Guidelines for Issuance of a Business Improvement Order to Prevent Hindrance in Ensuring the Secrecy of Communications

1. Purpose of Formulation

(1) Regulations related to Secrecy of Communications

Article 21, Paragraph 1 of the Constitution of Japan guarantees freedom of expression as a basic human right. Paragraph 2 prohibits censorship and protects the secrecy of any means of communication.[1] The protection of the secrecy of communications in the Constitution is considered important not only to protect the people's privacy, but also to guarantee the people's freedom of expression and right to know by maintaining the secrecy of communications.[2]

"Chapter I General Provisions" of the Telecommunications Business Act (Act No. 86 of 1984; hereinafter referred to as the "Act") stipulates, "The secrecy of communications handled by a telecommunications carrier must not be violated." (Article 4 of the Act)[3] This provision can be considered to embody the secrecy of communications at the legal level to secure the above constitutional

---

[1] The Constitution of Japan
Article 21. Freedom of assembly and association as well as speech, press and all other forms of expression are guaranteed.
2. No censorship shall be maintained, nor shall the secrecy of any means of communication be violated.

[2] State power must not violate the secrecy of communications. Furthermore, it is important to protect the secrecy of communications from violation by private individuals and to guarantee a communication system that can be used safely and securely by the people from the viewpoint of ensuring the people's freedom of expression and right to know.

[3] Telecommunications Business Act
(Protection of Secrecy)
Article 4. 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.

requirements.[4] Telecommunications service users'[5] communications are protected by prohibiting anyone including the telecommunications carriers that handle the services from violation on the secrecy of communications, then make users rest assured in using communications, which leads to guarantee of freedom of expression and the right to know. This is regarded as contributing to secure users' trust in the telecommunications network and the communication system itself, and as realizing the sound development of telecommunications and the people's convenience by various services and businesses.

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 available to others).

Even when obtaining information related to the secrecy of communications, it does not constitute a violation on the secrecy of communications if there are users' valid consent. Furthermore, in cases where it falls under justifiable acts (Article 35 of the Penal Code (Act No. 45 of 1907)), self-defense (Article 36),

---

[4] The prohibition of censorship is stipulated in Article 3 of the Act and Article 7 of the Postal Act (Act No. 165 of 1947). In addition, the protection of secrecy of communications is stipulated in Article 8 of the Postal Act, Article 59 of the Radio Act (Act No. 131 of 1950) and Article 9 of the Wired Telecommunications Act (Act No. 96 of 1953). The penalties are stipulated in Article 80 of the Postal Act, Article 109 and Article 109-2 of the Radio Act, and Article 14 of the Wired Telecommunications Act.

[5] Article 1 specifies, "The purpose of this Act is to ensure that telecommunications services are provided smoothly, and the interests of the users of the services are protected, through making the operation for telecommunications services proper and reasonable and promoting the fair competition in telecommunications business in consideration of the public nature of telecommunications business, thereby ensuring the sound development of telecommunications and the convenience of the lives of the people, and increasing the public welfare." The protection of users in the secrecy of communications protects those who actually receive services, and in *Guidelines for Protection of Personal Information in Telecommunications Business*, the term "users" refers to those who use telecommunications services (see Article 3, Paragraph 4 of the Guidelines).

necessity (Article 37), it is considered to be exceptionally justified. For example, regarding communications history, Article 32 of the *Guidelines for Protection of Personal Information in Telecommunications Business*[6] (hereinafter referred to as the "Guidelines") stipulates, "Telecommunications carriers may record communication history...only where necessary in order to charge fees, issue invoices, respond to complaints, prevent unauthorized use or conduct other operations." These are positioned as lawful business acts.[7]

It is understood that in view of the purpose of protecting the secrecy of communications, the scope of "the secrecy of communications" includes not only the content of individual instances of communications, but also any matter from which the communications content can be inferred, such as the date and time, and places of individual instances of communications, the corresponding person's name, address or locations, identification codes of the party involved such as telephone numbers, as well as the number of communication times.[8] Based on this, the commentary for the Guidelines stipulate "the secrecy of

---

[6] MIC Notice No. 152 of 2017

[7] According to the commentary for Article 32 of the Guidelines, "if it is necessary in order to charge fees, issue invoices, respond to complaints, prevent unauthorized use, or conduct other operations, such recording is deemed at least as a lawful business act, and illegality is precluded."

[8] It is understood that the scope of guarantee of the secrecy of communications in the latter part of Article 21, Paragraph 2 of the Constitution of Japan extends to external facts related to communications, such as the names of the senders and recipients of communications, and the date and time of each communication (Nagoya District Court, September 2, 2016 and others). Furthermore, regarding the scope of guarantee of the secrecy of communications in Article 4, Paragraph 1 of the Act, it should be understood that the secrecy of communications includes the content of communications, as well as the addresses, names, telephone numbers, sending and receiving locations of the party to the communications, date and time of each communication, as well as number of times of communications. In any case, the purpose of guaranteeing the secrecy of communications is to effectively protect the privacy of individuals and to guarantee the freedom of thought and expression of individuals. It is because even if a person knows the address, name, telephone number, etc. of the other party of communication, the freedom of thought and expression of the other party may be suppressed (Tokyo District Court, April 30, 2002). In addition, the scope of guarantee of secrecy of correspondence in Article 8, Paragraph 1 of the Postal Act is not limited to the content of communication, but extends to information on the presence of each communication itself, that is, the names, addresses, locations, etc. of the sender and recipient of the correspondence (Osaka District Court, November 29, 2017).

communications (which includes not only the content 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) ." [9]

"Section 3 Operations of Telecommunications Carriers, Chapter II Telecommunications Business" of the Act stipulates "[the case where] there is a hindrance in ensuring secrecy of communications concerning the telecommunications carrier's means of conducting operations" (Article 29, Paragraph 1, Item 1)[10] as one of the cases where 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." [11] The Act requires that telecommunications carriers "ensure the secrecy of communications," and if these provisions are not observed, rectification will be requested by ordering business improvement based on Article 29, Paragraph 1, Item 1 of the Act.[12]

---

[9] Commentary 2-13 (Consent of the Person) of Article 2 of the Guidelines

[10] Telecommunications Business Act
(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;
(ii) (Omitted)

[11] It is stipulated that "if a telecommunications carrier suspends its telecommunications operations or commits a violation of secrecy of communications or any other serious accident specified by Order of the Ministry of Internal Affairs and Communications 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." (Article 28)

[12] The Minister for Internal Affairs and Communications shall be able to request telecommunications carriers to report necessary matters to the extent necessary for the enforcement of this Act, and to have authority for on-site inspection (Article 166, Paragraph 1).

"Chapter VI (Penal Provisions)" of the Act stipulates penalties etc. for those who violated the secrecy of communications handled by a telecommunications carrier (Article 179),[13] and penalties for those who violated the order pursuant to Article 29, Paragraph 1, Item 1 of the Act (Article 186, Item 3 of the Act).[14] The Act protects "interests of the users" (Article 1 of the Act) by protecting the secrecy of communications under these provisions.

(2) Purpose of Formulating the Enforcement Guidelines

In the information and communications field, telecommunications carriers' services are becoming more diversified and complicated due to new technologies development and market structure changes, and it is expected that telecommunications carriers will provide various services one after another by utilizing user information, including information related to the secrecy of communications. Regarding the information related to the secrecy of communications that each telecommunications carrier handles in providing these services, since provided service, the type and scale of handled information related to the communications, the usage pattern, etc. vary depending on each carrier, each carrier is required to autonomously take appropriate action according to each situation.

---

[13] Telecommunications Business Act
Article 179 (1) A person that has violated the secrecy of communications handled by a telecommunications carrier (including communications under Article 164, paragraph (3) (omitted) is punished by not more than two years or a fine of not more than one million yen.
(2) A person engaging in telecommunications business (omitted) 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.

[14] Telecommunications Business Act
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 29, paragraph (1) or paragraph (2)...;
(iv) through (vi) (Omitted)

When a telecommunications carrier attempts to autonomously take appropriate action, it is useful to perform a risk assessment from the perspective of ensuring the secrecy of communications, in order to consider appropriate business methods from the perspectives of obtaining and use of information related to the secrecy of communications, an effective system for obtaining consent from users, managing information, responding to complaints and consultation requests, etc.

To ensure that telecommunications carriers take appropriate action, if there is a hindrance in ensuring the secrecy of communications, e.g., the telecommunications carrier's autonomous action does not function sufficiently or the handling of information related to the secrecy of communications regarding the telecommunications carrier's business method is inappropriate, it is important to enable users to use telecommunications services with security, by the Minister for Internal Affairs and Communications' issuance of an order against any telecommunications carrier to improve operations, which is an administrative disposition (hereinafter referred to as a "business improvement order") based on Article 29, Paragraph 1, Item 1 of the Act.

Based on such background, for the purpose of clarifying the concept of ensuring the secrecy of communications and for increasing the transparency and predictability by typologically offering the criteria and cases as criteria for the Minister for Internal Affairs and Communications' issuance of a business improvement order based on judging the efforts of telecommunications carriers did not function sufficiently, these guidelines for issuance of a business improvement order have been formulated (hereinafter referred to as the "Enforcement Guidelines").

The Enforcement Guidelines, which are concerning Article 29, Paragraph 1, Item 1 of the Act, have been newly established and published. It is expected that each carrier will refer to the Enforcement Guidelines to ensure the proper

handling of information related to the secrecy of communications and further enhance the information management system and complaint consultation system. The Ministry of Information and Communications (MIC) will hold continuous dialogues with each telecommunications carrier, considering that new technologies and service trends are expected in the future as the development in the information and telecommunications field. MIC will continue reviewing the Enforcement Guidelines as necessary in light of their operational status and changes in circumstances.

2. Enforcement Guidelines for Business Improvement Orders

1. Purpose of Article 29, Paragraph 1, Item 1 of the Act

Telecommunications services provided by telecommunications carriers play a major role in the socio-economic infrastructure supporting people's daily lives and industrial economic activities. Therefore, if "the secrecy of communications" is not secured because means of conducting operations are inappropriate, "the protection of users' interests" as specified in the purpose of Article 1 of the Act will not be possible, and there will be a significant impact on the interests of the users.

For this reason, Article 29, Paragraph 1, Item 1 of the Act stipulates, as a requirement for business improvement orders, "[cases where] there is a hindrance in ensuring secrecy of communications with respect to the telecommunications carrier's means of conducting operations."

This item's purpose is that if the telecommunications carrier's means of conducting operations are found to fall under this item and hinders interests of the users, MIC encourages telecommunications carriers to make efforts, take measures to protect the secrecy of communications properly, and protect

interests of the users,[15] by ordering a telecommunications carrier to improve the means of conducting operations and take different measures.

Incidentally, because business improvement order is an extremely strong measure against a telecommunications carrier, it can be issued “to the extent necessary for removing obstacles to the interests of users or the public interest,” and it is stipulated that the Minister for Internal Affairs and Communications must consult the Telecommunications Dispute Settlement Commission on the issuance of a business improvement order (Article 160) and hold a hearing of the Committee members as official presiding(Article 161, Paragraphs 1 and 2). If a telecommunications carrier violates a business improvement order, a penalty (a fine of not more than two million yen) shall be imposed (Article 186, Item 3).

2. Concept of Telecommunications Carriers

Business improvement orders are discipline for “Telecommunications Carriers” subject to registration based on Article 9 of the Act or notification based on Article 16 Paragraph 1 of the Act on operating telecommunications businesses. Those outside the scope of the above registration or notification (Article 164, Paragraph 1) are not directly subject to this business improvement orders.[16]

In cases where “Telecommunications carriers” also provide other

[15] There is administrative guidance for the purpose of carrying out kind of disciplinary action on carriers, investigation of causes, prevention of recurrence of the same type or similar cases, and alerting users. Administrative guidance is defined as “guidance, recommendations, advice, or other acts by which an Administrative Organ may seek, within the scope of its duties or affairs under its jurisdiction, certain action or inaction on the part of specified persons in order to realize administrative aims, where such acts are not Dispositions.” (Article 2, No. 6 of the Administrative Procedure Act (Act No. 88 of 1993))

[16] Although not falling under “communications handled by a telecommunications carrier,” Article 4 (Protection of Secrecy) of the Act also applies to communications handled by those engaged in the telecommunications businesses specified in each item of Article 164, Paragraph 1, which are exempt from the application of the Act (Article 164, Paragraph 3). Similarly, there are penal provisions for the violation of communications stipulated in Article 164, Paragraph 3 of the Act (Article 179, Paragraph 1 noted in brackets).

telecommunications services together that are exempted from the application of the Act and are not subject to registration or notification, if it is evaluated that "a hindrance in ensuring secrecy of communications" in such telecommunications services may indirectly "[hinder] ensuring secrecy of communications" in their main telecommunications services which is subject to registration or notification, then such telecommunications carriers may be subject to business improvement orders.

3. Concept of "Means of Conductions Operations"

The term "business activities" stipulated in Article 29, Paragraph 1 of the Act refers to telecommunications carriers' operations, so this term is mainly assumed for the telecommunications operations stipulated in Article 2, Item 6 of the Act, i.e., telecommunications services provided by telecommunications carriers' according to others' demands. However, it is not limited to telecommunications services per se but it includes broader services such as services provided as part of telecommunications services and inseparable from such services(such as filtering on the network, lease of router and other network devices, and system development and maintenance), services based on the use of telecommunications services provided by a telecommunication 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), and business work like contractual work and charge collection, and maintenance of telecommunications equipment related to that operation.

The means of "conducting operations" covers all business operations for handling information related to "the secrecy of communications", such as business management and daily business handling, including window services and the means of conducting operations is not only formally evaluated by the

internal rules of telecommunications carriers but is objectively evaluated in light of the actual situation of the business. Furthermore, it does not matter whether the operations are handled by humans or by machine.

4. Concept of "[Cases where] there is a Hindrance in Ensuring Secrecy of Communications"

(1) Scope of "Secrecy of Communications"

As mentioned above, it is understood that the scope of "the secrecy of communications" includes not only the content of individual instances of communications, but also any matter from which the communications content can be inferred, such as the date and time, places of individual instances of communications, the corresponding person's name and address or locations, identification codes of the party involved such as telephone numbers, and the number of communication times.

(2) "If there is a Hindrance in Ensuring Secrecy of Communications"

"[Cases where] there is a hindrance in securing the secrecy of communications" mean cases where the operational handling of the secrecy of communications is inappropriate, cases where a system for protecting the secrecy of communications is insufficient, etc., and specific cases that are assumed are shown in Section 5 below.

In principle, violation of "the secrecy of communications handled by telecommunications carriers" (Article 4, Paragraph 1 and Article 179, Paragraph 1) is considered to fall under the case "if there is a hindrance in ensuring the secrecy of communications."

5. Assumed Cases "[where] there is a Hindrance in Ensuring Secrecy of Communications"

To demonstrate some acts which fall under cases "[where] there is a hindrance in ensuring the secrecy of communications" as stipulated in Article 29, Paragraph 1, Item 1 of the Act and "business improvement orders may be issued," namely, acts which may cause problems, the Guidelines categorize the acts into four types and illustrate them by the following examples: (i) Inappropriate policies of handling user information, including information related to the secrecy of communications;[17] (ii) Inappropriate obtaining and use etc. of the secrecy of communications, (iii) Inappropriate information management; (iv) Inappropriate response to complaints and consultations.

As described above, even if obtaining information related to the secrecy of communications, it does not constitute a violation of the secrecy of communications if the user has provided valid consent, which does not fall under cases where "there is a hindrance in ensuring the secrecy of communications." To obtain the user's "valid consent", "how to obtain consent" is important, but how to obtain consent should be evaluated for each service. In general, it is required to properly go through a risk assessment process for the service and obtain consent in a way that users can recognize. Regarding "how to obtain consent", refer to the commentary for the Guidelines and "*Reference Document on How to Obtain Consent*," and respond appropriately.

Even in the case of acts not illustrated here, whether they fall under cases

---

[17] Regarding the handling of information related to the secrecy of communications, all acts "unauthorized obtaining", "unauthorized use" "unauthorized leakage" etc. are in principle illegal acts, and are only justified if there is valid consent of the users or justifiable cause for noncompliance with the law. Regarding the handling of information related to the secrecy of communications, as the Act on the Protection of Personal Information (Act No. 57 of 2003, hereinafter referred to as the "Personal Information Protection Act") stipulates the handling of personal information, it should be kept in mind that it is not sufficient to just notify and announce the purpose of use for the acquisition of personal information (see Article 18 of the Personal Information Protection Act).

"[where] there is a hindrance in ensuring the secrecy of communications" should be determined on a case-by-case basis in light of the provision of Article 29, Paragraph 1, Item 1 of the Act, and even in the illustrated cases, a business improvement order will not necessarily be issued only because of a single applicable act.

(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

[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*.

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.

(3) Examples of Inappropriate Information Management Systems

(i) Examples of Inappropriate Organizational Security Control Actions

i. As a telecommunications carrier's internal control structure (so-called internal control system) related to the secrecy of communications, including the compliance system for laws and regulations related to protecting the secrecy of communications and the risk management system, is insufficient, the handling of the secrecy of communications is

inappropriate.

ii. In the event of a communication system failure or malfunction etc., a telecommunications carrier's system risk assessment related to the secrecy of communications was inappropriate, which resulted in accidents, including leakages of the secrecy of communications.

iii. Although a telecommunications carrier was aware of the possibility of accidents such as leakages of secrecy of communications, the fact was concealed or falsified.

iv. When an accident such as leakages of the secrecy of communications occurred, the cause of the accident was insufficiently or inappropriately investigated, then the preventive measures for recurrence taken were insufficient or inadequate and not practically functioning.

(ii) Examples of Inappropriate Human Security Control Actions

i. As a telecommunications carrier's in-house dissemination, education, and training regarding the secrecy of communications were inappropriate, the employees' [19] understanding of the secrecy of communications is inadequate.

ii. In violation of company rules, employees of a telecommunications carrier repeatedly took out business terminals that handle the secrecy of communications, then the telecommunications carrier overlooked such actions even though it was aware of such acts.

iii. Employees of a telecommunications carrier or its contractor

[19] The term "employee" 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 includes not only employees in an employment relationship (such as full-time employees, contractual employees, commissioned employees, part-time workers, and temporary employees, etc.), but also directors, executive officers, board members, statutory auditors and dispatched workers, etc.

unnecessarily informed third parties of the secrecy of communications which came to their knowledge on their service, used it for an unreasonable purpose, or leaked it due to negligence.

(iii) Examples of Inappropriate Physical Security Control Actions

i. A communications carrier's management and operation of areas where communications system including servers handling the secrecy of communications is managed (controlled areas) and areas where office work handling the secrecy of communications is operated (handling areas) were inappropriate.
ii. A communications carrier's management and operation of equipment were inappropriate, e.g., it neglected to manage machine room entry and exit records.
iii. Although a telecommunications carrier strictly set the storing period of information related to the secrecy of communications, the storage status was inappropriate, e.g., in violation of this, the telecommunications carrier stored information unnecessarily even after the lapse of the period.

(iv) Examples of Inappropriate Technological Security Control Actions

i. A telecommunications carrier took insufficient measures to minimize system troubles such as malfunctions and incorrect settings due to repairs of the information and communication system.
ii. A telecommunications carrier's technological security control actions from security threats and environmental threats (e.g., water leakage, fire, power outage) for equipment and devices that handle the secrecy communications were insufficient.

iii. A telecommunications carrier did not take appropriate access control actions, then employees who no longer needed to access information related to the secrecy of communications due to organizational changes were left in a state where they could access the information.
iv. Information related to the secrecy of communications was backed up unnecessarily for business handling and information was in a state where it could be taken out by those who were not permitted or approved to take it out.

(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.