Reference Document on How to Obtain Consent

Table of Contents

Introduction

In Chapter I (General Provisions), the Telecommunications Business Act (Act No. 86 of 1984; hereinafter referred to as the "Act") specifies the protection of secrecy (Article 4). In Chapter II (Telecommunications Business), the Act specifies, against telecommunications carriers, reporting on the suspension of telecommunications operations and on serious accidents (Article 28), order to improve business activities (Article 29), and etc. In Chapter VI (Penal Provisions), the Act specifies the violation of the secrecy of communications (Article 179), and etc.

There are three types of acts that violate on the secrecy of communications, namely, "unauthorized obtaining" (to obtain a secret of communication actively for the purpose of knowing it), "unauthorized use" (to use a secret of communication contrary to intention of a sender or a recipient of the communication), and "unauthorized leakage" (to leave a secret of communication in a state that others available). However, it is understood that even when obtaining information related to the secrecy of communications, it does not constitute a violation of the secrecy of communications if there is valid consent of the user[1] or a justifiable cause for noncompliance with the law. Therefore, it is extremely important whether or not it can be determined that there is the user's valid consent or a justifiable cause for noncompliance with the law.

Commentary for Article 3 of the Guidelines for Protection of Personal Information Protection in Telecommunications Business[2] (hereinafter referred to as the "Guidelines") (2-13 Principal's Consent) states that "with regard to the handling of personal information protected under the secrecy of communications…the correspondent's individual, specific and clear consent is required." Users' consent and justifiable causes for noncompliance with the law have been deeply examined, focusing on practical operation cases.

For the sake of increasing telecommunications carriers' predictability by clarifying rules in the future, and of the government's flexible ex-post-facto issuance of orders to improvement business activities and etc. if necessary, this document to be published mainly examines and organizes issues[3] related to how to obtain consent from users as an essential factor.

---

[1] The term "users" refers to those who conclude contracts with telecommunications carriers to receive telecommunications services under the Telecommunications Business Act. However, as seen in subscriber telephones, it is possible to use telecommunications services whether or not they are contractors. Therefore, in order to protect the secrecy of communications of these people, a telecommunications service user is referred to as a "user" hereinafter.

[2] MIC Notice No. 152 of April 18, 2017

[3] Study on consent is being deepened both domestically and internationally in various legal fields. Since the meaning of consent varies with each legal area and it needs to be studied on a case-by-case basis in the light of the protection law benefits. This document organizes thoughts on users' consent in the secrecy of communications and the privacy area related to communications. The document refers to the interpretation theory on users' consent in violation of the secrecy of communications as stipulated in Article 179 of the Act, which has been studied.

1. Meaning of Obtaining Consent in the Secrecy of Communications

1) Relationship between the Purpose of Protecting the Secrecy of Communications (Protection Law Benefit) and Users' Consent

The purposes of protecting the secrecy of communications are (1) Effectuating freedom of expression, (2) Protecting privacy (the secrecy of private life), and (3) Protecting users' trust and expectations for safe and secure communications (communications system).[4] To this effect, the secrecy of communications is protected by Article 4[5], Article 28, Article 29, Article 179, and etc. of the Act.[6]

The obtaining and use of individual users' communication information are legalized with the valid consent of the users as the party to the communication, or otherwise a justifiable cause for noncompliance with the law. In that case, the users' valid consent is a waiver of their right to the secrecy of communications, which is a significant constitutional right. Therefore, it is required that the users agree at their own will with understanding the meaning accurately to be evaluated as the users' valid consent.[7]

2) How to Obtain Consent Required for Valid Consent of Users

A. Consent of Users under Article 179 of the Act

Article 179 of the Act stipulates punishment for "A person that has violated the secrecy of communications handled by a telecommunications carrier." Behaviors that violate on the secrecy of communications conducted by third parties other than the parties of communications mean unauthorized obtaining (to obtain a secret of communication actively for the purpose of knowing it), unauthorized use (to use a secret of communication contrary to intention of a sender or a recipient of the communication), and unauthorized leakage (to leave a secret of communication in a state that others available). However, with the valid consent of users as the party to the communication, it is

---

[4] Page 35 of *Article-by-Article Commentary for the Telecommunications Business Act, Revised Edition*, TAGAYA Kazuteru et al., and page 8 of *Interim Report of the Study Group on Platform Services*, the Ministry of Internal Affairs and Communications

[5] Article 4, paragraph 1 of the Act provides for the protection of the secrecy of communications and paragraph 2 provides for the protection of "other persons' secrets which came to their knowledge…with respect to communications". From the perspective of maintaining user trust in the telecommunications business, paragraph 2 imposes a wider range of confidentiality obligations than paragraph 1 does on those engaged in the telecommunications business as a duty obligation.

[6] As a general rule in punishment, consent must relate to legal interests (personal legal interests) that can be disposed of by oneself. It can be said that in the case of the violation of the secrecy of communications, not only the protection legal benefits of trust in the communication system (3), which can be said to be national and social legal benefits, but also freedom of expression (1) and personal legal benefits (2), such as privacy protection, have been considered important. It may be pointed out that the consent of communications parties (people in communication) alone is not sufficient when the protection legal interests include national legal interests and social legal interests. If the aspect of personal legal interests is considered to be as important as national legal interests and social legal interests, there is a view that the establishment of a crime is denied as the infringement of one of the legal interests is denied. (Page 349 of *Commentary Penal Code Vol. 1, General Remarks §1-72*, NISHIDA Noriyuki et al.).

[7] In order to obtain valid consent, the party to the communication must agree at their own will with understanding the meaning accurately. Therefore, it should be noted that depending on the service mechanism and data utilization in the first place, there are cases exceeding the users' cognitive limits and cannot be legalized even if consent is obtained.

understood that the use of the information does not go against the intention of the party to the communication and therefore does not violate the secrecy of communications.[8]

Whether or not it being the user's valid consent is ultimately left to the judicial decision on a case-by-case basis, and it is a subjective matter related to the user's mind. Therefore, a study so far has been focused on the appropriateness of carriers' procedural and objective way of obtaining consent by examining whether there is individual, specific and clear consent by a typological analysis. As a general expression of that, various documents, including reports and the explanation of Article 3 of the Guidelines (2-13 Principal's Consent), have stated that with regard to the handling of the information related to secrecy of communications "the correspondent's individual, specific and clear consent is required." On the other hand, it should be noted that what is originally required of users as a communication party is valid consent, and that whether an apparent consent obtaining method is appropriate is, strictly speaking, a different concept (Details of each interpretation is described later in *3. Valid Consent and How to Obtain Consent*).

Article 179 of the Act covers the case of "A person that has violated the secrecy of communications handled by a telecommunications carrier." Since the Act does not provide for punishment for negligence, and no one is subject to discipline in the case of unintentional negligence (including gross negligence).[9]

B. How to Obtain Consent under Article 29 of the Act

On the other hand, Article 29 is a stipulation for the means of conducting operations, covering cases where "there is a hindrance in ensuring secrecy of communications with respect to the…means of conducting operations," etc. and directly covers how to obtain consent (in point of procedural ensuring by carriers), which is objectively denoted as means of operation. This document is for how to obtain consent itself and sets a benchmark based on the ordinary person (user of general understanding) using the service. This document evaluates whether consent obtaining procedures can be recognized, fully understood, and judged by users with general understanding. For example, there is a method of confirming whether individual, specific and clear consent has been obtained. The study to date on Article 179 of the Act applies to how to obtain consent here, which can lead to valid consent, that is, whether users utterly understand and agree.[10]

---

[8] Even a mechanism of mechanical and automatic processing, such as mechanically and automatically detecting communications under specific conditions e and using them without permission of the party to the communications, may fall within unauthorized obtaining or unauthorized use (*First Interim Report from Study Group on Proper Dealings of Telecommunications Business with Cyber-attacks*, April 2014).

[9] It is understood that the case, however, falls under "a violation of secrecy of communications" referred to in Article 28 (Page 37 of *Article-by-Article Commentary for the Telecommunications Business Act, Revised Edition*).

[10] Regarding violation of the secrecy of communications (Article 179 of the Act), as in the general idea of the Penal Code, the obtaining and use of information related to the secrecy of communications have been legalized subject to the user's

Article 29 of the Act covers cases where “there is a hindrance in ensuring secrecy of communications concerning the telecommunications carrier’s means of conducting operations,” and covers cases of negligence (including gross negligence). Therefore, for example, even if a telecommunications carrier and its workers leaked information due to unintentional reasons, such as accidents and crime damage (e.g., cyber-attacks), whether there was “a hindrance in ensuring secrecy” referred to in Article 29 of the Act is the issue.

3) Effect of Enforcement Guidelines for Article 29, Paragraph 1, Item 1 of the Act

A. Scope of Enforcement Guidelines

When Article 29, Paragraph 1, Item 1 of the Act was introduced, “there is a hindrance in ensuring secrecy of communications” is interpreted as “cases where the management and operation of the equipment are sloppy neglecting to manage entry and exit records on the machine room, resulting in leakages of the secrecy of communications, as an example.”[11] It can be considered that security control action[12] for information related to the secrecy of communications were focused on.

Also, “the telecommunications carrier’s means of conducting operations” are said to be methods of managing and operating the business, and daily business handling such as counter work, and all situations of obtaining, using, and providing information related to the secrecy of communications fall into the “means of conducting its operations.” Accordingly, a carrier’s appropriate consent obtaining method of the secrecy of communications is meaningful as a basis for justifying the obtaining etc. of information related to users’ secrecy of communications. Therefore, if the way of obtaining consent to obtain etc. information related to the secrecy of communications is inappropriate, it may be regarded as “a hindrance in ensuring secrecy of communications with respect to the…means of conducting operations,” resulting in being subject to Article 29 of the Act.

B. Relationship with Enforcement Guidelines for Article 29, Paragraph 1, Item 1 of the Act

As rapid technological innovation and diversification of communication services are

---

consent or a justifiable cause for noncompliance with the law even when the factual requirements are met. Administrative discipline borrowed the idea of violation of the secrecy of communications, and has been studied within the corresponding framework.

[11] Page 154 of *Article-by-Article Commentary for the Telecommunications Business Act, Revised Edition*

[12] In light of current telecommunications services (e.g., telephone and Internet connection services), security management measures also include: (i) security control action for physical equipment such as servers to establish communications, (ii) technological security control action to determine whether access authority for information related to the secrecy of communications managed and stored on the server and etc. are properly performed, (iii) human security control action measures to educate and etc. employees and etc. who handle information related to the secrecy of communications, (iv) organizational security control action to establish a system to respond to disciplines that have been prepared in advance and deal with leaks and etc. of the secrecy of communications.

progressing, multilateral and complex services centered on communication services are emerging. Accordingly, the role and position of telecommunications in social and economic activities have developed, and the dependence of society on telecommunications is increasing. As a result, telecommunications are becoming more important as a part of social infrastructure, not just an information infrastructure. For this reason, with regard to the protection of the secrecy of communications, there are more opportunities than ever to ensure the flexible implementation, to review lawful business acts, and to ensure the protection of the secrecy of communications, in a complex structure with mutual relationships of various stakeholders. Accordingly, the need for an autonomous judgment by carriers is also increasing.

Until now, regarding the handling of information related to the secrecy of communications, it was often the case that carriers conducted individual consultations in advance to ensure proper handling. Besides, it seems that there were many cases in which the interpretation was comprehensively examined from the viewpoint of whether or not the penalties under Article 179 of the Act could be applied, rather than discussion with a clear awareness of the difference between Article 29 of the Act stipulating administrative enforcement situations and Article 179 of the Act stipulating penalties (both of which are concerning the discipline regarding secrecy of communications). However, as the importance of an autonomous judgment of each carrier will increase in the future, it is expected that there will be more occasions to combine carriers' judgment and the flexible enforcement of administrative discipline rather than always implementing strict discipline centered on punishment.

With consideration of this situation, in light of increasing the predictability and transparency of carriers and further enabling and supporting the speedy and flexible development of communication services, the Guidelines for Issuance of a Business Improvement Order to Prevent Hindrance in Ensuring the Secrecy of Communications, which is based on Article 29, Paragraph 1, Item 1 of the Act, has been published for the first time. In these guidelines, items related to judgment on users' valid consent are also shown. It is effective to refer to this reference document along with the Enforcement Guidelines.

(Reference) *Guidelines for Issuance of a Business Improvement Order to Prevent Hindrance in Ensuring the Secrecy of Communications* (Excerpt)

(1) Example of Inappropriate Policies, Principles, etc. Indicating the Handling of Information related to the Secrecy of Communications

i. Policies, agreements, etc. (hereinafter referred to as "policies, etc.") that indicate the handling of information related to the secrecy of communications impair user convenience because they are not described in a simple and easy-to-understand manner.[18]
ii. Methods for access to policies, etc. are insufficient.
iii. As a condition of using the service, it is required to use information related to the secrecy of communications more than operationally necessary to offer the service.
iv. As a condition of using the service, a service requires users to virtually give up their right to the secrecy of communications without giving them the opportunity to provide consent or to opt-out required for handling the secrecy of communications.
v. A telecommunications carrier does not take responsibility for any accidents, such as leakages of the secrecy of communications.

(2) Examples of Inappropriate Obtaining and Use etc. of the Secrecy of Communications

i. A telecommunications carrier's consent process under terms of the policy etc. is constantly applied without any rational reason for obtaining or utilizing users' secrecy of communication.

ii. In cases where the obtaining and use etc. of the secrecy of communications do not fall under a lawful act or a lawful business act, a telecommunications carrier obtains and uses the secrecy of communications without obtaining consent properly by clearly stating the purpose of the obtaining and use of it, or uses the secrecy of communications beyond the purpose of the obtaining and use of it specified at the time of obtaining the users' consent.

iii. Beyond the scope assumed as a lawful act or a lawful business act, the obtaining and use of the secrecy of communications are made without justification, such as appropriately obtaining users' consent.

iv. Regarding the secrecy of communications obtained, a telecommunications carrier prevents users from commitment on providing consent or opt-out required for handling the secrecy of communications, and uses the secrecy of communications virtually unlimitedly.

(4) Examples of Inappropriate Response Systems for Complaints and Consultations

i. Due to deficiencies in a telecommunications carrier's internal rules for consultation for complaints regarding the secrecy of communications, its complaint and consultation handing counter did not function, while complaints occurred frequently.

ii. A telecommunications carrier's complaint and consultation counter lost substance, then oversights of important information as a clue of accidents such as leakages of the secrecy of communications frequently occurred.

iii. In the case of an accident such as leakages of the secrecy of communications, as responses including explanations to users and information provision were insufficient, relief measures for users did not function properly, causing further damage.

iv. A telecommunications carrier's settings for accessible time and means (telephone, mail, fax, email, etc.) were insufficient in consideration of the diversity of users and its reception system was insufficient for complaints regarding the secrecy of communications.

18 For the disclosure to the public of telecommunications carriers' privacy policy (a concept or policy under which such telecommunications carrier promotes the protection of personal information), refer to Article 14, Paragraph 1 of *Guidelines for Protection of Personal Information in Telecommunications Business*.

2. Importance of Risk Analysis (Identification, Assessment, and Management) from the Perspective of Preventing Violation of the Secrecy of Communications

1) Risk Analysis and How to Obtain Consent in the Secrecy of Communications

A. Importance of Autonomous Action by Carriers through a Risk-Based Approach

A risk-based approach is the recommended idea as a framework that can deal with newly occurring risks,[13] taking into consideration that privacy risks are diversifying as a response to various technologies and services newly created with the progress of digitalization, and that it is becoming difficult for the government and carriers to predict and understand them.

A risk-based approach focuses on securing basic rights by enabling carriers to identify and detect potentially high risks in advance and to address them flexibly and promptly. A risk-based approach is expected to function as a methodology that will overcome the limitations of legal pre-regulations in the rapidly evolving and competitive information and telecommunications society, and to be more effective by mutually complementing of carriers' autonomous self-assessment and self-management under their

[13] For example, the EU's General Data Protection Regulation (GDPR) and the Privacy Framework of the National Institute of Standards and Technology (NIST) for private businesses (January 16, 2020: *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*) also show the concept of risk-based approach . SP800-53 Revision 5 (September 2020: *Security and Privacy Controls for Information Systems and Organizations*) is a more practical version of the Privacy Framework and the Cybersecurity Framework (April 2018: *Framework for Improving Critical Infrastructure Cybersecurity*).

responsibility and the flexible post-regulation by the government.

In a risk-based approach, since the concept of risk is ambiguous, it is necessary to consider the core of the risk in each situation. As risks to be considered, it is possible to consider risks to each target user and the social aspect if there is a great social impact, depending on the nature of each service. It is common that a risk-based approach is integrally considered with privacy impact assessment (PIA), data administrators' system, and etc.[14]

B. Application of Privacy Impact Assessment (PIA) to Secrecy of Communications

Privacy Impact Assessment (PIA)[15] is a means for identifying and assessing the potential impact on privacy in information processing etc. when providing new services etc. It is conducted to figure out the privacy risk in advance and design[16] an appropriate action method. PIA is considered useful for appropriately figuring out and managing the impact and risk on users' rights and freedom particularly in handling important data with high privacy related to users (i.e., when the risk is high). In general, the disclosure of PIA is not mandatory, but it is required to be notified in the case of prior consultation or when requested by the supervisory authority. PIA is considered useful for fostering the credibility of carriers and ensuring their accountability and transparency.[17]

In general, when introducing PIA, it may be appropriate to consider factors including: (i) What information is processed? (ii) What is the purpose of the process? (iii) What are the benefits brought to the information subject or society as a whole by processing information? (iv) Who is the recipient of information, and how will the information be handled? (v) What is the business process implemented by this processing of information? (vi) Which information subject is influenced by this process? (vii) How is the privacy process implemented (consent, denial, access, modification, and deletion, etc.)? (viii) How will the information subject be notified, and will it be asked for consent? Does the process match the situation?[18]

---

[14] It is pointed out that A risk-based approach may neglect user rights for low-risk matters and it is possible that it may not function at all if the data manager is not conscious of the protection of users' rights.

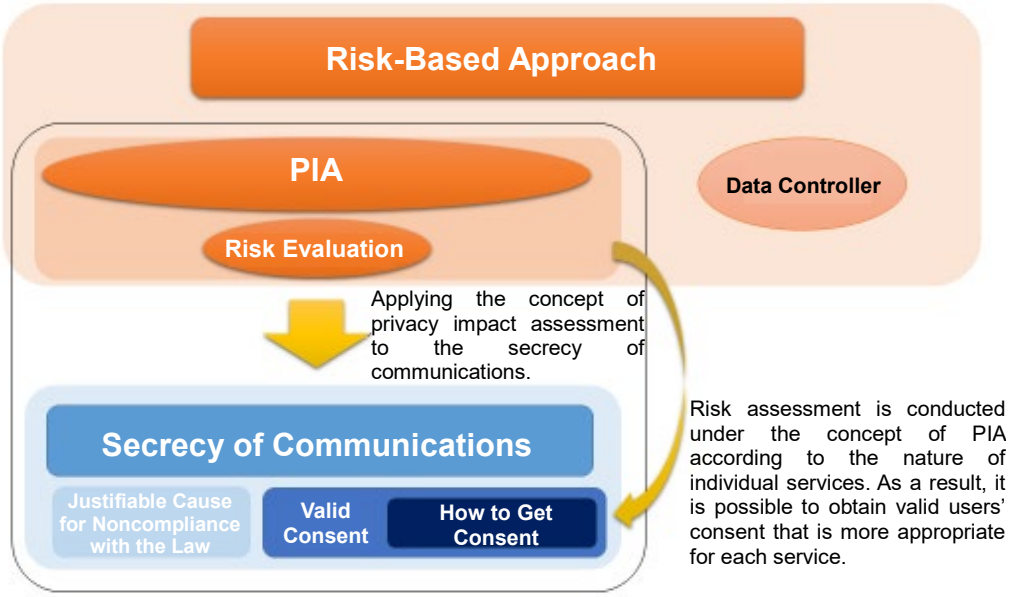
[15] PIA has been conducted in mainly the United States, Canada, and Australia. GDPR has the same kind of discipline as a Data Protection Impact Assessment (DPIA). In particular, it is obliged to introduce a DPIA when handling information that is expected to have a significant impact on privacy. It is also introduced in the so-called My Number Act (the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures) in Japan.

[16] When considering providing new services etc., it is desirable to consider PIA from the earliest possible stage to realize privacy-by-design that incorporates appropriate handling in advance.

[17] See Chapter 4, Section 3 of the GDPR.

[18] ISO/IEC 29134: 2017

* Image of obtaining valid consent according to risk



PIA is a method for identifying, assessing, and managing privacy risks. In general, information on the secrecy of communications is important data with high privacy for telecommunications service users. Applying PIA will make it possible to appropriately figure out and manage impacts and risks on the rights and freedom of the subject of information related to the secrecy of communications. Furthermore, by applying the idea of PIA, it will be possible to take into consideration social aspects such as threats and risks to freedom of expression and user trust and expectations for a safe and secure communication network to a certain extent. Applying the idea of PIA to the secrecy of communications (hereinafter referred to as "risk assessment") is considered to be useful.[19]

In the context of the secrecy of communications, risk assessment can identify and assess risks in advance and make it possible to study the following matter more specifically: (i) risks to users' privacy, freedom of expression, and trust in safe and secure communications entailed by obtaining, using, etc. information related to the secrecy of the communication (e.g., the nature of the act, the seriousness of the consequences, and the probability of the result); and (ii) methods of obtaining consent and other appropriate measures required to mitigate the risks. Risk assessment is an approach that can be applied to acts justified as lawful business acts, but this document focusing

[19] More careful consideration is required if there is a great impact in relation to social and national legal interests.

on and considering how to obtain consent.

C. How to Obtain Valid Consent by Applying Risk Assessment

Since the secrecy of communications is an important right, in principle, the way of obtaining consent to the waiver of such right has been strictly interpreted as requiring individual, specific and clear consent. However, conventionally, there have been some cases where the principle of individual, specific and clear consent procedures were flexibly interpreted on a case-by-case basis, such as allowing for prior comprehensive consent as the way of obtaining consent, by examining individual cases in detail and legal benefits (the legitimacy of purposes) realized by the violation of the secrecy of communications in each case, and by conducting risk assessment. The items considered in such cases will be helpful.[20]

Risk assessment is an attempt to create rules according to the risk, and contributes to carriers' examination when they decide on an appropriate consent obtaining method. Risk assessment analyzes factors such as the nature of the act, the seriousness of the consequences resulting from the act, and the probability of the result, which lead to taking measures according to the risk. It also has the meaning of ensuring transparency and trust-building for users by disclosing the result.

Because whether it is valid consent or not can be determined by considering various factors, it is not necessary to focus solely on the formal aspect of consent.[21] It is allowable, regarding how to obtain consent, to choose procedures according to certain risk assessment results instead of strict consent procedures, when it can be substantially considered obtaining users' valid consent as a result of the carriers' risk assessment. Among others, the point to be noted in risk assessment is that alternative attempts for user protection are required when the consent procedure is simplified, and that it is necessary to ensure that overall user protection will not fall to a low level. Alternative user protection could be, for example, ensuring transparency to users, by clearly explaining to users about the secrecy of communications-related information to be used and about handling thereof such as obtaining and use, and by making users' subsequent

---

[20] For example, regarding warning for the use of terminals that are highly likely to be infected with malware, in order to implement countermeasures without violating the secrecy of communications, obtaining comprehensive consent based on the contract terms when concluding a telecommunications service contract or changing the contract conditions is considered sufficient in certain cases, instead of obtaining individual, specific and clear consent. Specifically, even prior comprehensive consent based on the contract terms may be valid consent to the use etc. of matters falling under the secrecy of communications for such warning, if the following conditions are met: a. a system is established to ensure that the interests of those who do not wish to be warned (those who have opted out) will not be violated; b. users are allowed to change their consent at any time even after they agreed to the contract terms; c. other conditions for the provision are the same regardless of whether the consent is changed; and d. users are properly informed of such attempt and that those who do not want to be warned can change their consent (settings) at any time, and of the method thereof (*Third Interim Report from Study Group on Proper Dealings of Telecommunications Business with Cyber-attacks*, September 2018).

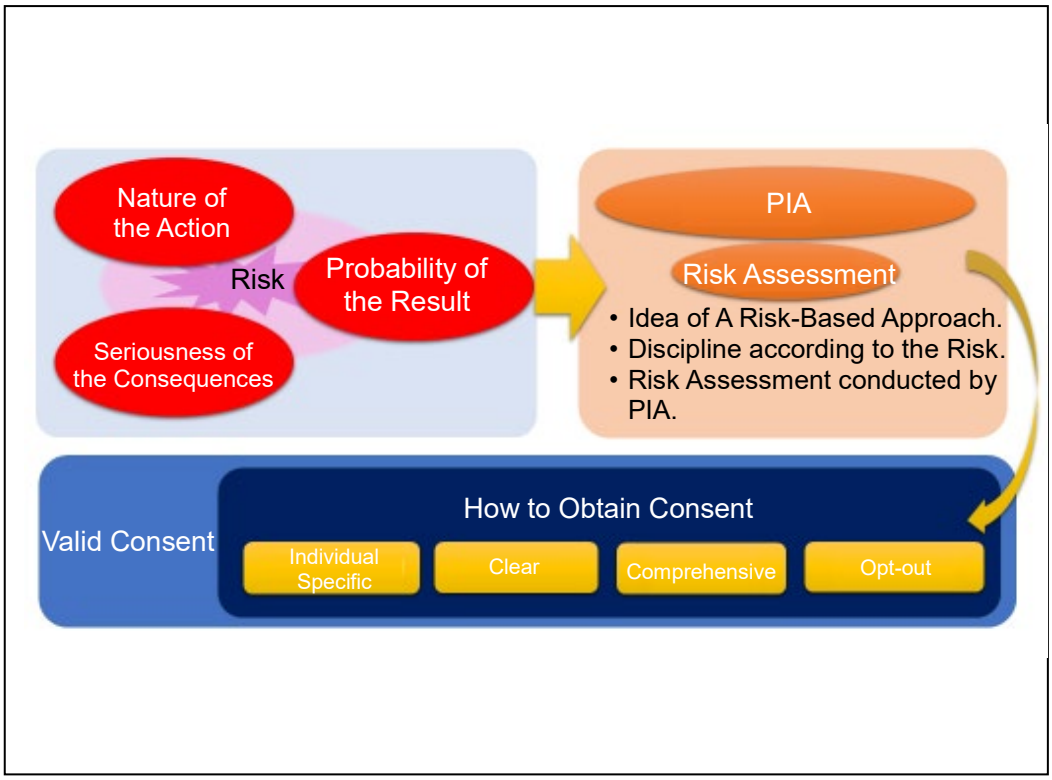
[21] Focusing only on the form of the consent causes a problem, so-called "consent fatigue," whereby users click without fully understanding the meaning of the consent. Consideration from users' point of view is required.

information control easy in terms of mechanism.

It is not mandatory to disclose the entire examination process of risk assessment. Nonetheless, in the cases where a telecommunications carrier makes a decision on consent procedure, which has been required to be strict, it would be appropriate for the carrier to clearly release to users its outline etc. when starting the service (or in advance).[22] It is also desirable to prepare for submitting a risk assessment report when consulting with the Ministry of Internal Affairs and Communications (MIC) in advance or when requested by MIC.

When considering how to obtain consent, it is essential to conduct risk assessment prior to providing the service, and regular reviews and checks are also required while the service is provided. Therefore, it is desirable to clarify the rules for updating risk assessment in advance.

* Image of Obtaining Valid Consent with Application of Risk Assessment



[22] In cases where the obtaining and use of information related to the secrecy of communications are justified on the grounds of lawful business acts etc. and carriers attempt to start using the information for a new purpose, a release prior to the service's launch will suffice. Needless to say, carriers are supposed to confirm actions necessary to comply with other laws and regulations, including the Act on the Protection of Personal Information (Act No. 57 of 2003; hereinafter referred to as the "Personal Information Protection Act").

D. Cases where Risk Assessment regarding How to Obtain Consent is Conducted not by Each Carrier

Risk assessment is considered to have the aspect of being the basis for determining how to obtain consent in the assessment activities and appropriate management. In cases where they conduct risk assessment etc. and consider the way of handling in similar services in such a form of the industry's rules in a field like an industry association, it is possible to introduce such rules.

2) Process of Risk Assessment

Risk assessment can be considered to consist of the following steps etc.: (i) service to be assessed, (ii) assessment of: necessity of obtaining, use, etc. of information related to the secrecy of communications; and proportionality, (iii) risk identification and assessment, (iv) decision on actions and risk management. It is necessary to consider in the process what factors affect how to obtain consent.[23]

(i) Service to be Assessed

- What is the purpose of use?
- What benefits can users or society obtain?
- Who are the parties concerned and responsible parties? How will they treat the information?
- Is it a new service or an additional service for an existing service?
- How will users be involved (consent, transparency, correction, deletion, etc.)?
- How high is users' literacy?

(ii) Assessment of: the Necessity of Obtaining, Use, etc. of Information related to the Secrecy of Communications; and Proportionality

- Is there any necessity of obtaining and use of information related to the secrecy of communications in the service to be assessed described in (i) (the purpose of use)? (i.e., Isn't it possible to achieve the purpose by other alternative information?)
- Is it proportionate? That is to say, is the information appropriately used in the service (in terms of the quality, quantity, period, etc. of the use) according to the purpose of use without unnecessary use?

(iii) Risk Identification and Assessment

- What kind of risk to secrecy of communications, privacy, etc. are there in (i)? What

[23] It is necessary to continue considering, for example, verification of the accumulations of carriers' studies on screen designing to obtain users' consent in various services, what and how factors are considered by users in the decision-making in consent to certain matters, and what and how information is recognized by users.

are the seriousness of the result and the probability of its occurrence?
- How are users influenced by each risk?
- Is anything for publishing provided regarding the assessment?

(iv) Decision on Actions and Risk Management
- What kind of action should be taken for each risk?
- In the service to be assessed: (a) is the risk which is entailed by obtaining, using, etc. the information related to the secrecy of communications big or small to user privacy, freedom of expression, and to ensuring trust-building in safe and secure communication?; and (b) what way to obtain consent and otherwise actions are appropriate to mitigate the risk?

3. Valid Consent and How to Obtain Consent

1) Overview and Definition

The existence or non-existence of valid consent should be determined in individual cases. MIC has so far interpreted that valid consent generally needs to be individual, specific and clear consent,[24] and that valid consent exists if carriers have procedurally confirmed it with the users to a certain level. In other words, to judge the validity of consent, MIC has formulated and taken an analytical approach through typological studies to the way of obtaining consent, from two viewpoints: whether it is individual and specific consent; and whether it is a clear consent, both of which are procedural factors.

However, it should be noted that the above two requirements are not necessary and sufficient conditions for valid consent because whether it can be considered valid consent does not hinge only on such factors, that is to say, for example, it is required to examine if the consent is voluntary in some individual cases.

Besides, the assessment result on whether it is valid consent and whether it is appropriate as the way of obtaining consent may change in proportion to the risk in each case. Also, it has been pointed out that there may be cases where, regarding matters difficult to understand for users, users' consent cannot be a ground of justification as valid consent.

2) Individual, Specific and Clear

A. What is "Individual and Specific"?

It is understood that "individual and specific"[25] means consent based on the subject's

[24] Incidentally, it was initially stated that individual and clear consent is required (*See Location Privacy Report*, etc.), and there is no requirement for being "specific." It has been pointed out that by carriers the meaning of "specific" is not clear.

[25] Incidentally, although it is possible to interpret "individual" as "each" consent for every individual instance of communication, each consent is not required for "consent" to the obtaining etc. and the like of the secrecy of communications.

recognition of it being for handling of the secrecy of communications for each service. It has been used for two meanings' (i) obtaining consent for each service; and (2) not a comprehensive consent to contract terms (consent to the terms on the conclusion of the contract for changing the contract), but the consent based on the subject's specific recognition of recognition of certain matters related to the secrecy of communications.

As for "specific," it is necessary to consider to what extent and how the information should be explained to users for the consent. It is also necessary to consider the clarity of the scope of consent, that is to say, it does not mean a comprehensive consent to contract terms[26] where users do not specifically recognize matters related to secrecy of communications (abstract consent to the entire contract at the time of the conclusion of the contract or consent only to changing the contract), but means obtaining consent based on the user's recognition of matters related to the secrecy of communications.[27]

The reason why consent is required to be "specific" is that, unless the communication party accurately recognize and understand the content and meaning of the consent and the consent is based on their true intention, it cannot be considered valid consent (waiver of legal interests) regarding the secrecy of communications.

Generally speaking, matters to be recognized for consent include:

- ✓ Contents of information to be obtained
- ✓ Subject of obtaining and use
- ✓ Purpose of use of information to be obtained
- ✓ Usage of information to be obtained
- ✓ Usage period of information to be obtained
- ✓ Contact point etc. regarding the information to be obtained
- ✓ Opportunity for and the means of withdrawal of consent

There is room for consideration for each service, regarding: what is to be presented to users in what way concerning the above matters, for obtaining users' consent; particularly, whether all purposes of use should be specified; how precisely they should be specified.

It is necessary to explain these matters so that users can fully understand their contents according to each various service, and to plainly explain according to their contents,

---

[26] Contract terms are a tool for classification for improving economic rationality by omitting detailed negotiations with each person and transactions in a one-size-fits-all matter. Hence, they are not oriented to the process of individual consensus building with each individual, and they are acceptable if both parties objectively consider the uniform transaction conditions rational. Therefore, for the same reason, as an example, when users' location information is obtained for location information service, because contract terms are assumed to be rational for both parties, the agreement thereof can be considered "valid consent" to the obtaining and use of location information (including items falling within the secrecy of communications). However, it is not appropriate to obtain matters related to the secrecy of communications other than location information. The use of location information for advertising purposes etc. is unintended use. Even if this is stated in the contract terms, except in special circumstances where users recognize that, it cannot be considered valid consent.

[27] It is considered appropriate for telecommunications carriers to publish a privacy policy (*See* Article 14 of *Commentary for Guidelines for Protection of Personal Information in Telecommunications Business*, and smartphone app businesses should see *Smartphone Privacy Initiative III*).

volume, and etc. Also, when users are requested to transit and to scroll multiple times, it should be particularly ensured that users can recognize the necessary information.

In this regard, if the information will be used within the ordinarily predictable scope according to the certain service type, consent may be obtained for the purpose of use with specifying the common purpose of use for each service type instead of specifying individual purposes of use in detail. That is because if the information is used within the predictable scope, it may be possible for users to understand the meaning without individual purposes of use being specified.

Generally speaking, it should be judged based on the recognition of ordinary people whether it is ordinarily predictable use according to a certain service type. However, that may vary over time even for the same service type, since the literacy of users varies with the progress of technology, changes with the times, and etc. Also, even regarding the same service type, the conclusion may differ depending on who provides the service, since the ordinarily predictable scope also varies depending on the service contents provided by the company and handling of information to be expected by users thereof.

As for consent regarding the obtaining and use of the secrecy of communications, it is considered that each carrier must make a judgment. It is considered necessary for each carrier to judge whether it is necessary to obtain not only the consent for each service type but also the consent for each purpose of use in the service. Risk assessment may be used as one of the grounds for such examination.

However, because it is not originally assumed that information related to the secrecy of communications is provided to a third party for purposes other than providing telecommunications services, and because the information can be spread after provided to a third party, in the case of the purpose of use including providing the information to a third party, it is necessary to ensure users can recognize that.[28]

B. What is “Clear”?

“Clear” refers to cases where the consent is objectively clear, such as consent by clicking on the screen or checking a check box, or in writing.[29] However, neither of pre-checked ON as default, starting using the service, or scrolling the screen on the website or application can be considered “clear” consent.

Incidentally, although the clarity of the scope of consent is also an important factor in users’ consent, here, whether the indication of intention is clear is to be considered, and the clarity of the scope is to be considered as whether it is “specific” or not as described

[28] *Location Privacy Report* and *Guidelines for Sufficient Anonymization in the Telecommunications Business* are organized with consideration of the usefulness and demands of the utilization of location information. In these documents, it is stated that location information that is sufficiently anonymized under certain requirements can be used and provided to third parties based on the prior comprehensive consent to contract terms.

[29] Page 27 of *Location Privacy Report* (July 2014)

above.

3) Others

It is required that valid consent exist at points of the unauthorized obtaining, the unauthorized using, and the unauthorized disclosure (acquiring, utilizing, and provision) of the information related to the secrecy of communications (it is allowable to obtain users' consent covering subsequent utilization at point of obtaining information), and that users' consent be given before obtaining etc. information (that is, ex-post-facto consent is not allowed).[30]

Valid consent is required to be based on the true intention of users capable of decision-making. Therefore, neither consent of infants/those with severe mental illness or consent based by coercion or error can be considered to be valid consent. Regarding minors, adult wards, those under curatorship, and those under assistance, who cannot judge the consequences of their consent, it is required to obtain consent from those in parental authority or their legal representatives.

Besides, even if obtaining the consent, the carrier is still required to ensure the transparency of information utilization for users, and to provide a service system where it is easy for users to withdraw their consent.[31]

4. Examination of Individual Cases

Typical questions frequently asked by carriers are reviewed as follows. However, as mentioned above, the relationship with the risk assessment in each case must be noted with regard to whether users' consent is valid to the utilization of information related to the secrecy of communications.

1-1) Collective Consent for Creating User Account

As mentioned above, valid consent regarding the secrecy of communications requires that the communication parties agree based on their true intentions with accurate understanding of the meaning.

On the other hand, similar procedures for obtaining consent are repeated as the information obtained from users increases, and explanation at point of obtaining consent becomes complicated and difficult to understand as the utilization methods become more complicated and diverse. As a result, there has been an issue, so-called "consent fatigue,"

---

[30] Telecommunications carriers may obtain and use information related to the secrecy of communications for the provision of telecommunications services. In that case, the act may be considered a lawful business act, and valid consent is required at point of use or provision for purposes other than the intended purpose.

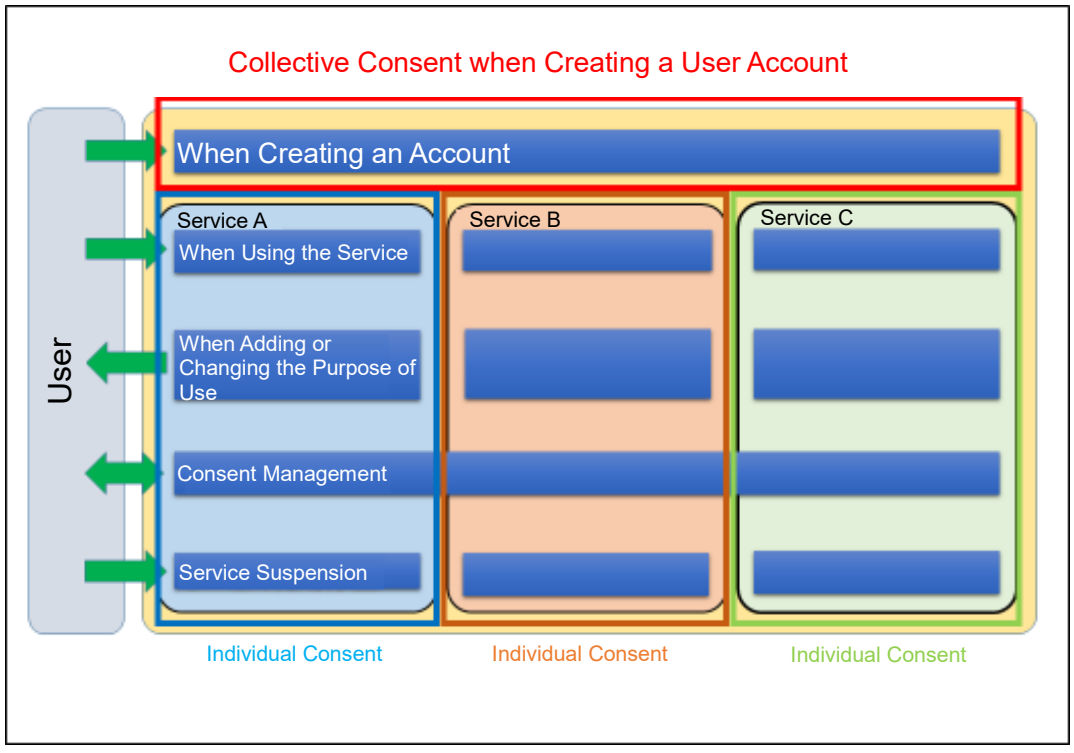
[31] However, with regard to obtaining, use, and provision of the secrecy of communications which are indispensable for providing services, it may be legalized as a lawful business act. A system for users' withdrawal of consent is not required for those justified not by users' consent.

where users consent without thorough understanding.[32]

For this reason, when there are multiple services, it is possible to obtain for each service each time in all cases, but it may be considered valid consent as well if they conduct an appropriate risk assessment process and collectively explain and obtain consent within the extent where the method of utilizing information related to the secrecy of communications in the services do not become complicated or diverse, and if the users can clearly recognize and understand that and consent based on their true intention. Even in cases where collective consent can be valid consent, it is required, for example, to enable users to withdraw their consent for each service later, and to make it easy to access the page to withdraw the consent.

Furthermore, since it is generally difficult for users to understand the explanation about obtaining consent collectively for multiple purposes of using information for multiple services, the process of explanation and obtaining users' consent requires considerable attention and thoroughness.

* Overall Consent Process (Image)



1-2) Obtaining Consent in Two layers

A. Tolerance

[32] Page 12 of *Final Report of the Study Group on Platform Services*, MIC (February 2020)

As mentioned above, to be considered valid consent regarding the secrecy of communications, it is required to be consent based on the true intention, with the communication party's accurately recognition and understanding of the contents and meaning of the consent.

On the other hand, similar procedures for obtaining consent are repeated as the information obtained from users increases, and explanation at point of obtaining consent becomes complicated and difficult to understand as the utilization methods become more complicated and diverse. As a result, there has been an issue, so-called "consent fatigue," where users consent without thorough understanding.

For this reason, it is rather inappropriate to just show users all the consent matters in detail. Instead, it is considered allowable, based on an appropriate risk assessment process, to obtain consent with a mechanism where an easy-to-understand summary with clear and plain language is offered in the first layer and only concerned users who clicked are led to the second layer (or the subsequent steps) offering detailed information, if the following points are ensured, and some measures are taken such as allowing the users to withdraw consent for each service later and making it easy to access the page for withdrawal.

B. What Items are to be Offered in the First Layer?

In order to be considered that communications parties accurately understood the contents and meaning, and consented based on their true intention, in light of the purpose of offering the summary version in the first step, as mentioned above, it is desirable to explain the consent matters within one or two screens on the terminal (without multiple screen transitions or scrolling).

Accordingly, the following items should be offered in the first layer: (i) the contents of the information to be obtained; (ii) the important ones among purpose of using the obtained information; and (iii) the way of use and the obtaining subject of the information to be obtained. As mentioned above, if the information will be used within the ordinarily predictable scope according to the certain service type, it is not required to specify individual purposes of use in detail, and consent may be obtained for each certain service type. However, since what items need to be explained to obtain users' consent in the first layer should be decided based on each case, each carrier is required to decide what items should be offered.[33]

[33] In light of risk assessment, when multiple service types (the purposes of use) are offered comprehensively in the first layer and it is considered valid consent to obtain consent without users' specific recognition, such case might be allowable if an opt-out procedure is provided for each service type (each purpose of use) in the second layer (or the subsequent steps). Besides, it is necessary to continue considering whether there are service types (the purposes of use) that should be particularly specified concerning the secrecy of communications.

1-3) How to Obtain Consent to Add Other Services to Existing Services

A. Whether New Consent is Required

In providing an additional service that has not provided as the initial service, consent for the new purpose of use should be additionally required unless the additional service can be ordinarily expected from the initial service.

For example, when a carrier that has provided an email service attempts to provide an additional service to personalize various services including the email service by newly analyzing email texts, new consent for the service is additionally required because such use is not ordinarily expected from the initial service.

On the other hand, it can be considered that new consent is not be required, as it is within the scope of valid consent for the initial service, in cases where valid consent has been obtained for the initial service and the additional service falls within the scope of use naturally expected from the initial service.

B. When New Consent is Required, Does Changing the Terms Suffice?

It has been frequently said by carries that it is difficult to obtain consent again from users who have been already using their services. In this regard, even when new consent is required, it is debatable whether changing the terms and conditions, terms of use, privacy policy, etc. suffices.

In order to for the consent under the contract terms to be considered as valid consent, it must contribute to users' interests, and it must be reasonably supposed that ordinary users will agree to the terms. For example, when adding a function such as a spam filtering service, changing the terms may be considered sufficient if certain conditions are met.[34] On the other hand, even if it will benefit users, users' individual and specific consent is considered to be additionally required if it cannot be reasonably supposed that ordinary users will consent, or if it relates to providing a service that would disadvantage the users.

2) Consent Management

A. Relationship between Consent Management and Valid Consent

Systems such as a privacy dashboard are desirable to ensure carries' transparency

[34] Regarding filtering spam email, it has been considered filtering based on users' valid consent if the following conditions are met: (i) even after the users consented to provision of the filtering service, such consent may be changed at any time (settings may be changed) at will; (ii) other conditions for provision are the same regardless of whether the users consent to the provision of the filtering service; (iii) the contents of the filtering service is clearly limited; (iv) it is reasonably supposed, from grounds such as questionnaire survey results, that ordinary users will consent to provision of the service; (v) sufficient prior explanations are offered to users about the contents etc. of the filtering service (such explanation is subject to the procedure based on the explanation of important matters stipulated in Article 26 of the Act). (Document 18-1 *Filtering and Secrecy of Communications* of the Round-table Conference on Privacy Information in the Telecommunications Business Field, January 1, 2006).

and facilitate withdrawal of users' consent. Furthermore, when considering how to obtain users' consent by risk assessment, providing a mechanism that allows users to easily manage their consent can be evaluated as one of the factors to justify simplifying the consent procedure.

If various services displayed on the management tool are set to OFF as default and users turns the corresponding tab ON by themselves as a new service is added, it has the meaning of users' clear consent.

B. Can a Dashboard (ON as Default) substitute users' consent when adding a new service?

i) Clear Consent

It cannot be considered clear consent required for the secrecy of communications to obtain fictitious consent under the terms of use and privacy policy by adding a new service set to ON by default to the privacy dashboard.

On the other hand, there might be valid consent in cases where ordinary users can assume the use of their information each time, a voluntary opt-out means is prepared as well, and a risk assessment is conducted.[35]

ii) Selection Detailedness on the Dashboard

Users' feelings about the appropriate degree of selection detailedness on the dashboard vary depending on the person. Since some users want detailed control, but other users are satisfied with simple control, whether the selection detailedness is appropriate depends on the case. However, it can be considered that, for example, system where users can withdraw their consent for each service is required if users' consent has been collectively obtained at point of obtaining consent.

C. Others

i) Regular Reminders of Consent Management

Even if users' valid consent is obtained at a certain point in time, they will not necessarily have intention of such consent continuously in the future. Therefore, it is evaluated as a desirable approach to confirm the users' consent by regular reminders for them. In such case, systems with considering the transparency, such as ones facilitating access to the privacy dashboard etc., are important.

[35] Regarding caller information notification services over the phone, if the caller does not prevent the caller information notification (such as when 184 is not pressed), it is considered that the caller does not intend to keep the caller information confidential to the other party. (*See* Article 34 of *Commentary for Guidelines for Protection of Personal Information in Telecommunications Business*)

(Attachment)

Reference

[Telecommunications Business Act (excerpt)]

Chapter I General Provisions

(Protection of Secrecy)

Article 4 (1) The secrecy of communications handled by a telecommunications carrier must not be violated.

(2) A person who is engaged in telecommunications business must not disclose other persons' secrets which came to their knowledge while in service with respect to communications handled by a telecommunications carrier. The same applies even after that person has left office.

Chapter II Telecommunications Business

(Reporting on the Suspension of Telecommunications Operations and on Serious Accidents)

Article 28 If a telecommunications carrier suspends its telecommunications operations in part pursuant to the provisions of Article 8, paragraph (2), or a violation of secrecy of communications or any other serious accident specified by Order of the Ministry of Internal Affairs and Communications has occurred with respect to telecommunications operations, it must report without delay to the Minister for Internal Affairs and Communications to that effect including its reason or cause.

(Order to Improve Business Activities)

Article 29 (1) If the Minister for Internal Affairs and Communications finds that the operations of a telecommunications carrier fall under any of the following items, the Minister may order the telecommunications carrier to improve its means of conducting the operations or take other measures to the extent necessary for ensuring the interests of users or the public interest:

(i) if there is a hindrance in ensuring secrecy of communications with respect to the telecommunications carrier's means of conducting operations;

(The rest is omitted.)

Chapter VI Penal Provisions

Article 179 (1) A person that has violated the secrecy of communications handled by a telecommunications carrier (including communications set forth in Article 164, paragraph (3), notifications issued by the Certified Association against Cyberattacks on Telecom Equipment as specified by Article 116-2, paragraph (2), item 1 (b), which is considered as communication during the handling of a telecommunications carrier pursuant to the provisions of paragraphs 4 and 5 of the same Article, and electromagnetic records of communication history handled by the Certified Association against Cyberattacks on Telecom Equipment as specified by item 2 (b) of the same paragraph.) shall be punished by not more than two years or a fine of not more than one million yen.

(2) A person engaging in telecommunications business (including the work listed in Article 116-2, paragraph (2), item (i) or item (ii) conducted by the Certified Association against Cyberattacks on Telecom Equipment, which

is considered to be engagement in the telecommunications business pursuant to the provisions of Article 164, paragraphs 4 and 5) that has undertaken the act set forth in the preceding paragraph is punished by imprisonment of not more than three years or a fine of not more than two million yen.

(3) An attempt to commit the offenses set forth in the preceding two paragraphs is subject to punishment.

Article 186 A person that falls under any of the following items is punished by a fine of not more than two million yen:

(i) and (ii) (Omitted.)

(iii) a person that has violated any order or disposition under Article 19, paragraph (2), Article 20, paragraph (3), Article 21, paragraph (4), Article 29, paragraph (1) or paragraph (2), Article 30, paragraph (5), Article 31, paragraph (4), Article 33, paragraph (6) or paragraph (8), Article 34, paragraph (3), Article 35, paragraph (1) or paragraph (2), Article 38, paragraph (1) (including as applied mutatis mutandis pursuant to Article 39), Article 39-3, paragraph (2), Article 43, paragraph (1) (including as applied mutatis mutandis pursuant to paragraph (2) of the same Article), Article 44-2, paragraph (1) or paragraph (2), Article 44-5, Article 51 or Article 121, paragraph (2), Article 73-4 or Article 121, paragraph (2);

(The rest is omitted.)

[Comparison with GDPR (ePR)]

- The draft ePrivacy Regulation refers to GDPR for the definition and handling of consent regarding the processing of communications and metadata.
- Article 4 (11) of the GDPR defines consent, stipulating "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." (Valid consent conditions are specified in Article 7)
- In November 2017, the *Guidelines on Consent* were formulated by the Working Group under Article 29 (partially revised by the EDPB in May 2020). The Guidelines describe details of "freely given," "informed," "unambiguous," "by statement of by an affirmative action," etc. Furthermore, the *Guidelines on Transparency* have also been formulated, showing how to inform users of handling of data etc.
- The GDPR requires consent for one or more specific purposes under the requirement of "specific" in the definition of consent.

[Comparison with Personal Information Protection Act]

- There are four provisions regarding the principal's consent in the Personal Information Protection Act: Article 16 (Restriction due to a Utilization Purpose); Article 17 (Proper Acquisition); Article 23 (Restriction on Third Party Provision); and Article 24 (Restriction on Provision to a Third Party in a Foreign Country).
- In the same Act, consent under the contract terms is not necessarily denied, because the principal's consent means an indication of intention to consent to having their personal information handled in a manner

indicated by the personal information handling business operator, and because it is permitted to obtain consent in a reasonable and appropriate manner that is considered necessary for the principal to decide on consent according to the nature of the business and the handling conditions of the personal information (*Guidelines for the Act on the Protection of Personal Information (General Rules)*). Also, MIC's Commentary for Guidelines states that "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...and such clauses are valid under private law…, it is interpreted to mean that "a principal's consent is being sought" or "a principal's consent has been obtained."

- On the other hand, regarding personal information that falls within the secrecy of communications, individual, specific and clear consent, and consent under the contract terms is not accepted because of the seriousness of the right.
- The specific age of children who need to obtain consent from a legal representative, etc. should be determined individually and specifically according to the items of personal information subject to the consent and the nature of the business. However, it is considered necessary to obtain the consent of legal representatives, etc., for children aged 12 to 15 years or younger.[36]

[36] *Guidelines for the Act on the Protection of Personal Information* and *Q & A regarding Response in Case of Leakage of Personal Data* (Q1-58)