously processed information and providing the anonymously processed information to a third party, shall, pursuant to rules of the Personal Information Protection Commission, in advance disclose to the public the categories of information concerning an individual contained in anonymously processed information to be provided to a third party and its providing method, and state to the third party explicitly to the effect that the information being provided is anonymously processed information.

Article 37 of the Act

An anonymously processed information handling business operator, when providing anonymously processed information (excluding those which it produced itself by processing personal information; hereinafter the same in this Section) to a third party, shall, pursuant to rules of the Personal Information Protection Commission, in advance disclose to the public the categories of personal information contained in anonymously processed information to be provided to a third party and state to the third party explicitly to the effect that the provided information is anonymously processed information.

Article 22 of the Rules

(1) Public disclosure pursuant to the provisions of Article 36, paragraph (4) of the Act shall be made by utilizing the Internet or other appropriate method.

(2) An explicit statement pursuant to the provisions of Article 36, paragraph (4) of the Act shall be given by sending an e-mail, delivering a written document or employing other appropriate method.

Article 23 of the Rules

(1) The provisions of the preceding Article, paragraph (1) shall apply mutatis mutandis to public disclosure pursuant to the provisions of Article 37 of the Act.

(2) The provisions of the preceding Article, paragraph (2) shall apply mutatis mutandis to an explicit statement pursuant to the provisions of Article 37 of the Act.

<Prohibition against the Act of Identifying (in Relation to Article 36, paragraph (5) and Article 38 of the Act)>

Article 36 of the Act (paragraph (5))

(5) A personal information handling business operator shall, when having produced anonymously processed information and making itself handle the anonymously processed information, not collate the said anonymously processed information with other information in order to identify a principal concerned with personal information used to produce the said anonymously processed information.

Article 38 of the Act

An anonymously processed information handling business operator, shall, in handling anonymously processed information, neither acquire information relating to those descriptions etc. or individual identification codes deleted from the personal information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph (1), Article 44-10, paragraph (1) (including as applied mutatis mutandis pursuant to the same Article, paragraph (2)) of the Act on the Protection of Personal Information Held by Administrative Organs (Act No. 58 of 2003), or Article 44-10, paragraph 1(including as applied mutatis mutandis pursuant to the same Article, paragraph (2)) of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, nor collate the said anonymously processed information with other information in order to identify a principal concerned with personal information used to produce the anonymously processed information.

4 Measures upon the Occurrence of an Incident of Leakage, etc.

If a leakage, etc. (*) of personal data handled by a telecommunications carrier (including those handled by a contractor) occurs, the telecommunications carrier shall take actions that are desirable for such telecommunications carrier to take from the perspective of preventing secondary damage and preventing a similar incident, as prescribed by the Personal Information Protection Commission. Additionally, upon the occurrence of a leakage in breach of the secrecy of communications set forth in Article 2, paragraph (5) of the Telecommunications Business Act, a telecommunications carrier has the duty to report to the Minister of Internal Affairs and Communications under Article 28 of such Act, and accordingly, the telecommunications carrier must report to the Minister of Internal Affairs and Communications such incident of leakage of personal information in breach of the secrecy of communications.

(*) "Leakage, etc." refers to a leakage, loss or damage (see 3-3-4 (Security Control Action)).

5 Handling of Various Types of Information (Chapter III)

5-1 Recording of Communications History (in Relation to Article 32)

5-1-1 Recording of Communications History (in Relation to Article 32, Paragraph 1)

Article 32
1. A telecommunications carrier may record communications history (which refers to dates and times of the user's use of telecommunications, counterparties in such telecommunications and other information concerning the user's telecommunications other than contents of such telecommunications; the same shall apply hereinafter) only where necessary in order to charge fees, issue invoices, respond to complaints, prevent unauthorized use, or conduct other operations.

Communications history is a component of communications and protected as a secret in communications, and recording it could breach the secrecy of communications. However, if it is necessary in order to charge fees, issue invoices, respond to complaints, ensure security of the system it controls, or otherwise conduct other operations, recording communications history to the minimum extent necessary is deemed at least as a lawful business act, and there is justifiable cause for noncompliance with the law.

Recording and storing communications history to the extent necessary in order to prepare usage details (see Article 33, Paragraph 1) is a legitimate right of a telecommunications carrier as an obligee in the point that it should have the ability to calculate usage fees and present a basis for charging such fees, therefore the telecommunications carrier may record and store communications history to the extent necessary in order to prepare usage details as a lawful

business act without obtaining the subscriber's consent.

Incidentally, because analysis of communications history to identify a sender is regarded as unintended use and breaches the secrecy of communications, such analysis cannot be conducted unless it complies with a warrant issued by a judge or is regarded as a lawful business act, or if there is other justifiable cause for noncompliance with the law.

<Examples if there is justifiable cause for noncompliance with the law as a lawful business act>

Case) If, in communications which are of a public nature such as web pages on the Internet, any illegal or harmful content is posted, and the provision of services by a telecommunications carrier may be interfered unless it gives a warning to the sender of such content (for instance, access from its service domain may be blocked), the telecommunications carrier may identify the sender in communications history that its holds for the purpose of identifying the sender and giving a warning, etc.

Communications history once recorded must be deleted (including not only deletion of information covered by the secrecy of communications but also deidentification of personal information which is not so covered) promptly after the elapse of a retention period established to the minimum extent necessary in order to achieve the purpose of recording. Furthermore, even if such retention period is not established, communications history must be deleted promptly after the purpose of recording it is achieved.

A retention period may vary for each telecommunications carrier, depending on the type of service provided, method of charging fees, etc. as well as the type of communications history, but such retention period must be established to a limited extent, in view of *inter alia* the necessity in conducting the business and the consequences of retention and so that the purpose of retention will not be ignored (*).

However, if the provisions of laws and regulations relating to requests for preservation of electromagnetic records of communications history under Article 197, Paragraphs 3 and 4 of the Code of Criminal Procedure apply, or if there is any other special reason, such records may be retained until the retention period based on such reason expires. Furthermore, if communications history is required to be retained as an emergency action to protect the right of the telecommunications carrier or a third party, then such records may be retained until it becomes no longer necessary to retain them.

(*) For instance, of all types of communication history, with regard to connection authorization logs in Internet connection service (records of authorization of a user and allocation of an IP address required for the Internet connection), while the retention of such history is highly necessary for the operation, for the purpose of responding to users' inquiries relating to contracts and usage situations, etc. and

using such history for security measures, because it has a relatively small relevance to expressions or privacy of users, such communications history may be retained for about six months in general if it is necessary in order for the telecommunications carrier to conduct its business, and the telecommunications carrier may be allowed to retain such communications history for about one year if a longer retention period is required for operational reasons, such as where the telecommunications carrier needs to keep track of the situations throughout a year from the perspective of ensuring appropriate network operations.

5-1-2 Provision of Communications History (in Relation to Article 32, Paragraph 2)

Article 32 2. A telecommunications carrier shall not provide communications history to others except in any of the following cases: where the user's consent has been obtained, where such provision is made to comply with a warrant issued by a judge, in the event of self-defense or necessity, or if there is other justifiable cause for noncompliance with the law.

Because communications history is protected as a secret in communications, a telecommunications carrier must not provide the same to the outside except where the corresponding person's consent has been obtained, where such provision is made to comply with a warrant issued by a judge, or otherwise if there is justifiable cause for noncompliance with the law. Because there is not necessarily cause for noncompliance with the law in providing communications history in response to an inquiry by a person who has the legal authority to make such inquiry, it is not appropriate to make such provision as a general rule (see 3-5-1 (Principles of Restrictions on Third-Party Provision)).

<Examples where there is justifiable cause for noncompliance with the law as a lawful business act>

Case) Where direct mail is mass-mailed at random, as in the case of an obstruction of business by damaging a computer (Article 234-2 of the Penal Code), and a telecommunications carrier's network or service is threatened, and it is recognized as inevitable to defend its own and/or others' rights, and the relevant portion of communications history (such as the sender's IP Address, time stamp, etc.) is provided to the originating telecommunications carrier in order to ask it to take an action to prevent the transmission of such direct mail.

5-2 Usage Details (in Relation to Article 33)

5-2-1 Indication of Usage Details (in Relation to Article 33, Paragraph 1)

> Article 33
> 1. The scope of information which a telecommunications carrier indicates in a statement of usage details (which refers to a statement that indicates dates and times of the user's use of telecommunications, recipients of such telecommunications, corresponding billing information, and other information concerning the user's use of such telecommunications; the same shall apply hereinafter) shall not exceed the extent necessary in order to achieve the purpose of a statement of usage details.

For a telecommunications carrier, usage details are a basis for charging fees, and a subscriber is able to confirm such fees by using such usage details. Accordingly, they are of significance to both parties, but on the other hand, the usage details nearly constitute communications history covered by the secrecy of communications, and for that reason, considerations must be given to the secrecy of communications and the principal's privacy. To that end, a telecommunications carrier must limit matters included in a statement of usage details to necessary matters to indicate a basis for charging fees, such as the date and time of transmission, duration of transmission, telephone number of a recipient, amount billed for each transmission, and destination location in the case of international transmission. Furthermore, it is desirable to take a measure such as omitting the last four digits of telephone number in the statement if the subscriber so wishes. Additionally, it is not appropriate to include in the statement any unnecessary information that violates the privacy of a recipient of transmission (*).

(*) For instance, if the recipient of transmission uses a mobile phone or PHS, and if there is any fee arrangement with the recipient's location or based on the distance with the recipient, then information concerning the recipient's location is necessary as a basis for charging fees. Accordingly, it is permissible to include information such as which fee rate area to which the recipient belongs, but further indication of detailed information regarding the recipient's location is likely to unduly violate the privacy of the recipient of transmission, and accordingly it is inappropriate.

5-2-2 Viewing, etc. of Usage Details (in Relation to Article 33, Paragraph 2)

> Article 33
> 2. In allowing a subscriber or other permitted person to view a statement of usage details or delivering such statement, a telecommunications carrier shall take necessary measures so as not to violate the user's secrecy of communications and personal information without

due cause.

The person who may view usage details is, basically, the subscriber; however, any constant user other than the subscriber or a fee payor who is not the subscriber may also have a legitimate interest in viewing such usage details (incidentally, when allowing any person other than the subscriber to view the same, the subscriber's consent must be obtained).

In issuing a statement of usage details, a telecommunications carrier must take necessary measures, such as forwarding it as a sealed letter, from the perspective of the secrecy of communications and protection of personal information. Furthermore, because a statement of usage details may include information relating to temporary users' communications, the telecommunications carrier must ensure that the secrecy of communications, privacy, etc. on the part of such user will not be violated unduly.

5-3 Caller Information (Article 34)

5-3-1 Display of Caller Information (in Relation to Article 34, Paragraph 1)

Article 34
1. When a telecommunications carrier provides a caller information display service (which refers to a telephone service of notifying the recipient of the telephone number of a caller, caller location information, etc., and such other information concerning the caller (hereinafter referred to as the "Caller Information"); the same shall apply hereinafter), the telecommunications carrier shall provide a function to prevent the display of the Caller Information for each instance of communications.

"Caller information" refers to information concerning the caller and may be a telephone number, name, address, birth date, and other description that is included in such information, a number, symbol, or other code assigned to each individual, or anything that can identify the caller visually or orally. A caller telephone number displayed in a caller number display service or a caller name displayed in a caller name display service falls under the category of caller information, and if information such as a face photo of the caller or a location of the caller is transmitted, such information is also regarded as caller information. Additionally, the term "telephone service" includes subscribed telephone, ISDN, mobile phone and PHS services as well as IP telephone services.

Because caller information is typically covered by the secrecy of communications, a telecommunications carrier must, in providing a caller information display service, set up a function to prevent the display of the caller information for each instance of communications from the perspective of having the caller determine whether to display the caller information. If the caller does not choose to prevent the display of caller information, then the secrecy of

communications will not be deemed breached because the caller is recognized as having no intention to keep the caller information secret from the recipient.

5-3-2 Provision of Caller Information (in Relation to Article 34, Paragraph 2)

Article 34 2. In providing a caller information display service, a telecommunications carrier shall take measures necessary in order to secure the user's rights.

Because the caller must adequately understand specifics of the caller information display service before the caller is recognized as having no intention to keep the caller information from the recipient, the telecommunications carrier is required to take measures such as ensuring that users are adequately aware of information to be displayed in order to protect users' right and how to prevent the display (*).

(*) With regard to the caller information display service, the "*Guidelines for the Protection of Caller's Personal Information in Connection with Utilization of Caller Information Display Service*" were prepared in 1996, and in providing such service, a telecommunications carrier must ask the subscriber to respect such Guidelines.

5-3-3 Restriction on Provision of Caller Information (in Relation to Article 34, Paragraph 3)

Article 34 3. A telecommunications carrier shall not provide Caller Information to others except where such provision is necessary for the provision of the caller information display service or other services. The foregoing, however, shall not apply where the user's consent has been obtained; where such provision is made to comply with a warrant issued by a judge; where an actual crime of intimidation by phone is being committed and a phone call of an offender is traced upon a request of a victim or an investigating authority; where an emergency call is made to report that a human life, body, etc. is in imminent danger and a phone call is traced upon a request of such informant; or if there is other justifiable cause for noncompliance with the law.

A telecommunications carrier must not provide caller information to others except where such provision is necessary for the provision of the caller information display service or other services (*). The foregoing, however, shall not apply, for instance, where a phone call is traced upon the satisfaction of necessity, or if there is justifiable cause for noncompliance with the law.

Additionally, with regard to an emergency call, because a caller is believed to have the intention to inform an emergency call accepting institution of the site location or his/her location under normal circumstances, in order to have the emergency call accepting institution act on such call immediately, the caller information shall be displayed as a general rule even if the caller chooses to have his/her caller information not displayed for regular calls other than emergency calls, and it is permitted to have an arrangement that the number will not be displayed only for instances as to which the user chooses to use the function to prevent the number display. However, when such arrangement is made, it is necessary to ensure that the user is adequately aware that (i) in the case of an emergency call, the caller information shall be displayed as a general rule even if the caller chooses to have his/her caller information not displayed for regular calls other than emergency calls, and (ii) how to prevent the caller information from being displayed for each instance in the case of an emergency call.

(*) For instance, as cases "where such provision is necessary for the provision of…other services", cases in which caller number information is exchanged between telecommunications carriers for the purpose of charging fees or for the operation of networks to the extent necessary or in which information that can specify the caller is provided to the recipient in a collect call are anticipated.

5-4 Location Information (in Relation to Article 35)

5-4-1 Acquisition of Location Information (in Relation to Article 35, Paragraph 1)

Article 35

1. A telecommunications carrier may obtain location information (which refers to certain information which indicates a location of a mobile device holder and which is not Caller Information; the same shall apply hereinafter) only where the user's prior consent has been obtained; where such activity is conducted in pursuit of a lawful business in relation to the provision of telecommunications service; or if there is other justifiable cause for noncompliance with the law.

The term "mobile device" in this Article refers to a mobile telephone device (Article 2, paragraph (2), item (v) of the Terminal Facilities Rules (Ministry of Posts and Telecommunications Order No. 31 of 1985)) and a wireless paging terminal (Article 2, paragraph (2), item (xi) of such Rules) as well as other devices used for facilitating communications by using electric waves, etc. broadly. Additionally, the term "location information" refers to information that indicates a place at which the holder of a mobile device is located (and that indicates a base station area or a location registration area or a range narrower than those, but does not include areas such as an incoming area indicated in a statement of usage details (fee rate area, etc.)), and

is a broader term than location information defined in Article 22 of the Terminal Facilities Rules (it is noted that, because the handling of information that indicates the location of a caller is provided in the preceding Article, such information is excluded from the definition of location information).

Location information held by a telecommunications carrier is protected under the secrecy of communications because such information is a component of communications if it relates to an individual instance of communications, and the telecommunications carrier is not permitted to acquire such information except where the consent of a user (the holder of a mobile device) has been obtained in advance, where such acquisition is a lawful business act in providing a telecommunications service, or if there is other justifiable cause for noncompliance with the law.

In this regard, a "lawful business act" refers to, from the perspective of providing telecommunications services, an act which is for a legitimate business purpose and which is deemed necessary in order to achieve such purpose and deemed reasonable in its means. For instance, an act of acquiring location information such as location registration information, etc. at a base station, etc. for facilitating communications by a cellular phone is considered to be a lawful business act.

In contrast, location registration information, which is not part of an individual instance of communications, but is sent to a telecommunications carrier as the holder of a mobile devices moves from one area to another, is merely information that is mechanically sent to the telecommunications to facilitate individual instances of communications, and accordingly, it is believed that such location information accumulated at a service control station is not protected under the secrecy of communications, but is rather protected as a privacy matter. Of course, even in the case of location information not covered by the secrecy of communications, a location of a certain person is a matter that needs to be highly protected among all privacy issues, and because it is a matter closely associated with communications, it is appropriate to give such information a high level of protection. Accordingly, even in the case of location information not covered by the secrecy of communications, it is strongly expected that such information is acquired only where the user's prior consent has been obtained, where such activity is conducted in pursuit of a lawful business in relation to the provision of telecommunications service, or if there is other justifiable cause for noncompliance with the law.

Incidentally, Paragraphs 4 and 5 illustrate cases where location information can be acquired other than the cases where the user's prior consent has been obtained and where such activity in conducted in pursuit of a lawful business in relation to the provision of telecommunications service.

5-4-2 Use of Location Information (in Relation to Article 35, Paragraph 2)

Article 35 2. A telecommunications carrier may provide to others or otherwise use location information only where the user's prior consent has been obtained; where such provision is made to comply with a warrant issued by a judge; or if there is other justifiable cause for noncompliance with the law.

A telecommunications carrier must not provide to others or otherwise use location information except where the user's prior consent has been obtained; where such provision is made to comply with a warrant issued by a judge; or if there is other justifiable cause for noncompliance with the law.

Accordingly, when location information, which is covered by the secrecy of communications, is deidentified and then provided to others or otherwise used, such location information must be sufficiently deidentified so that such location information cannot be associated with individual instances of communications, and the user's prior consent must be obtained with regard to such deidentification and provision to others or other uses. In such case, as a general rule, a valid consent cannot be regarded as obtained unless an individual, specific and clear consent is obtained, but where a telecommunications carrier ensures the user is fully aware of the terms and conditions of a contract, and is able to change the terms of the user's agreement subsequently without any harm from time to time and to request that such location information will not be deidentified and used thereafter, and as a result so that the user may avoid any risk of suffering any unforeseen harm, and if it can be anticipated that an ordinary user would permit the use of such information upon deidentification in view of (i) the scope of information to be deidentified and (ii) the appropriateness of the processing method and the administrative and operational system, then it shall be deemed that a valid consent has been given even by a prior blanket consent under the terms and conditions of the contract.

Even in the case of location information not covered by the secrecy of communications, because a location of a certain person is a matter that needs to be highly protected among all privacy issues and because it is a matter closely associated with communications, it is appropriate to give such information a high level of protection. Accordingly, in providing to others or otherwise using such information, it is strongly expected that such provision to others and other use of such information is limited to cases where the user's prior consent has been obtained or if there is justifiable cause for noncompliance with the law. Additionally, for the case where anonymously processed information is prepared in connection with location information, see 3-8 (Duties of Anonymously Processed Information Handling Business Operators, etc.).

5-4-3 Necessary Measures in Order to Prevent Undue Violation of Rights (in Relation to Article 35, Paragraph 3)

> Article 35
> 3. When a telecommunications carrier provides or has a third party provide a service to inform a subscriber or his or her designees of location information, it is appropriate for such telecommunications carrier to take necessary measures in order to prevent undue violation of the user's rights.

When a telecommunications carrier provides or has a third party provide location information, it is appropriate for such telecommunications carrier to take necessary measures in order to prevent undue violation of the user's rights, taking into consideration a balance between the social usefulness of such information and the secrecy of communications or privacy protection.

Specific actions of "necessary measures" may be: (i) provision of location information based on the user's intentions; (ii) securing of the user's awareness and foreseeability with regard to the provision of location information; (iii) appropriate handling of location information; and (iv) where a service is provided through collaboration with a third party, considerations to the protection of the user's privacy by having provisions such as terms and conditions in relation to an agreement for the collaboration.

With regard to the provision of location information based on the user's intentions in (i), the user's consent may be obtained for each provision of location information, or in advance at the time when the service provision is commenced. However, the consent should be obtained in a clear manner through an operation of a mobile device, through confirmation in writing, or in such other manner, and even in the case of location information not covered by the secrecy of communications, it is not desirable to obtain a blanket consent for all occasions, and it is desirable to specify the scope of persons who provide location information. Furthermore, the prior consent must be irrevocable as a general rule.

With regard to the securing of the user's awareness and foreseeability with regard to (ii), the user may be made aware of the provision of location information by a display on the screen, a vibration of a mobile device, and such other method. Furthermore, it is desirable that the user is able to check the history for a reasonable period and that the user is made sufficiently aware or warned about the service provided or the functions of a mobile device for the purpose of preventing location information from being released by mistake.

With regard to the appropriate handling of location information in (iii), so that an unauthorized person would not be able to view location information of a mobile device, measures such as the setup of a PIN and limitation of devices with access may be taken, and furthermore, where a telecommunications carrier has a different telecommunications carrier provide a location information service, the regulations on management of base station information may be established so that base station information managed by the former telecommunications carrier

would not be used unduly by others.

With regard to the provision of service through collaboration with a third party in (iv), by way of terms and conditions, etc. relating to a collaboration agreement, the measures for privacy protection on the part of the third party may be secured, or if it turns out that the user's privacy is unduly breached, the provision of location information shall be suspended.

Incidentally, even where a mobile device is mounted on an object and information of where such object is located is traced, because the right of the holder of such device may be infringed through such object, it is considered appropriate to take necessary measures similar to the foregoing.

5-4-4 Acquisition of Location Information upon Request of Investigative Authority (in Relation to Article 35, Paragraph 4)

Article 35
4. When a telecommunications carrier is asked by an investigating authority to obtain certain location information, such location information may be obtained only to comply with a warrant issued by a judge.

It is regarded that location information is protected under the secrecy of communications because such information is a component of communications if it relates to an individual instance of communications. Furthermore, even if location information does not relate to individual instances of communications and is not covered by the secrecy of communications, a location of a certain person is a matter that needs to be highly protected among all privacy issues, and because it is a matter closely associated with communications, if location information is sought by an investigative authority, such location may be acquired only in accordance with a warrant issued by a judge.

5-4-5 Acquisition of Location Information upon Request by a Rescuing Institution (in Relation to Article 35, Paragraph 5)

Article 35
5. In addition to the preceding paragraph, when a telecommunications carrier is asked by the police, the Japan Coast Guard, a fire department, or any other institution similar to the forgoing, which searches for a person who needs to be rescued and conducts rescue activities, to obtain such rescuee's location information, such telecommunications carrier may obtain such location information only if it is recognized that such rescuee's life or body is in imminent and great danger and that such location information is indispensable

in order to find such rescuee expeditiously.

GPS location information, which is not the kind of information necessary to facilitate communications, is not covered by the secrecy of communications and should be treated as a privacy issue, and it is information involving a significant privacy issue in comparison with location information associated with a base station.

Accordingly, a telecommunications carrier may acquire GPS location information in an emergency situation only where (i) the life or body of a person who needs to be aided or rescued (hereinafter referred to as a "rescuee") is in imminent and great danger and (ii) the acquisition of GPS location information pertaining to such rescuee is indispensable in order to find such rescuee expeditiously. Furthermore, as to whether these requirements are met, because it is indispensable to procure a professional assessment by the police, the Japan Coast Guard, a fire department, etc. or any other institution with the authority, knowledge and responsibility (hereinafter referred to as a "rescuing institution") based on objective facts put together based on a story provided by a family member or other involved persons of the rescuee in order to search for such person in such situation and conduct a rescue, it is strongly urged that the acquisition of such information is limited to a case where such rescuing institution makes a request. Additionally, even if such acquisition is based on a rescuing institution's request, in order for a telecommunications carrier to take an appropriate measure upon receiving a request for acquisition and provision of GPS location information, it is necessary to be furnished with (i) the rescuing institution's determination that the requirements above are met based on the objective facts as described above and (ii) a reason sufficient to warrant the reasonableness of such determination.

5-5 Exchange of Non-paying Person Information (in Relation to Article 36)

5-5-1 Exchange of Non-paying Person Information (in Relation to Article 36, Paragraphs 1 through 3)

Article 36
1. A telecommunications carrier may exchange with another telecommunications carrier non-paying person information (which refers to the name, address, unpaid amount, telephone number, or other information concerning a person who fails to pay fees for a telecommunications service past the due date, or a person named in a contract concerning the provision of mobile voice communications services in the cases under the respective items of Article 11 of the Act on Identification, etc. by Mobile Voice Communications Carriers of their Subscribers, etc. and for Prevention of Improper Use of Mobile Voice Communications Services (Act No. 31 of 2005); the same shall apply hereinafter) only if such exchange is recognized as particularly necessary and appropriate in order to prevent

non-payment of fees for telecommunications services or unauthorized use of mobile voice communications services. The foregoing, however, shall not apply if it is recognized that the principal's rights and interests will be violated without due cause by exchanging such non-paying person information.

2. When a telecommunications carrier exchanges non-paying person information with another telecommunications carrier, it is appropriate for such telecommunications carrier to inform a principal in advance of, or put them into a state where a principal can easily know, such exchange as well as items of non-paying person information to be exchanged, the scope of telecommunications carriers exchanging such information, and the name or appellation of a person in charge of the management of non-paying person information to be exchanged.
3. When a telecommunications carrier changes the name or appellation of the person in charge of the management of non-paying person information to be exchanged pursuant to the preceding paragraph, it is appropriate for such telecommunications carrier to inform a principal in advance of, or put them into a state where a principal can easily know, the specifics of such change.

Because "non-paying person information" includes the name, address, birth date, unpaid amount, or other information concerning a person who fails to make payments, and constitutes personal information, a telecommunications carrier is not permitted to provide such information to the outside without permission.

However, for instance, mobile device businesses have experienced problems such as follows:

- There are more and more cases where a person whose contract was terminated by a different business operator due to the failure to pay fees executes a contract with a new business operator, and again such person does not pay fees to such new business operator.
- A business operator executes a contract with a person against whom a different business operator suspended the provision of service for a reason such as such person refused a verification of his/her identity, and as a result, the contracting business operator cannot invoice or has severe difficulty in invoicing fees because of the inability to verify his/her identity likewise, which leads to unauthorized use such as an emergence of mobile phones whose owner is unidentifiable.

In order to resolve these problems, a special need has been acknowledged to allow an exchange of a minimum amount of non-paying person information and prevent non-paying persons, etc. from entering into new contracts, and thereby reduce operational risk. To this end, a telecommunications carrier may exchange non-paying person information with another telecommunications carrier by having an explicit provision to that effect in contractual terms and conditions where the subscriber's consent has been obtained (accordingly, this falls under the case where personal information is provided to a third party upon obtaining a principal's consent under

Article 15, Paragraph 1) and where the legitimate right of a principal (non-paying person, etc.) required to be protected is protected.

For this purpose, so as not to "infringe the rights and interests of a principal", it is appropriate to take measures such as limiting the subject of such information exchange to those whose contracts have been terminated and who are actually not paying and those who are named contractors where the respective items of Article 11 of the "Act on Identification, etc. by Mobile Voice Communications Carriers of their Subscribers, etc. and for Prevention of Improper Use of Mobile Voice Communications Services" (Act No. 31 of 2005) and subscribers are well informed of the system of such exchange in accordance with Paragraphs 2 and 3.

Furthermore, in utilizing the data so exchanged, careful handling of such data is required so as not to breach the duty of provision under the Telecommunications Business Act, for example, through the measures such as follows: limiting those who will be rejected for subscription by using the exchanged non-paying person information to delinquent persons whose delinquent amount exceeds a certain amount; utilizing a deposit, etc. for persons whose delinquent amount is below a certain amount; and accepting an application for screening for subscription if the respective items of Article 11 of the "Act on Identification, etc. by Mobile Voice Communications Carriers of their Subscribers, etc. and for Prevention of Improper Use of Mobile Voice Communications Services" (Act No. 31 of 2005) becomes no longer applicable to the telecommunications carrier which provided the exchanged information.

Incidentally, Articles 17 and 18 are applicable to the exchange of non-paying person information as well.

5-5-2 Restriction on Utilization Purpose of Non-Paying Person Information (in Relation to Article 36, Paragraph 4)

Article 36
4. It is appropriate for a telecommunications carrier which has exchanged non-paying person information to refrain from using such non-paying person information for any purpose other than screening at the time of entering into a subscription contract.

Non-paying person information exchanged is a type of personal credit information and must not be used for any purpose other than intended.

5-5-3 Appropriate Management of Non-paying Person Information (in Relation to Article 36, Paragraph 5)

Article 36 5. It is appropriate for a telecommunications carrier which has provided or received non-paying person information to take all possible measures, in particular, to manage such non-paying person information in an appropriate manner.

A principal's rights and interests are likely to be violated if non-paying person information is not current or accurate or a leakage, etc. of such information occurs. Accordingly, it is appropriate for a telecommunications carrier which has provided or received non-paying person information to take all possible measures, in particular, to manage such non-paying person information in an appropriate manner.

5-6 Subscriber Information Concerning Sending of Unsolicited Email, etc. (in Relation to Article 37)

5-6-1 Exchange of Subscriber Information Concerning Sending of Unsolicited Email, etc. (in Relation to Article 37, Paragraphs 1 through 3)

Article 37 1. A telecommunications carrier may exchange with another telecommunications carrier subscriber information (which refers to a subscriber's name, address, and other information concerning such subscriber against whom a telecommunications carrier has taken usage suspension measures or whose contract has been terminated because such subscriber sent electronic mail to many persons simultaneously in violation of the provisions of the Act on Regulation of Transmission of Specified Electronic Mail (Act No. 26 of 2002) or otherwise sent electronic mail which is likely to cause hindrances to transmission and reception of electronic mails; the same shall apply hereinafter) if such exchange is recognized as particularly necessary and appropriate in order to prevent hindrances to transmission and reception of electronic mails due to simultaneous transmission to many persons. The foregoing, however, shall not apply if it is recognized that the principal's rights and interests will be violated without due cause by exchanging such subscriber information. 2. When a telecommunications carrier exchanges subscriber information with another telecommunications carrier, it is appropriate for such telecommunications carrier to inform a principal in advance of, or put them into a state where a principal can easily know, such exchange as well as items of subscriber information to be exchanged, the scope of telecommunications carriers exchanging such information, and the name or appellation

of the person in charge of the control of subscriber information to be exchanged.

3. When a telecommunications carrier changes the name or appellation of the person in charge of the control of subscriber information to be exchanged pursuant to the preceding paragraph, it is appropriate for such telecommunications carrier to inform a principal in advance of, or put them into a state where a principal can easily know, the specifics of such change.

Mass emailing with false sender information (such as the sender's email address) for the purpose of advertisement and promotion, etc. or mass emailing by indicating a fictitious email address for the sender's own or any other person's marketing purposes (hereinafter referred to as "unsolicited email") violates the Specified Email Act, and if the transmission is a lot, it puts a burden on a telecommunications carrier's server and other systems and delays or otherwise interferes with other users' email transmissions, causing tremendous damage to the information and communications networks.

As a telecommunications carrier's measures against mass emailing such as unsolicited email, a utilization cease action of the service (including termination of a contract; the same shall apply hereinafter) is taken against a subscriber who engaged in emailing to a large number of recipients at one time in violation of the Specified Email Act or other mass emailing which could interfere with other email transmissions, to the extent necessary to prevent such interference, which was effective to some degree against unsolicited email and other mass emailing, but there have been cases where a person who became subject to a utilization cease action by one telecommunications carrier subsequently enters into a contract with another telecommunications carrier and continued to send unsolicited email and other mass emailing action (so-called "drifting (*watari*)").

As stated above, given that unsolicited email and other mass emailing action inflict tremendous damage to the information and communications networks, special necessity to take appropriate measure against persons who continue to engage in unsolicited email and other mass emailing action through "drifting (*watari*)" has been acknowledged in order to enhance the effectiveness of measures taken by telecommunications carriers against unsolicited email and other mass emailing action and protect the information and communications networks.

Accordingly, so long as the legitimate right of a principal (a subscriber subject to a utilization cease action) required to be protected is protected, it is regarded that telecommunications carriers may exchange information (*) pertaining to a subscriber who engaged in emailing to a large number of recipients at one time in violation of the Specified Email Act or mass mailing which is likely to interfere with other email transmissions and use such information for a screening of subscription applications.

(*) Information so exchanged may include "information pertaining to a subscriber who became subject to a utilization cease action by reason of mass mailing which is

likely to interfere with email transmissions, such as such subscriber's name, address, and birth date (hereinafter referred to as "subscriber information relating to sending of unsolicited email, etc.")". Such subscriber information relating to sending of unsolicited email, etc. does not relate to the contents of email, recipients, date and time sent, place of email transmission, number of transmissions, etc., and because it is not information concerning individual instances of email transmissions, they are not interpreted to be information covered by the secrecy of communications (incidentally, because sender information relating to specified individual instances of email transmissions is a component of individual instances of communications and covered by the secrecy of communications, obtaining or third-party provision of it is limited to cases in which the corresponding person's consent has been obtained, or if there is justifiable cause for noncompliance with the law such as necessity, etc.).

However, subscriber information relating to sending of unsolicited email, etc. is information required to be protected from the perspective of privacy in the sense that such information can sufficiently identify the "person who the telecommunications carrier determines engaged in mass emailing which is likely to interfere with email transmissions and who becomes subject to a utilization cease action", and is required to be handled as personal information in a careful and strict manner.

Accordingly, so as not to "violate the rights and interests of a principal", information to be exchanged must be limited to information pertaining to a subscriber who became subject to a utilization cease action by reason of mass emailing which is likely to interfere with email transmissions; the accuracy of subscription information to be exchanged shall be sufficiently assured; the fact of engaging in unsolicited email or other emailing action must be confirmed in an appropriate manner; a subscriber's consent must be obtained by *inter alia* having an explicit provision in contractual terms and conditions (accordingly, in applying Article 15, the foregoing shall be regarded as a case in which the "principal's prior consent" is required for the provision of personal information to a third party); a subscriber shall be made aware of the system of such information exchange in accordance with the provisions of Paragraphs 2 and 3; and sufficient security control actions are required to be taken with regard to information so exchanged.

In utilizing the information so exchanged, when not approving a subscription as a result of using the information so exchanged, a period for such measurement must be limited to a certain reasonable duration after the utilization cease action was taken, and if a telecommunications carrier who took a utilization cease action lifts such action, the relevant information must be removed from the information so exchanged and otherwise handled in an appropriate manner, so that such measure will not violate a prohibition of unduly discriminatory handling under the Telecommunications Business Act (Article 6 of the Telecommunications Business Act) and the

duty of providing services (Article 121, paragraph (1) of such Act).

Additionally, Articles 17 and 18 are also applicable to the exchange of subscriber information pertaining to sending unsolicited email, etc.

5-6-2 Restriction, etc. on Utilization Purpose of Subscriber Information Concerning Sending of Unsolicited Email, etc. (in Relation to Article 37, Paragraphs 4 and 5)

Article 37

4. It is appropriate for a telecommunications carrier which has exchanged subscriber information to refrain from using such subscriber information for any purpose other than screening at the time of entering into a subscription contract.
5. It is appropriate for a telecommunications carrier which has provided or received subscriber information to take all possible measures, in particular, to manage such subscriber information in an appropriate manner.

The concept under Articles 4 and 5 is the same as the concept under Paragraphs 4 and 5 of Article 36.

5-7 Telephone Number Information (in Relation to Article 38)

5-7-1 Inclusion, etc. of Telephone Number Information in a Telephone Directory (in Relation to Article 38, Paragraph 1)

Article 38

1. When a telecommunications carrier publishes a telephone directory or provides a telephone directory service by using telephone number information (which refers to the name of a subscriber which the telecommunications carrier may obtain in connection with the execution of a telephone subscription contract, or the appellation and associated telephone number which a subscriber wishes to be included in the telephone directory or the telephone directory service, and other subscriber information; the same shall apply hereinafter), it is appropriate for such telecommunications carrier to give the subscriber an opportunity to opt out from such inclusion in the printed telephone directory or the telephone directory service. In this case, if the subscriber opts out, such subscriber's information shall be removed from the telephone directory or the telephone directory service without delay.

When a person wishes to make a call to another person, communications cannot be made if such other person's telephone number is not known. Therefore, even though telephone number information is personal information, such information is made open to the public upon request

and made available in a printed telephone directory or through a telephone directory service. However, because such request is not prioritized over a subscriber's privacy, it is appropriate for a telecommunications carrier to give the subscriber the opportunity to choose to have his/her telephone number not included in a telephone directory or a telephone directory service (*).

(*) Because an ID (such as an email address) in a telecommunications service other than a telephone service is not requested to be made open under current situations, it is not covered by this Article, and Chapter II (Articles 4 through 31) shall apply to the handling of such information which is treated as personal information.

5-7-2 Restriction on Provision of Telephone Number Information (in Relation to Article 38, Paragraph 2)

Article 38
2. Where a telecommunications carrier publishes a telephone directory or provides a telephone directory service, it is appropriate for such telecommunications carrier to ensure that the scope of telephone number information to be provided shall not exceed the scope necessary for the purpose of achieving the respective operations. The foregoing, however, shall not apply where the subscriber's consent has been obtained.

A telephone directory should include the minimum information to specify a subscriber, and the name, address and telephone number are necessary to be included, but it is not appropriate to include further personal information (however, it is possible to include an occupation in a classified telephone directory). Furthermore, it is worthwhile to consider offering an option to omit part of the address.

5-7-3 Form of Provision of Telephone Number Information (in Relation to Article 38, Paragraph 3)

Article 38
3. Where a telecommunications carrier publishes a telephone directory or provides a telephone directory service, it is appropriate to ensure the form of the provision of telephone number information not to violate the principal's rights and interests without due cause.

The form in which a telecommunications carrier provides telephone number information in publishing a telephone directory or providing a telephone directory service must not unduly violate the rights and interests of a principal.

Conventionally, a telephone directory was in paper, and a telephone directory service was normally provided by an operator, but as computer processing advances, a telephone directory in a CD-ROM, a telephone directory service on the Internet, and such other forms have emerged. These are beneficial to users in light of the enhancement of convenience, but on the other hand, considerations must be given to subscribers' privacy. For instance, from the perspective of preventing unduly secondary use of personal information through modification or processing of electronic data, it is necessary to disallow downloading or reverse search of data at least. On the other hand, as to whether it is necessary to confirm once again a subscriber's intention as to the inclusion in a CD-ROM, assessment on social consensus must be determined with paying attention to the trends in respective countries in Europe and other foreign countries. Additionally, because the wider dissemination of information included in a classified telephone directory is beneficial to the society, and because there is not much content in such directory which must be protected as personal information, such directory is already available in a CD-ROM and on the Internet.

5-7-4 Provision of Telephone Number Information to Outside (in Relation to Article 38, Paragraph 4)

Article 38 4. Except in connection with the publication of a telephone directory or the provision of a telephone directory service, it is appropriate for a telecommunications carrier to refrain from providing telephone number information. This, however, shall not apply in any of the following cases: (1) when the publication of a telephone directory or the provision of a telephone directory service is outsourced; (2) when telephone number information is provided to a party who publishes a telephone directory or conducts a telephone directory service; (3) when any of the items in Article 5, Paragraph 3 is otherwise applicable.

3-5-1 (Principle of Restriction on Third-Party Provision) shall apply to the provision of telephone number information to the outside (*).

(*) For instance, an inquiry of who the subscriber is for a certain telephone number used by a caller in a particular call requires a warrant issued by a judge, etc. because it is a matter covered by the secrecy of communications, but an inquiry of who the subscriber is for a certain telephone number does not breach the secrecy of communications, such inquiry may be responded to if such inquiry is made by a person who has the legal authority to make such inquiry.

5-7-5 Provision of Telephone Number Information to Party who Publishes Telephone Directory or Provides Telephone Directory Service (in Relation to Article 38, Paragraph 5)

> Article 38
>
> 5. When a telecommunications carrier provides telephone number information to a party which publishes a telephone directory or provides a telephone directory service, it is appropriate to set forth, in such provision agreement, etc., that such telephone number information shall be handled in the manner equivalent to that under the respective preceding paragraphs.

It is considered permissible as an act within the scope of purpose to provide telephone number information to a party which publishes a telephone directory or provides a telephone directory service. A medium used for the provision in this case may be a magnetic medium. However, it is necessary to execute an agreement, etc. with regard to the handling of such information with a person who receives such information, setting forth *inter alia* that the use of such information shall be limited to the publication of a telephone directory or the operation of a telephone directory service; that the form of the original telephone directory, etc. shall be maintained; and that measures shall be taken to prevent a leakage of information.

6 Reexaminations of Guidelines (in Relation to Article 39)

> Article 39
>
> These Guidelines shall be reexamined as it becomes necessary in view of various environmental changes, such as a change in social circumstances, change in public awareness, and change in technological trends.

Because the views on the protection of personal information may change, depending *inter alia* on a change in social circumstances, change in public awareness, technological developments, and international trends, these Guidelines shall be reexamined as it becomes necessary in view of various environmental changes after the enforcement of the Act.

7 (Attached Material) Contents of Security Control Action to be Taken

Followings are examples etc. of the actions that a telecommunications carrier shall take and the measures for implementing the said actions as security control action specified in Article 11.

As for specific measures for taking security control action, in consideration of the magnitude of the infringement on the rights and interests that a principal may suffer in case of leakage etc. of personal data, the contents of the measures should be those necessary and appropriate in accordance with the scale and nature of the business, a status of personal data handling (including the nature and volume of personal data to be handled), risks resulting from the nature etc. of the medium with personal data recorded. And therefore, it is not always necessary to take actions for all the contents indicated in the examples below, and the appropriate measures are not limited to the contents indicated in the examples.

7-1 Establishment of basic policy

It is important for a telecommunications carrier to establish a basic policy to tackle, as an organization, the security of an appropriate handling of personal data.

As for examples of specified items, “business operator’s name,” “compliance with related laws and regulations/guidelines etc.,” “matters related to security control actions,” “windows for accepting questions and dealing with complaints” etc. are conceivable.

7-2 Making out the rules on handling of personal data

A telecommunications carrier shall make out the rules on specific handling of personal data for the security control of personal data including preventing the leakage etc. of its handled personal data.

Actions to be taken	Examples of measures
○ Making out the rules on handling of personal data	Making out personal data handling rules, in which a handling method, a responsible person, a person in charge and his/her duties etc. are stipulated at each stage of acquisition, utilization, preservation, provision, deletion/disposal etc., respectively, is conceivable. In addition, for the matters to be specified, it is important to include the contents of later-described organizational security control action,

	personal security control action and physical security control action, as well as the contents of technological security control action in a case where personal data is to be handled using the information system (including equipment such as a personal computer), (including a case of sending/receiving the data to/from outside through the internet etc.).

7-3 Organizational security control action

A telecommunications carrier shall take the following actions as organizational security control actions.

(1) Establishment of an organizational set-up

A telecommunications carrier shall establish an organizational set-up to take safety control actions.

(2) Operation in compliance with the rules on personal data handling

A telecommunications carrier shall handle personal data in compliance with the rules being made out in advance on handling of personal data. It is also important to record system logs or records of use in order to check the situation of management in accordance with such made-out rules on handling of personal data.

(3) Determination of the measures to confirm a status of personal data handling

A telecommunications carrier shall determine the measures to confirm a status of personal data handling.

(4) Establishment of a set-up to respond to incidents of leakage etc.

A telecommunications carrier shall establish a set-up to appropriately and promptly respond to when incidents of leakage etc. occurred or having found the sign of those.

In addition, when incidents of leakage etc. occurred, it is important to quickly disclose the facts and related matters and preventive measures for recurrence etc. to the public in view of preventing secondary damages, occurrence of similar case etc. (*)

(*) Specific responses when incidents of leakage etc. occurred at a telecommunications carrier are prescribed separately (see (4 (responses when incidents of leakage etc. occurred etc.)).

(5) Taking hold of a status of handling and reviewing security control action

A telecommunications carrier shall take hold of a status of personal data handling and strive for evaluation, review and improvement of security control action.

Actions to be taken	Examples of measures

(1) Establishment of an organizational set-up	(Examples of items to be established as an organizational set-up) ・ Appointment of a responsible person for personal data handling and clarification of his/her responsibility ・ Clarification of the employee handling personal data and his/her responsibility ・ Clarification of the scope of personal data that the employee above mentioned handles ・ A set-up for reporting/contact to/with a responsible person when having found the fact or a sign of violation of the Act or the rules on personal data handling that are established at a personal information handling business operator ・ A set-up for reporting/contact to/with a responsible person when incidents of leakage etc. of personal data occurred or having found a sign of those ・ Division of roles for each section and clarification of its responsibility in a case where multiple sections are handling personal data
(2) Operation in compliance with the rules on personal data handling	It is conceivable that, in order to secure an operation in compliance with the rules on personal data handling, for example, making out system log and other records of personal data handling or keeping business diaries, whereby personal data handling may be verified. ・ A status of utilization/outputting of a personal information database etc. ・ A status of carrying documents/medium etc. with personal data written or recorded etc. ・ A status of deletion/disposal of a personal information database etc. (including the records verifying deletion/disposal in case of entrusting) ・ A status of utilization of an information system by a person in charge in a case where a personal information database etc. being handled in the information system (log-in facts, access-log etc.)
(3) Determination of the measures to confirm a status of personal data handling	For example, clarification in advance of the following items, whereby a status of personal data handling may be taken hold of, is conceivable. ・ Type and name of a personal information database etc. ・ Items of personal data ・ A responsible person/handling section ・ A utilization purpose

	・ A person having the right to access etc.
(4) Establishment of a set-up to respond to incidents of leakage etc.	For example, establishment of a set-up to respond to the followings at the time that incidents of leakage etc. occurred is conceivable. ・ Facts and related-matter-finding examinations and investigations of the cause ・ Contact with a principal who may be affected ・Report to the Personal Information Protection Commission etc. ・ Study and determination of preventive measures for recurrence ・ Disclosure of the facts and related matters and preventive measures etc. for recurrence to the public, etc.
(5) Grasping the handling situation and reviewing security control action	・ Conducting a periodic self-inspection or an inspection by other sections etc. ・ Conducting an inspection in conjunction with an inspection by an external entity

7-4 Human security control action

A telecommunications carrier shall take the following actions as personal security control action. In addition, a telecommunications carrier shall exercise supervision over employees under Article 11, paragraph (1) in having the employees handle personal data (see 3-3-5 (Supervision over employees)). Furthermore, a telecommunications carrier shall, in case of entrusting the handling of personal data, etc., exercise supervision over an entrusted person (see 3-3-6 (Supervision over Contractors)).

○ Education of employees

A telecommunications carrier shall carry out an appropriate education of its employees as well as making them aware thoroughly of an appropriate handling of personal data.

○ Non-Disclosure Agreement

Actions to be taken	Examples of measures
○ Education of employees	・ Conducting periodic training etc. of employees about the matters an attention should be paid to on handling personal data ・ Including the matters on confidentiality of personal data in the employment rules etc.

○ Non-Disclosure Agreement	・ Executing a non-disclosure agreement with employees at the time of the execution of the employment contract, and executing a non-disclosure agreement between the entrusting party and the contractor of the entrustment agreement etc. (including a dispatch labor contract). ・ Prescribing non-disclosure obligation regarding personal data etc. in company regulations such as rules of employment etc.

7-5 Physical security control action

A telecommunications carrier shall take the following actions as physical security control action.

(1) Control of the area in which personal data is handled

A telecommunications carrier shall exercise an appropriate control over the area in which important information systems are to be controlled, such as servers or main computers etc. handling a personal database etc. (hereinafter referred to as the "control area"), and the area in which the affairs of handling other personal data is to be carried out (hereinafter referred to as the "handling area").

(2) Prevention of theft etc. of equipment and electronic medium etc.

A telecommunications carrier shall exercise an appropriate control to prevent theft or loss etc. of the equipment, electronic medium and written documents etc. handling personal data.

(3) Prevention of leakage etc. when carrying electronic medium etc.

A telecommunications carrier shall, when carrying an electronic medium or written documents etc. with personal data recorded, take safety measures to prevent the personal data from being identified easily.

In addition, "carrying" means a transfer of personal data outward from the control area or the handling area, or a transfer of personal data to the said areas from outside, and an attention should be paid to loss, theft etc. of personal data even for a transfer etc. within a business office.

(4) Deletion of personal data and disposal of the equipment and electronic medium etc.

A telecommunications carrier shall, when deleting personal data and disposing of the equipment and electronic medium etc. with personal data recorded, carry out those by employing an un-restorable means.

In addition, when having deleted personal data or having disposed of the equipment and electronic medium etc. with personal data recorded, it is important to preserve the record of deletion and the disposal, and, when entrusting those works, it is also important to confirm that a trustee certainly deleted or disposed of by a written certificate etc.

Actions to be taken	Examples of measures
(1) Control of the area in which personal data is handled	(Examples of control measures in the control area) ・ Control of room entry/leaving and limiting the equipment etc. brought in the room etc. In addition, as for the measures for control of room entry/leaving, installation of a room entry/leaving control system etc. such as IC cards or number keys is conceivable. (Examples of control measures in the handling area) ・ Prevention of an unauthorized person from browsing personal data etc. by installation of walls or partitions, devices of seating layout, implementation of peeping prevention measures etc.
(2) Prevention of theft etc. of equipment and electronic medium etc.	・ Storing the equipment handling personal data, electronic medium with personal data recorded or written documents containing personal data in a lockable cabinet/book storeroom etc. ・ In a case where the information system handling personal data is operated with equipment only, fixing the equipment with security wire etc.
(3) Prevention of leakage etc. when carrying electronic medium etc.	・ Comprehensively assessing specific potential risk in case of taking personal data etc., considering and deciding on actions necessary to address the risk (personal authentication at the point of booting PCs etc., connection limit on external media, maintaining state-of-the-art security standards in preparation for information leakage due to viral invasion, advanced encryption measurements and appropriate control of decryption keys, encryption of communication pathways, device verification in internal servers), and conducting an appropriate operation of the decided actions ・ Storing personal data to be carried in an electronic medium after performing encryption, protection with password etc. ・ Sealing, pasting a blindfold seal ・ Using a lockable transport container
(4) Deletion of personal data and disposal of equipment and electronic medium etc.	(Examples of measures for disposal of written documents containing personal data) ・ Adopting un-restorable means such as an incineration, dissolution, appropriate shredding (Examples of measures for deleting personal data or disposal of the equipment and electronic medium etc. with personal data recorded)

	・ Adopting means that cannot easily be restored when deleting personal data in the information system (including the equipment such as a personal computer) ・ Adopting measures such as using a dedicated data deletion software or physical destruction when disposing of the equipment and electronic medium etc. with personal data recorded

7-6 Technological security control action

A telecommunications carrier shall take the following actions when it handles personal data (including cases in which personal data is transmitted to and received from an outside party etc. through the internet) using the information system (including equipment such as a personal computer), as technological security control action.

(1) Access control

An appropriate access control shall be exercised in order to limit the scope of the person in charge and that of the personal information database etc. to be handled.

(2) Identification and authentication of the person who accesses

On the basis of the results of identification, the fact that an employee who uses the information system handling personal data is the person having a legitimate right to access shall be authenticated.

(3) Prevention of unauthorized access from outside

A mechanism to protect the information system handling personal data from unauthorized access or illegal software shall be incorporated and operated properly.

(4) Prevention of leakage etc. associated with the use of the information system

An action to prevent leakage etc. associated with the use of the information system shall be taken and operated properly.

Actions to be taken	Examples of measures
(1) Access control	・ Limiting the information system that may handle a personal information database etc. ・ Limiting a personal information database etc. that may be accessed through the information system ・Limiting an employee who may use the information system handling a personal information database etc. by the right to access granted to user ID

(2) Identification and authentication of the person who accesses	(Examples of the measures for identification and authentication of the employee using the information system) ・ User ID, password, magnetic/IC card etc.
(3) Prevention of unauthorized access etc. from outside	・ Intercepting unauthorized access by installing a firewall etc. at the connecting point between the information system and external network ・ Installing security software etc. (anti-virus software etc.) into the information system and the equipment ・ Updating the software etc. to the latest version by applying an automatic updating system etc. provided on the equipment or software etc. as a standard function ・ Detecting unauthorized access etc. by analyzing log etc. periodically
(4) Prevention of leakage etc. associated with the use of the information system	・ Ensuring safety at the time of designing the information system, and reviewing the system continuously (including implementation of measures against attacks to vulnerability of the information system) ・ Encrypting the route or the contents of communications containing personal data ・ Protecting personal data to be sent with a password etc.