Mobile Software Competition Act Guidelines
(Draft)

Japan Fair Trade Commission

I. Introduction

These guidelines, based on Article 46 of the Act on Promotion of Competition for Specified Smartphone Software, or the Mobile Software Competition Act (Act No. 58 of 2024, hereinafter referred to as "the Act"), aim to clarify actions that violate the prohibited conduct stipulated in Section 1 of Chapter 3 of the Act and measures that designated providers must take to comply with the provisions regarding measures to be taken by designated providers, or compliance measures, in Section 2 of the same chapter. The goal is to contribute to the smooth and appropriate application of the Act by clarifying the Japan Fair Trade Commission's (JFTC) policy for its enforcement.

Given the rapid advancements in technology and services surrounding specified software (basic operation software, application stores, browsers, and search engines) particularly necessary for smartphone use, new challenges may arise in the future. Therefore, these guidelines will be reviewed as necessary, taking into account changes in market conditions and business practices related to specified software.

II. Basic Understanding

1. Importance of Promoting Competition in the Field of Specified Software

With smartphones becoming the foundation of daily life and economic activity, it's crucial to ensure fair and open competition in the market for specified software, beginning with competition between third-party app providers regarding the provision of individual software. Through such fair and open competition, innovations in specified software and individual software are promoted, for example, by allowing new application stores to emerge and encouraging the development of innovative software solutions that utilize advanced smartphone features. As a result, smartphone users can make informed choices and enjoy a wider array of benefits from the diverse services created.

The seamless and appropriate application of this Act is essential to secure fairness and openness in these software markets. The Japan Fair Trade Commission (JFTC) will engage in ongoing dialogue with designated providers to ensure their compliance, strictly addressing violations such as prohibited conduct under Articles 5 to 9 and promoting their compliance with necessary measures under Articles 10 to 13, making the regulations proportionate to the competition related problems at hand. Furthermore, in the market for specified software, there

are various stakeholders other than designated providers, such as third-party app providers. The JFTC will engage in ongoing dialogue with these stakeholders and collaborate with relevant government ministries and agencies, as well as competition authorities in other countries, to ensure the smooth and appropriate application of the Act.

Additionally, smartphone users are important stakeholders. It is crucial to continue ensuring necessary and sufficient responses regarding cybersecurity for smartphone use, protection of information related to smartphone users, and safeguarding youth who use smartphones. The aim is to balance ensuring fair and open competition in the specified software market with ensuring safety and security for smartphone users. Through dialogue with various stakeholders, including designated providers, the JFTC will work to improve the competitive environment among businesses in the market for specified software.

2. Relationship Between This Act and the Antimonopoly Act

Actions violating prohibited conduct under Articles 5 through 9 of this Act are generally categorized as antitrust violations. Considering the intent behind the enactment of this Act, which is to swiftly eliminate practices restricting competition by making determinations of violations based on formal act requirements, cases (concerning designated providers and their conduct) that overlap between this Act and the Antimonopoly Act shall, as a general rule, prioritize the application of this Act.

Furthermore, for restrictive actions concerning the use of technology due to the existence of intellectual property rights such as copyrights, patent rights, utility model rights, design rights, and trademark rights, the determination will be made in accordance with conventional practices under the Antimonopoly Act, considering the purpose and nature of the conduct and its impact on competition, to assess whether it deviates from or goes against the purpose of the intellectual property system which encourages innovation and the utilization of technology. In such cases, if the restriction of technology is recognized as a legitimate exercise of intellectual property rights, it will be determined that the conduct is not in violation of Articles 5 through 9 of this Act.

(Note) Restrictive actions concerning the use of technology include: ① actions by a rights holder of a certain technology to prevent others from using that technology, ② actions to

license that technology to others with limited scope of use, and ③ actions to impose restrictions on the activities of the licensee when licensing the technology to others.

III. Understanding Prohibited Conduct and Compliance Requirements

To clarify actions that violate the prohibited conduct stipulated in Chapter 3 Section 1 of the Act and measures that designated providers should take to comply with the provisions regarding measures to be taken (compliance requirements) by designated providers in Section 2 of the same chapter, the following sections organize the basic understanding, specific interpretations, and hypothetical scenarios of violations for each of these articles.

It should be noted that the hypothetical scenarios provided are merely illustrative examples, and the application of the Act will be determined based on individual case-specific circumstances. Furthermore, actions not described in these hypothetical scenarios may also be deemed a violation of the Act based on individual case-specific circumstances.

1. Article 5: Prohibited Conduct Related to Unjust Usage of Acquired Data

(1) Basic Approach

Article 5 of this Act prohibits designated providers (those designated for their basic operation software, application store, or browser) from using data acquired through the utilization of such specified software to competitively benefit their own (or their subsidiaries') goods or services, specifically when those goods or services are in a competitive relationship with those provided by other third-party app providers or website operators. The use of data collected by designated providers for their own goods or services may lead to competition issues by providing advantages in marketing, development, etc., compared to third-party app or website providers. The prohibition aims to promote competition among individual software.

(2) Specific Understanding of Article 5

A. Approach to the Scope of Covered Data

It is challenging to comprehensively confirm what kind of data designated providers of basic operation software, application stores, or browsers acquire. Additionally, the technological advancements and market developments surrounding specified software for smartphones are significant. Thus, the types of data subject to Article 5 are comprehensively and abstractly defined in the Enforcement Rules (Rules of the Japan Fair Trade Commission No. 5 of

December 13, 2024, hereinafter referred to as "the Rules") established by the JFTC. Guidelines enumerate specific examples of what data is primarily anticipated to be in scope, ensuring foreseeability for designated providers and allowing flexible enforcement in response to technological progress and market changes.

The specific examples of data listed below are illustrative and do not prevent the application of Article 5 to data not explicitly mentioned. Whether data falls within the scope of Article 5 will be determined on a case-by-case basis, in light of the provisions of the Rules.

(A) Common Items (Data concerning smartphone users)

Examples of "data concerning smartphone users utilizing individual software or viewing web pages" as prescribed in Rules Article 14, Item 1, Article 15, Item 1, and Article 16, Item 1 include the following data:

- Data related to smartphone user attributes (name, age, gender, place of residence, contact information, etc.)
- Data related to identifiers of smartphone users or smartphone devices (account ID, cookies, advertising ID, IP address, etc.)
- Data necessary for smartphone users' payments (credit card numbers, bank account numbers, payment service provider account numbers, etc.)

It should be noted that some of this data, for example, may be entered by smartphone users during initial smartphone setup, meaning designated providers may acquire it directly from users without the user's utilization of individual software or browsing of web pages. Even if designated providers use such data for the provision of their own (or their subsidiaries') goods or services, it generally does not create the competitive issues mentioned in (1). Therefore, the data defined in Rules Article 14, Item 1, Article 15, Item 1, and Article 16, Item 1 excludes data provided by smartphone users without the use of individual software or viewing web pages. Consequently, if a designated provider uses only data acquired directly from smartphone users for the provision of goods or services that are in a competitive relationship with those provided by other third-party app providers or website operators, it does not violate Article 5 of the Act.

(B) Basic Operation Software Related

"Data acquired by the designated provider in connection with the use of the basic operation

software for the provision of individual software by other third-party app providers" as referred to in Article 5, Item 1 of the Act, includes cases where the designated provider (referring to those designated for basic operation software; hereinafter the same in (B)) acquires data when smartphone users utilize individual software provided by third-party app providers, as well as cases where the designated provider acquires data during the review of individual software when third-party app providers provide individual software.

Examples of data prescribed in Rules Article 14, Item 2 and Item 3, respectively, include the following data (including data obtained by statistically processing this data):

a. "Data generated or provided while smartphone users are utilizing individual software"

- Data related to the status of smartphone users' downloads, installations, and uninstallations of individual software.
- Data related to the duration, period, and frequency of smartphone users' use of individual software.
- Location information data related to smartphone users' use of individual software.
- Data related to websites displayed within individual software or displayed by browsers launched from individual software.
- Data related to purchase history and other usage status associated with smartphone users' use of individual software.
- Data related to OS functions (functions controlled by the designated provider's basic operation software, such as audio output functions and other smartphone operation functions) used by individual software and their usage status.
- Data related to errors during individual software operation.
- Data related to memory used by individual software, power consumption, and other operational functions.

b. "Data related to the content and specifications of individual software"

- Data related to the service content of individual software.
- Data related to the technical specifications when individual software uses OS functions.
- Other data related to the technical specifications of individual software.

(C) Application Store Related

"Data acquired by the designated provider in connection with the use of the application store for the provision of individual software by other third-party app providers" as referred to in Article 5, Item 2 of the Act, includes cases where the designated provider (referring to those designated for application stores; hereinafter the same in (C)) acquires data when third-party

app providers provide or update individual software through the application store, as well as cases where the designated provider acquires data during the review of individual software when third-party app providers provide individual software.

Examples of data prescribed in Rules Article 15, Item 2 and Item 3, respectively, include the following data (including data obtained by statistically processing this data):

a. "Data generated or provided while smartphone users are utilizing individual software"
- Data related to smartphone users' access to the application store for individual software and search status within the application store.
- Data related to the status of smartphone users' downloads, installations, and uninstallations of individual software.
- Data related to responses to notifications concerning individual software.
- Data related to ratings and comments for individual software.
- Data related to purchase history and other usage status associated with smartphone users' use of individual software.
- Data related to errors during individual software operation.

b. "Data related to the content and specifications of individual software"
- Data related to the service content of individual software.
- Data related to the technical specifications when individual software uses OS functions.
- Other data related to the technical specifications of individual software.

(D) Browser Related

"Data acquired by the designated provider in connection with the display of web pages presented by other website operators using the browser" as referred to in Article 5, Item 3 of the Act, refers to cases where the designated provider (referring to those designated for browsers; hereinafter the same in (D)) acquires data when website operators present web pages or after they have presented them.

Examples of data prescribed in Rules Article 16, Item 2 and Item 3, respectively, include the following data (including data obtained by statistically processing this data):

a. "Data generated or provided when smartphone users display web pages"
- Data related to the number of times smartphone users display web pages.
- Data related to the duration, period, and frequency of smartphone users' browser usage.
- Data related to OS functions used by the browser and their usage status.
- Data related to other individual software launched via the browser and their usage status.

- Data related to the language used in the browser.
- Data related to smartphone users' Browse history, download history, and bookmarks in the browser.
- Data related to smartphone users' installation and uninstallation of browser plugins and other usage status.
- Data related to display errors during web page operation, plugin crashes, and other status.

b. "Data related to the content and specifications of web pages"

- Data related to the content of web pages.
- Data related to the technical specifications when web pages use OS functions.
- Other data related to the technical specifications of web pages.

(E) "Already Publicly Available Data"

The use of "already publicly available data" by designated providers is excluded from the scope of Article 5 because the competitive prerequisites with other third-party app providers or website operators are the same. "Already publicly available" refers to data that can be acquired and viewed by anyone using readily available methods, such as data published on a web page, listed in an application store, described within the individual software itself, or accessible through information sources like market information services.

In this regard, even if data acquired by a designated provider is not already publicly available data, it is conceivable that the third-party app provider or website operator providing the source individual software or web page may consent to share and use such data for the purpose of developing goods or services in partnership. Article 5 does not prohibit such data sharing and use associated with business partnerships, but when such data sharing and use occur, it must be based on sufficient consultation with and agreement from the third-party app provider or website operator. It should be noted that if a designated provider of basic operation software or an application store engages in unfair treatment towards other third-party app providers, such as forcing data sharing, it may violate Article 6 of the Act.

B. When Acquired Data is Processed or Modified

Data acquired by designated providers as described in A (A) to (D) above, even if processed by combining it with other data or by statistical processing, is also subject to Article 5 of the Act.

Furthermore, if designated providers combine data acquired through the use of basic operation software or application stores by other third-party app providers for the provision of individual software, or data acquired through the display of web pages presented by other website operators using the browser, it does not prevent the application of Article 5 of the Act.

C. "Using for the Provision of Goods or Services that are in a Competitive Relationship with Goods or Services Provided by the Other Third-Party App Provider (or Website Operator), or Causing its Subsidiaries to Use Such Data" (Common to Article 5, Items 1 to 3)

(A) "Goods or services in a competitive relationship" refers to goods or services of the same type from the perspective of smartphone users, including not only individual software or websites (e.g., individual software for video viewing or websites providing video streaming services) but also goods or services offered in practical conjunction with individual software (e.g., tag devices to prevent lost items or cloud storage services).

On the other hand, in general, using data acquired through basic operation software, application stores, or browsers for the purpose of improving the functions of each specified software is not hindering from the perspective of promoting innovation. Such data usage is, as a general rule, not considered to be "used for providing goods or services in a competitive relationship." However, if a designated provider incorporates functions provided by other third-party app providers as individual software into a part of its basic operation software (e.g., incorporating battery capacity management functions into the basic operation software when other third-party app providers provide individual software for battery capacity management), then the functions of the basic operation software can also be said to be in a competitive relationship with that individual software.

Furthermore, "in a competitive relationship" includes hypothetical competitive relationships. For example, even if a designated provider of basic operation software or an application store uses data acquired during the pre-review of individual software that other third-party app providers are about to launch, it cannot be said that there is no competitive relationship simply because the individual software has not yet been launched.

(B) Whether data has been "used for providing goods or services in a competitive relationship" is determined holistically based on factors such as the similarity and relevance of competing goods or services, the timing of development or update of designated providers' first party

goods and services, and the data required for such development or update. Hypothetical scenarios where acquired data is deemed to be "used for providing goods or services in a competitive relationship" and thus constitute a violation of Article 5 include the following actions:

Hypothetical Scenarios: (In the hypothetical scenarios, "individual software" may also be referred to as "app." The same applies hereinafter.)

- **Hypothetical Scenario 1:** A designated provider of basic operation software uses data related to the usage status of an Alpha app (individual software for operating smartphone peripherals) developed by another third-party app provider and provided on smartphones running its basic operation software, to develop and launch a peripheral device with similar functions to that peripheral device.
- **Hypothetical Scenario 2:** An application store designated provider uses smartphone user purchase history data acquired by the application store in connection with charges made through the payment management service provided by that designated provider within individual software (Beta app) developed by another third-party app provider, and from the perspective of promoting the sale of in-app items in a similar individual software (Gamma app) provided by the designated provider, intensively conducts advertising activities targeting smartphone users who frequently purchase in-app items in the Beta app.

(C) Regarding "usage." Usage can occur in various forms. The determination of whether data has been "used for providing goods or services in a competitive relationship" is made by considering its relevance to the purpose ("for providing goods or services in a competitive relationship") and the manner of data "usage". For example, if it is determined that data processing has been carried out in a way that can only be used for providing goods or services in a competitive relationship, it is strongly presumed that the data has been "used for providing goods or services in a competitive relationship."

On the other hand, if a designated provider with internal regulations regarding data usage ensures that data that could be used for providing goods or services in a competitive relationship is not shared from the data management department to the development department for such goods or services due to the functioning of those internal regulations, then it is considered that the internal regulations have functioned appropriately to prevent actions that violate Article 5 of the Act.

(3) Desirable Practices by Designated Providers to Avoid Violations

Since it is difficult to externally verify whether data subject to the prohibitions in Article 5 has been used, it is important that designated providers establish effective internal systems to ensure compliance. Also, given that data utilization itself generally promotes innovation, effective internal systems through organizational development by designated providers are crucial to prevent violations of Article 5.

Therefore, designated providers are encouraged to create transparent decision-making processes and data management frameworks to prevent the use of data for goods and services in competitive relationships. When such internal systems are developed, it is expected that, within a scope that does not hinder the business activities of designated providers and related businesses, disclosure under Article 10 of the Act will be required, and it is anticipated that this disclosure will allow verification that the regulations are being complied with.

(4) Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

The matters to be included in the compliance reports submitted by designated providers under Article 14 of the Act and their accompanying documents are common with the reporting matters related to Article 10 of the Act. Therefore, reports on compliance with Article 5 and Article 10 are required to be submitted together (see 6 (3) below).

2. Article 6: Prohibition of Unjust Discrimination or Otherwise Unfair Treatment of Individual App Providers

(1) Basic Approach

Article 6 of this Act prohibits designated providers designated for their basic operation software or application stores from engaging in unfair or unjustly discriminatory treatment towards third-party app providers regarding the conditions for using such basic operation software or application stores by third-party app providers and the execution of transactions based on those conditions. This provision regulates various forms of unfair treatment toward individual app providers. A typical example of when Article 6 is applicable is when a designated provider conducts reviews or examinations (their framework to confirm whether certain

individual software meets the conditions for using the basic operation software or application store, including automated and manual processes) concerning individual software (including cases where a designated provider of basic operation software conducts reviews or examinations for individual software that uses alternative application stores; see (2) A below for details).

(2) Application of Article 6

A. Reviews and Examinations of Individual Software by Designated Providers

As mentioned in (1), Article 6 typically regulates the review items and their operation in reviews or examinations conducted by designated providers for individual software. This includes reviews or examinations conducted by a designated provider of an application store for individual software that uses that application store, as well as reviews or examinations conducted by a designated provider of basic operation software for individual software that uses an alternative application store on that basic operation software. The act of conducting such reviews or examinations does not, in itself, violate Article 6. However, if the criteria used for such reviews or the way they are implemented involve "unjust discrimination or otherwise unfair treatment," it would constitute a violation of Article 6.

Conducting reviews or examinations based on the following criteria generally does not violate Article 6. However, this principle does not apply if the implementation of such reviews is discriminatory without reasonable grounds, or if the reviews are conducted in ways inconsistent with the established criteria:

Ensuring cybersecurity, etc. (see 3 (1) D (A) below for details); maintaining public order and morals (e.g., preventing defamatory or discriminatory content such as hate speech, content promoting violence, pornographic content, false or inaccurate information, etc.); and preventing so-called 'dark patterns' (deceptive or manipulative user interfaces) (Note 2).

Furthermore, designated providers may set review items from the perspective of ensuring a certain level of consistency for individual software that uses their basic operation software or application store. Such review items for consistency are not unlimited in their acceptance under Article 6; their permissibility will be examined in light of the Act's purpose of promoting competition among basic operation software or application stores, including quality improvement. (For example, conducting reviews based on items that limit widgets and notifications to content and functions relevant to the individual software, or items that require

methods for contacting third-party app providers to be clearly stated within the individual software, generally do not violate Article 6.) Even if the review items themselves do not violate Article 6, if the criteria for judgment lack reasonableness, or if the operation of the reviews based on those items is discriminatory without reasonable grounds or inconsistent with the established criteria, it will constitute a violation of Article 6 (Note 3).

(Note 1) The "Smartphone Privacy and Security Initiative" (published on November 29, 2024, hereinafter referred to as "SPSI") by the "Study Group on the Improvement of the Usage Environment for ICT Services," an expert committee held by the Ministry of Internal Affairs and Communications, incorporates the spirit of relevant domestic laws and regulations, and also considers trends in foreign systems and initiatives by businesses. It specifies desirable measures for relevant businesses related to smartphone applications from the perspective of ensuring smartphone user privacy and security. The SPSI summarizes desirable practices for third-party app providers in providing individual software from the perspective of ensuring cybersecurity for smartphone use and protecting information related to smartphone users. It can serve as a reference for examples of individual software review items that are generally not problematic from the perspective of Article 6 when designated providers conduct reviews or examinations of individual software.

(Note 2) In the SPSI, "dark patterns" are defined as "designing, configuring, and operating user interfaces in a way that deceives or manipulates service users, or substantially distorts or impairs their ability to make free and informed decisions."

(Note 3) Regarding the application of Article 6, the Japan Fair Trade Commission, when deemed necessary, will make determinations while giving full consideration to the opinions of relevant government ministries and agencies with specialized knowledge (see 5.2 (2) below for the approach to cooperation with relevant government ministries and agencies).

B. Relationship with Other Provisions (Addressing Circumvention)

As mentioned in (1), Article 6 regulates unfair treatment towards third-party app providers. Actions that fall under the prohibited conduct of Article 7 or Article 8 and violate those provisions may also overlap with and violate Article 6. In such cases, as a general rule, Article 7 or Article 8 will be preferentially applied.

On the other hand, if an action does not formally meet the requirements for prohibited conduct under Article 7 or Article 8, but can be considered an act circumventing the intent of other provisions of the Act, and falls under the prohibited conduct of Article 6, then Article 6 will be

applied. However, even if an action falls under the prohibited conduct of each item of Article 7 or Article 8, Item 1 to 3 (excluding cases where the specified software under Article 8, Item 3 is a browser), it will not constitute a violation of Article 6 if it falls under the proviso of Article 7 or Article 8, respectively, meaning a justifiable reason is recognized.

It should be noted that the mere act of a designated provider conducting reviews or examinations of individual software does not immediately fall under the prohibited conduct of Article 7 and Article 8. Therefore, the reviews and examinations of individual software by designated providers will first be judged for their applicability to the prohibited conduct under Article 6. In this regard, if the results of reviews or examinations conducted by a designated provider are within the scope that does not violate Article 6, then even if the designated provider of basic operation software does not permit the provision of specific individual software on its basic operation software (e.g., if the provision of many specific individual software is not permitted due to reviews based on public order and morals as mentioned in A above), it cannot be said to hinder the provision of alternative application stores and therefore does not constitute a prohibited conduct under Article 7, Item 1.

(3) "Conditions for using the basic operation software or application store by third-party app providers and the execution of transactions based on those conditions"

"Conditions for using the basic operation software or application store by third-party app providers" broadly includes conditions for the use of basic operation software or application stores by third-party app providers. For example, conditions related to the display content and method presented to smartphone users when they use individual software, display design, and review items in the application store are applicable. For both basic operation software and application stores, the conditions set by designated providers for third-party app providers are diverse. Regardless of the method of setting these conditions (e.g., through basic operation software license agreements or application store product supply agreements), if a designated provider requires any conditions from third-party app providers, all such conditions are subject to Article 6 of the Act.

"Execution of transactions based on those conditions" means that Article 6 also covers not only the conditions for using basic operation software or application stores by third-party app providers themselves, but also the actual execution of transactions based on those conditions. That is, even if a designated provider providing basic operation software or an application store sets conditions for the use of such software or store, and those conditions themselves are not considered unfair treatment, any actions taken by the designated provider in the context of

enforcing those conditions are all subject to Article 6 of the Act.

(4) "Unjust Discriminatory Treatment"

"Unjust discriminatory treatment" refers to cases where a designated provider of basic operation software or an application store treats third-party app providers differently without reasonable grounds, either compared to the designated provider itself (its own goods or services) or where certain third-party app providers are treated differently from others. "Treatment" here refers to any action that affects the business activities of third-party app providers, regardless of the method, such as setting or changing conditions for using basic operation software or application stores, or operating those conditions.

Whether there is a reasonable grounds for such treatment by a designated provider is determined comprehensively by considering factors such as the purpose of the treatment, its impact on smartphone users or the designated provider's specified software business, the availability and nature of alternative measures to achieve the same purpose, and the content and degree of disadvantages incurred by third-party app providers. It should be noted that if the purpose of such treatment, for example, is merely to pursue operational rationality in the designated provider's specified software business and results in cost reductions that are not returned to smartphone users or third-party app providers, it is generally determined that there are no reasonable grounds.

If a designated provider treats others differently from itself and such treatment lacks necessity or reasonableness, it will generally constitute "unjust discriminatory treatment" under Article 6.

A. Actions by Designated Providers Regarding Basic Operation Software

Hypothetical scenarios of actions by designated providers of basic operation software that constitute "unjust discriminatory treatment" include the following:

It should be noted that the following actions are listed as typical hypothetical scenarios that fall under Article 6, but depending on the nature of the action, some may also raise issues in relation to other provisions of the Act (the same applies to hypothetical scenarios in (4) and (5) below).

Hypothetical Scenarios:

- **Hypothetical Scenario 3:** When a designated provider of basic operation software conducts reviews or examinations of individual software that uses alternative application stores, it establishes additional review criteria only for specific third-party app providers. However, for example, establishing additional review criteria that require child-oriented individual software not to provide inappropriate content, or that require individual software to provide information to smartphone users to prevent dark patterns for in-app purchases, generally has reasonable grounds.
- **Hypothetical Scenario 4:** When a designated provider of basic operation software conducts reviews or examinations of individual software that uses alternative application stores, despite the absence of factors such as the provision of inappropriate content that fails to meet the established review criteria, it refuses to allow distribution through the alternative application store or its basic operation software, or prolongs the review process, etc., without causes beyond the designated provider's control (e.g., delays resulting from other third-party app providers), thus operating in a manner that disadvantages specific third-party app providers.
- **Hypothetical Scenario 5:** A designated provider of basic operation software, despite the absence of technical constraints, cybersecurity concerns, or other issues related to ensuring such functionalities, refuses to allow third-party app providers other than itself (including its subsidiaries) to use OS functions with equivalent performance that the designated provider itself uses.

B. Actions by Designated Providers Regarding Application Stores

Hypothetical scenarios of actions by designated providers of application stores that constitute "unjust discriminatory treatment" include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 6:** An application store designated provider, in the review process for using its application store, introduces additional review criteria for individual software that uses alternative application stores without particular circumstances justifying the need for such criteria.
- **Hypothetical Scenario 7:** An application store designated provider, in the review process for using its application store, despite the absence of factors such as the provision of inappropriate content that fails to meet the established review criteria, refuses to allow distribution on its application store, or prolongs the review process, etc., without causes beyond the designated provider's control (e.g., delays resulting from other businesses), thus operating in a manner that disadvantages third-party app providers other than

itself, or disadvantages specific third-party app providers.

- **Hypothetical Scenario 8:** An application store designated provider, in the review process for using its application store, regarding the act of using identifiers such as advertising IDs linked to smartphone users to identify those users for advertising businesses, despite the scope and nature of such acts by third-party app providers being similar and there being no difference in the risk from the perspective of protecting smartphone user information, makes it a condition for individual software provided by third-party app providers other than itself to display a negative pop-up message emphasizing such risks, while for individual software provided by itself, it displays a pop-up message emphasizing safety.
- **Hypothetical Scenario 9:** An application store designated provider, despite the absence of circumstances making implementation difficult, does not allow other third-party app providers to access application store functions (e.g., parental control features), or exclusively permits access to such functions for specific third-party app providers.
- **Hypothetical Scenario 10:** An application store designated provider, in the application rankings within its application store based on objective metrics such as download counts or review scores, displays its own individual software or specific third-party app providers' individual software at a higher position than the actual ranking, or in the search results within its application store, preferentially displays its own individual software or specific third-party app providers' individual software.
- **Hypothetical Scenario 11:** An application store designated provider, in the application rankings within its application store based on objective metrics such as download counts or review scores, does not display specific third-party app providers' individual software or displays it at a lower position than the actual ranking, or in the search results within its application store, does not display specific third-party app providers' individual software or displays it in an inferior position.

(5) "Otherwise Unfair Treatment"

"Otherwise unfair treatment" refers to actions that restrict the business activities of third-party app providers or cause them disadvantages without reasonable grounds. The method of determining whether reasonable grounds exist is consistent with the approach for assessing "unjust discriminatory treatment" as described in (4) above.

When actions restrict the business activities of third-party app providers or cause them disadvantages, and the necessity or reasonableness of such treatment is absent, it will generally constitute "otherwise unfair treatment" under Article 6.

A. Actions by Designated Providers Regarding Basic Operation Software

Hypothetical scenarios of actions by designated providers of basic operation software that constitute "otherwise unfair treatment" include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 12:** When a designated provider of basic operation software conducts reviews or examinations of individual software that uses alternative application stores, despite the absence of a need from the perspective of ensuring cybersecurity, etc. (see 3 (1) D (A) below for details), it refuses to allow provision through the alternative application store without providing clear reasons for the review results, or withholds the review results for an extended period without clear reasons, for any individual software.
- **Hypothetical Scenario 13:** When a designated provider of basic operation software permits third-party app providers to use OS functions, it unilaterally imposes conditions that cause disadvantages exceeding the reasonable scope, as determined by considering the benefits obtained by the third-party app providers from such use, or unilaterally imposes conditions requiring the mandatory purchase or use of other goods or services provided by the designated provider.
- **Hypothetical Scenario 14:** A designated provider of basic operation software stops the operation of individual software provided by a third-party app provider (e.g., individual software with ad-blocking functions) on its basic operation software, citing the reason that it affects the designated provider's other businesses (e.g., advertising business).
- **Hypothetical Scenario 15:** A designated provider of basic operation software sets conditions that restrict third-party app providers who provide individual software on its basic operation software from filing lawsuits or making reports to courts or other public institutions regarding actions of the designated provider that they suspect violate the Act.

B. Actions by Designated Providers Regarding Application Stores

Hypothetical scenarios of actions by designated providers of application stores that constitute "otherwise unfair treatment" include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 16:** An application store designated provider suspends the account of a third-party app provider or halts the distribution of their individual software

through the designated provider's application store, despite the absence of circumstances such as violations of the application store's terms of use or factors beyond the designated provider's control (e.g., delays caused by other businesses).

- **Hypothetical Scenario 17:** An application store designated provider, regarding in-app purchases of individual software provided through its application store, imposes so-called "parity obligations" concerning pricing, such as requiring that the sales price in its application store not be higher than the sales price in an alternative application store or on a website, or that the sales price in its application store not be higher than the sales price in its application store provided on devices other than those equipped with the designated provider's basic operation software (e.g., PCs or tablets).
- **Hypothetical Scenario 18:** An application store designated provider, in the search results within its application store for a specific individual software when a smartphone user enters its name, consistently displays its own individual software or an advertisement for its own individual software that is in a competitive relationship with that specific individual software, immediately adjacent to it.
- **Hypothetical Scenario 19:** An application store designated provider, when determining whether to approve refund requests from users of individual software provided through its application store, routinely accepts these requests without implementing appropriate processes to verify the validity of each refund request (including automated verification systems), creating a situation where third-party app providers are forced to handle fraudulent refund requests.
- **Hypothetical Scenario 20:** An application store designated provider, regarding in-app purchases of individual software in the review process for using its application store, requires pricing to be based on a widely tiered price list, making it difficult for third-party app providers to set flexible prices, despite there being no restrictions that make flexible pricing difficult for third-party app providers.
- **Hypothetical Scenario 21:** An application store designated provider imposes conditions on third-party app providers who seek to provide individual software that affects the designated provider's other businesses (e.g., individual software with ad-blocking functions) within its application store, such as suspending the third-party app provider's account or halting the provision of that individual software in the application store, unless the third-party app provider stops providing that individual software.
- **Hypothetical Scenario 22:** An application store designated provider sets conditions that restrict third-party app providers who provide individual software in its application store from filing lawsuits or making reports to courts or other public institutions regarding actions of the designated provider that they suspect violate the Act.

(6) Desirable Practices by Designated Providers to Avoid Violations

To prevent violations of Article 6, it is desirable for designated providers of basic operation software or application stores to implement the following practices:

- **Practices Related to Establishing Necessary Systems and Procedures to Ensure "Unjust Discriminatory Treatment or Otherwise Unfair Treatment" Does Not Occur**
  Designated providers are encouraged to establish necessary systems and procedures to ensure that "unjust discriminatory treatment or otherwise unfair treatment" does not occur regarding the conditions for using their basic operation software or application store and the execution of transactions based on those conditions. If such systems and procedures are established, it is desirable to undertake the following practices regarding the conditions for using basic operation software or application stores and the execution of transactions based on those conditions:
  - Regularly confirm internally within the designated provider whether "unjust discriminatory treatment or otherwise unfair treatment" is occurring.
  - If treating all or part of third-party app providers differently from itself or other third-party app providers, explain the reasons for such treatment to the third-party app providers, providing supporting evidence.
  - Explain to third-party app providers, with objective evidence, that the designated provider is engaging in fair treatment.

(7) Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

Designated providers are required to report to the Japan Fair Trade Commission on the status of their compliance with Article 6, including the matters specified in Rules Article 36, Paragraph 2. Examples of other necessary information for confirming compliance as referred to in Item 4(c) of the same paragraph include the following:

A. Designated Provider of Basic Operation Software

- If the designated provider treats all or part of third-party app providers differently from itself or other third-party app providers regarding the conditions for using basic operation software by third-party app providers or the execution of transactions based on those conditions, the content of such treatment and the reasons for it.

B. Designated Provider of Application Store

- If the designated provider treats all or part of third-party app providers differently from

itself or other third-party app providers regarding the conditions for using the application store by third-party app providers or the execution of transactions based on those conditions, the content of such treatment and the reasons for it.

3. Article 7: Prohibited conduct by Designated Providers of Basic Operation Software

(1) Item 1 (Prohibition on Hindering the Provision of Alternative Application Stores)

A. Basic Approach

Article 7, Item 1 of this Act prohibits designated providers of basic operation software from limiting application stores provided through their basic operation software solely to those provided by the designated providers themselves or their subsidiaries (hereafter referred to as "designated providers, etc." in this section). It also prohibits actions that interfere with other businesses providing alternative application stores through the basic operation software or smartphone users utilizing alternative application stores via the basic operation software. By prohibiting such actions that hinder the provision of alternative application stores by designated providers of basic operation software, this Item aims to promote new entries into the alternative application store market and foster competition in application stores.

B. Specific Understanding of Article 7, Item 1

(A) Actions that "Limit" Application Stores to Those Provided by the Designated Provider

Article 7, Item 1(a) refers to actions where a designated provider of basic operation software limits application stores provided through its basic operation software to those provided by the designated provider itself or its subsidiaries. Such actions include prohibiting smartphone users from utilizing alternative application stores through licensing agreements or terms of use of the designated provider's basic operation software, or establishing technical specifications within the basic operation software that make it impossible to provide alternative application stores.

(B) Actions that "Prevent" the Provision or Use of Alternative Application Stores

Article 7, Item 1(b) refers to conduct that creates a high likelihood of making it difficult for other businesses to continue providing alternative application stores or to initiate new ones through the designated provider's basic operation software. It also refers to conduct that creates a high likelihood of making it difficult for smartphone users to continue utilizing alternative application stores or to begin utilizing new ones through the designated provider's

basic operation software. Such actions include, even while nominally permitting the provision or use of alternative application stores, imposing unreasonable technical constraints, contractual terms, or excessive financial burdens on other businesses, or steering smartphone users away from utilizing alternative application stores, thereby creating a high likelihood of making the provision or use of alternative application stores practically difficult.

For a designated provider's action to be considered as "preventing" the provision or use of alternative application stores, it is not necessary for the provision or use of alternative application stores to be completely impossible. The determination of whether an action falls under this category is made based on the degree of likelihood that such a result will occur.

The degree of "likelihood of difficulty (to provide services)" caused by such actions is assessed comprehensively based on factors such as the nature of the designated provider's actions, the duration of those actions, the extent of impact on businesses providing alternative application stores, and the degree of impact on third-party app providers attempting to offer individual software through alternative application stores.

(C) Understanding Regarding the Demand for Financial Burdens, Including Fees

Regarding the demand for financial burdens such as fees as described in C (B) below, for example, if a designated provider imposes financial burdens such as fees for the use of basic operation software on third-party app providers who provide or intend to provide individual software through an alternative application store, third-party app providers will consider not only the financial burdens such as fees paid for using the alternative application store but also these financial burdens required by the designated provider when deciding whether to use the alternative application store.

The level of financial burdens, such as fees, that are likely to make it difficult for third-party app providers to use alternative application stores is evaluated based on specific circumstances. Considerations include, for example, the financial burdens applied by designated providers to third-party app providers for using their application stores, financial burdens applied by businesses for offering alternative application stores (taking into account whether efficient businesses providing alternative application stores can sustain their operations), and the financial burdens applied by designated providers when using alternative application stores. These factors are evaluated to ensure competitive conditions between designated providers' application stores and alternative application stores.

C. Hypothetical Scenarios

(A) Hypothetical scenarios of actions where a designated provider limits application stores provided through its basic operation software to those provided by the designated provider, etc., and thus falls under Article 7, Item 1(a) of the Act, include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 23:** A designated provider prohibits smartphone users from utilizing alternative application stores through the licensing agreements or terms of use of its basic operation software.
- **Hypothetical Scenario 24:** A designated provider establishes technical specifications within its basic operation software that make it impossible for smartphone users to utilize alternative application stores (excluding specifications related to settings that allow smartphone users to choose to restrict the use of alternative application stores for a duration they prefer).

(B) Hypothetical scenarios of actions where a designated provider, while permitting the provision or use of alternative application stores in relation to its basic operation software, substantially creates a high likelihood of difficulty in their provision or use, and thus falls under Article 7, Item 1(b) of the Act, include the following:

a. A designated provider imposes unreasonable technical constraints, contractual terms, or other conditions regarding the provision or use of alternative application stores on other businesses that provide or intend to provide alternative application stores, or on third-party app providers that use or intend to use alternative application stores, in relation to its basic operation software.

Hypothetical Scenarios:

- **Hypothetical Scenario 25:** When setting requirements related to the business scale or financial status of other businesses as conditions for providing an alternative application store on the basic operation software, a designated provider, without reasonable grounds, sets a high standard such that the number of other businesses meeting the requirement is extremely limited.
- **Hypothetical Scenario 26:** When conducting reviews or examinations for other businesses providing an alternative application store on the basic operation software, a designated provider, without reasonable grounds, imposes additional review requirements exclusively on a specific alternative application store that are not applied to other alternative application stores, or, even if the review criteria are identical, conducts the review process in a way that disadvantages a specific alternative application store.

- **Hypothetical Scenario 27:** When conducting reviews or examinations for other businesses providing an alternative application store on the basic operation software, a designated provider, without causes beyond the designated provider's control (e.g., delays resulting from the other business), takes an excessively long time to complete the reviews or examinations for an alternative application store.
- **Hypothetical Scenario 28:** A designated provider, without reasonable grounds, disadvantages the majority or all third-party app providers who provide or intend to provide individual software through alternative application stores, for example, by delaying the completion of reviews or examinations when third-party app providers use the designated provider's application store to provide individual software, thereby steering third-party app providers towards abandoning the provision of individual software in alternative application stores.
- **Hypothetical Scenario 29:** A designated provider enters into a contract with a third-party app provider that provides influential individual software (e.g., popular game apps for smartphones) that operates on the basic operation software, where the designated provider pays financial compensation or other consideration to the third-party app provider in exchange for the third-party app provider not launching its own alternative application store to provide its individual software or not taking steps to provide it through an alternative application store.

b. A designated provider imposes excessive financial burdens regarding the provision or use of alternative application stores on other businesses that provide or intend to provide alternative application stores, or on third-party app providers that use or intend to use alternative application stores, in relation to its basic operation software.

It should be noted that the imposition of financial burdens such as fees on third-party app providers who use or intend to use alternative application stores will be judged based on the understanding described in B (C) above.

Hypothetical Scenarios:

- **Hypothetical Scenario 30:** A designated provider imposes financial burdens, such as usage fees, on other businesses that provide or intend to provide alternative application stores on the basic operation software, to such an extent that there is a high likelihood of making the provision of alternative application stores difficult, for example, by expanding the criteria for calculating the usage fees for basic operation software imposed on individual software.
- **Hypothetical Scenario 31:** In a situation where a third-party app provider adopts a

method of earning revenue from advertisements displayed in individual software provided by itself, and is not required to pay financial burdens to the designated provider, etc., when providing specific individual software only through the designated provider, etc.'s application store, the designated provider imposes financial burdens, such as usage fees, on that third-party app provider that create a high likelihood of making the use of alternative application stores difficult, when the third-party app provider attempts to provide that specific individual software in an alternative application store.

c. A designated provider steers smartphone users away from utilizing alternative application stores when they use or intend to use alternative application stores, in relation to its basic operation software.

Hypothetical Scenarios:

- **Hypothetical Scenario 32:** A designated provider implements technical specifications in its basic operation software that make it difficult for smartphone users to utilize alternative application stores, such as unnecessarily complicating the setup process for downloading and installing alternative application stores.
- **Hypothetical Scenario 33:** When a smartphone user attempts to use an alternative application store, the designated provider displays a pop-up promoting the convenience of the designated provider, etc.'s application store, thereby steering users toward its own application store.
- **Hypothetical Scenario 34:** Between the installation of an alternative application store and the installation of individual software via the alternative application store, the designated provider engages in actions or places displays that induce users to abandon installation (e.g., presenting warnings that convey an exaggerated sense of risk associated with the installation, repeatedly showing screens requesting permissions for necessary access rights without reasonable grounds, or requiring users to change settings each time an installation is performed).

D. Understanding Justifiable Reasons

(A) General Principles

For Article 7 and Article 8, Items 1 to 3 of this Act (excluding cases where the specified software under Article 8, Item 3 is a browser), actions deemed necessary for ensuring cybersecurity for smartphone use, protecting information related to smartphone users, safeguarding youth who use smartphones, or achieving other objectives stipulated by the

Cabinet Order (prevention of gambling and other criminal activities conducted using smartphones, and prevention of significant delays, freezes, or other abnormal operations of smartphones, as defined in Article 2 of the Cabinet Order for the Mobile Software Competition Act (Cabinet Order No. 376 of 2024, hereinafter referred to as "the Order")) (collectively defined as "Ensuring Cybersecurity, etc.") may qualify as "justifiable reasons" for noncompliance if these objectives are difficult to achieve through other less competition-restricting actions. Even if a designated provider's action appears to fall under Article 7 or Article 8, Items 1 to 3 of this Act, it will not constitute a violation of Articles 7 and 8 as long as there is an accepted justifiable reason.

(B) Specific Examples of Justifiable Reasons

Specific examples of the objectives for justifiable reasons listed in (A) above are as follows. These examples are illustrative only, and whether a justifiable reason is recognized requires individual, case-by-case examination.

a. **Ensuring cybersecurity for smartphone use** refers to ensuring cybersecurity in smartphones as defined in Article 2 of the Cybersecurity Basic Act (Act No. 104 of 2014) (Note 1).

Specifically, this includes:

- Measures to prevent OS functions from being used in a way that harms the smartphone or smartphone user due to unauthorized access by third parties to OS functions.
- Measures to prevent data stored on smartphone devices (e.g., confidential business documents, location history on business smartphones) from being leaked, lost, or damaged due to unauthorized access by third parties.
- Measures to prevent smartphone operation from stopping or smartphone performance from significantly deteriorating due to excessive load on smartphone functions through the use of OS functions (including cases where unauthorized use of Wi-Fi or other networks by third parties results in the cessation or significant deterioration of network functions).
- Measures to prevent data stored on the smartphone device (e.g., photo data, contact data) from being leaked, lost, or damaged due to defects (e.g., those caused by programming bugs) in individual software that accesses OS functions on the smartphone.
- Measures to prevent alternative application stores that do not implement measures against malicious software (malware, ransomware, etc.) from being provided on the basic operation software of a designated provider of basic operation software.

- Measures to prevent individual software (excluding browsers) that incorporates browser engines without vulnerability countermeasures from being provided in the application stores of designated providers, etc., of basic operation software.

(Note 1) Article 2 defines "cybersecurity" as "measures necessary for the safe management of information, such as preventing the leakage, loss, or damage of information recorded, transmitted, or received by electronic, magnetic, or other intangible means (hereinafter referred to as 'electromagnetic means' in this Article), as well as measures necessary for ensuring the safety and reliability of information systems and information communication networks (including measures necessary to prevent damage from unauthorized activities against electronic computers through information communication networks or recording media created by electromagnetic means (hereinafter referred to as 'electromagnetic recording media')), and that such state is appropriately maintained and managed."

(Note 2) From the perspective of national security and economic security, it is also important to take sufficient measures to prevent actions such as the leakage of data stored on smartphone devices via smartphones. Such measures to ensure cybersecurity for smartphone use or protection of information related to smartphone users generally constitute a justifiable reason under the Act.

b. **Protecting information related to smartphone users** refers to protecting information related to smartphone users, such as information stored on the smartphone device or information generated in connection with the use of the smartphone.

Specifically, this includes responses required by existing laws, such as the Act on the Protection of Personal Information (Act No. 57 of 2003) and the Telecommunications Business Act (Act No. 86 of 1984) concerning user information, as well as responses to protect information related to smartphone users in line with the spirit of existing laws.

Examples of such responses required by existing laws or in line with the spirit of existing laws to protect information related to smartphone users include:

- Measures to require alternative application stores to implement measures to prevent the acquisition of information related to smartphone users (e.g., advertising IDs, device IDs, third-party cookies) for the purpose of advertising delivery and display without the user's consent.
- Making consent from the smartphone user a condition for using OS functions that

acquire information related to smartphone users (e.g., voice data recorded by microphone, location information, photo data, video data) through the smartphone's OS functions.

- Measures to prevent alternative application stores that provide individual software (presumably not provided in the designated provider, etc.'s application store) that acquires information related to smartphone users through misleading user interfaces from being provided on the basic operation software.
- Measures to require alternative application stores to describe in their privacy policy the purpose of use, items of information to be provided, and the name of the country where the third party, consignee, or joint user is located when providing information related to smartphone users to a third party, consignee, or joint user located abroad, in relation to the alternative application store and individual software provided by it.
- Measures to prevent third-party app providers providing individual software with in-app purchase items from acquiring information related to smartphone users through misleading interfaces.

c. **Safeguarding youth who use smartphones** refers to preventing minors from becoming involved in trouble or problems when using smartphones.

Specifically, this includes:

- Regarding in-app purchases in individual software, measures to establish parental control functions in the basic operation software to prevent excessive or erroneous charges by minors, and to restrict the use of all payment systems (including alternative payment systems) by minors based on parental consent.
- Regarding alternative application stores that provide individual software containing harmful content for minors, measures to establish parental control functions in the basic operation software to prevent minors from using such alternative application stores, and to restrict their use by minors based on parental consent.
- Measures to require alternative application stores to implement appropriate age restrictions (ratings) for individual software or content/functions provided through individual software, and to restrict the use of such functions, from the perspective of appropriate use by minors.
- Measures to require alternative application stores to set stricter privacy protection standards for information related to minor smartphone users than for non-minors (e.g., not displaying targeted advertisements based on profiling of information related to minor smartphone users).

d. **Prevention of criminal activities conducted using smartphones** refers to preventing various criminal activities carried out using smartphones.

Specifically, this includes:

- Measures to require alternative application stores to restrict the display of deceptive advertisements and contract methods regarding the terms of service for goods or services sold through individual software, to prevent misleading smartphone users.
- Measures to require alternative application stores to display the duration, number of uses, fees, and cancellation/refund policies in the final confirmation screen when subscribing to a subscription service in individual software.
- Measures to require alternative application stores to prevent the provision or promotion of individual software related to goods or services that are legally prohibited from being provided to users in Japan or that require licenses, etc., but are provided without obtaining such licenses, etc..
- Measures to prevent alternative application stores that provide individual software (presumably not provided in the designated provider, etc.'s application store) with a high probability of being used for criminal activities from being provided on the designated provider's basic operation software.
- Measures to prevent alternative application stores that provide individual software (presumably not provided in the designated provider, etc.'s application store) with so-called "pirated content" from being provided on the designated provider's basic operation software.
- Measures to impose reasonable and necessary conditions on the provision of link-outs, including requirements for providing link-outs in individual software and requirements for link-out landing pages, etc., to minimize the risk of smartphone users being redirected to misleading or deceptive websites through fraud.

e. **Prevention of abnormal operation of smartphones** refers to preventing abnormal operation from occurring from the perspective of ensuring the physical safety of smartphone hardware during smartphone use.

Specifically, this includes:

- Measures to prevent the smartphone's battery from catching fire due to excessive load on the battery caused by the operation of individual software.
- Measures to prevent the smartphone's hardware from malfunctioning due to excessive load on the smartphone's semiconductor (e.g., modem chip for communication) caused

by the operation of individual software.

- Measures to prevent the smartphone from ceasing to function due to excessive load on the smartphone's battery, central processing unit (CPU), or graphics processing unit (GPU) caused by the operation of individual software.
- Measures to prevent the smartphone's performance from significantly deteriorating due to excessive load on the smartphone's battery or semiconductor (e.g., modem chip for communication) caused by the operation of individual software.

(C) Basic Approach Regarding Applicability of Justifiable Reasons

Even if actions fall under Article 7 and Article 8, Items 1 to 3 of this Act, they will not violate Article 7 and Article 8 if they are deemed necessary for ensuring cybersecurity, etc., and if it is difficult to achieve that purpose through other actions. That is, if a designated provider carries out actions that fall under Article 7 and Article 8, Items 1 to 3 of this Act for the purpose of ensuring cybersecurity, etc., and if those actions are objectively evaluated as being carried out for that purpose, and if it is difficult to achieve that purpose through other less competition-restricting actions, then those actions will not violate Article 7 and Article 8 of the Act. The determination of whether it is "difficult to achieve that purpose through other actions" is made by comparing it with actually feasible alternative means, taking into account factors such as the designated provider's costs.

To ensure that smartphone users can safely utilize diverse alternative application stores and individual software distributed through them, it is necessary to accurately determine whether such justifiable reasons are truly recognized for the actions of designated providers. If a justifiable reason is not recognized when it should be, and cybersecurity, etc., is not ensured, it would go against the intent of establishing justifiable reasons in Article 7 and Article 8. Conversely, if a justifiable reason is recognized when it should not be, the prohibited conduct stipulated in Article 7 and Article 8 would be rendered meaningless, deviating from the intent of establishing those prohibited conduct. Therefore, it is important to make judgments regarding justifiable reasons while considering the balance between the two imperatives of ensuring cybersecurity, etc., and promoting competition.

The determination of whether a designated provider's action falls under a justifiable reason will be made on a case-by-case basis. However, from the perspective of ensuring predictability for designated providers, businesses providing or intending to provide alternative application stores, third-party app providers, and other businesses, hypothetical scenarios where justifiable reasons are considered acceptable and not in violation, and hypothetical scenarios

where justifiable reasons are not considered acceptable and constitute violations, are described below for each item of Article 7 and Article 8, Items 1 to 3. These hypothetical scenarios are merely illustrative examples, and whether a justifiable reason is recognized will be determined based on individual case-specific circumstances.

In particular, for measures to prevent criminal activities conducted using smartphones, it is appropriate to consider the severity of such activities and the magnitude of the risks when determining the extent of the measures. The determination of whether it is difficult to achieve the purpose of preventing criminal activities conducted using smartphones through less competition-restricting actions other than those of the designated provider will be made on a case-by-case basis for each specific instance.

It is important for the Japan Fair Trade Commission to make judgments while giving full consideration to the opinions of relevant government ministries and agencies with specialized knowledge regarding whether an action is deemed necessary for ensuring cybersecurity, etc., and whether it is difficult to achieve that purpose through other actions. The approach to cooperation with relevant government ministries and agencies is detailed in Section 5 below.

E. Hypothetical Scenarios of Justifiable Reasons

Based on the basic understanding of the applicability of justifiable reasons in D above, hypothetical scenarios where justifiable reasons are typically recognized and do not constitute violations, and hypothetical scenarios where justifiable reasons are typically not recognized and constitute violations, are as follows:

(A) Hypothetical Scenarios Where Justifiable Reasons are Accepted and Not Considered Violations

Hypothetical scenarios of actions that are typically recognized as having justifiable reasons and are not considered violations of Article 7 include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 35:** When a designated provider conducts reviews or examinations based on necessary standards for ensuring cybersecurity, etc., regarding alternative application stores used with the basic operation software under its designation, and finds that the alternative application store does not meet such standards, the designated provider may prohibit the provision of such alternative application store on its basic operation software. This action, while hindering the provision of alternative

application stores by other businesses by preventing their provision on the basic operation software if they do not meet the review criteria set by the designated provider, contributes to ensuring cybersecurity, etc. Furthermore, if the review criteria (Note) and their application are limited to the necessary scope in light of their purpose, a justifiable reason is recognized, and it does not violate Article 7 of the Act.

(Note) The SPSI (Smartphone Privacy and Security Initiative) states that desirable practices from the perspective of ensuring security for application store providers include "showing security requirements that apps provided in the app store should meet and reviewing whether those requirements are met (e.g., use of industry-standard encryption technology, least privilege, secure coding, etc.)" and desirable practices from the perspective of appropriate handling of user information include "providing a display location for privacy policies and an overview of acquired information on individual application pages within the app store, and supporting application providers, etc., in taking appropriate measures such as indicating items to be displayed and standard icons." The content of the SPSI shall be a reference.

- **Hypothetical Scenario 36:** From the perspective of safeguarding youth who use smartphones—such as preventing the use of age-restricted individual software, unintended excessive charges, or erroneous charges—designated providers may enable settings (commonly referred to as parental control functions) to restrict the use of alternative application stores by minor smartphone users based on parental consent. This action, while restricting the use of alternative application stores and potentially hindering smartphone users' access to them, contributes to safeguarding youth who use smartphones. Furthermore, if alternative application stores do not provide parental control functions equivalent to those of the designated provider, etc.'s application store, it is considered that there are no other less competition-restricting means to achieve this purpose. Therefore, a justifiable reason is recognized, and it does not violate Article 7 of the Act.
- **Hypothetical Scenario 37:** A designated provider causes an alternative application store to change its name, logo, user interface, etc., if there is a risk that it infringes intellectual property rights by closely resembling another application store's name, logo, user interface, etc., from the perspective of preventing criminal activities conducted using smartphones. This action, while potentially hindering the provision of alternative application stores by other businesses, contributes to the prevention of criminal activities conducted using smartphones and seeks to prevent actions prohibited by law. As there are no other less competition-restricting means to achieve this purpose, a

justifiable reason is recognized, and it does not violate Article 7 of the Act.

- **Hypothetical Scenario 38:** A designated provider disables the use of an alternative application store on its basic operation software due to a high risk that the protection of information related to smartphone users, etc., cannot be ensured by that alternative application store. This situation arises, for example, when the Japanese government requests the designated provider to take measures to prevent the provision of such an alternative application store in Japan, based on the high risk that information related to smartphone users collected by an alternative application store operated by a party obligated to cooperate with information collection activities by a foreign government, etc., under a contract with a foreign government, etc., or under foreign laws, etc. (where the collection of information that poses a high risk of harming national security is not excluded from the scope of collection by that foreign government, etc.), may harm national security. This action, while making the use of alternative application stores impossible and thus hindering their use, contributes to the protection of smartphone user information, etc. If there are no other less competition-restricting means to achieve this purpose, a justifiable reason is recognized, and it does not violate Article 7 of the Act.

(B) Hypothetical Scenarios Where Justifiable Reasons Are Not Accepted and Constitute Violations

Hypothetical scenarios of actions that are typically not recognized as having justifiable reasons and are considered violations of Article 7 include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 39:** When smartphone users attempt to download and install alternative application stores, designated providers, without conducting any reviews or examinations for any alternative application store, uniformly issue warning messages to smartphone users attempting to download and install alternative application stores, suggesting that such stores are unsafe from the perspective of ensuring cybersecurity or protecting user information, and encouraging users to refrain from using them. This action, despite having the legitimate purpose of ensuring cybersecurity for smartphone use or protecting information related to smartphone users, does not qualify as having a justifiable reason because that purpose can be achieved by conducting necessary reviews or examinations from the perspective of ensuring cybersecurity or protecting information related to smartphone users and preventing the provision of alternative application stores that are unsafe for smartphone users, meaning there are other less

competition-restricting means to achieve that purpose. Therefore, it violates Article 7 of the Act.

- **Hypothetical Scenario 40:** When smartphone users attempt to download and install individual software through an already installed alternative application store, designated providers, citing the necessity for ensuring cybersecurity or protecting user information, require smartphone users to make complex configuration modifications each time they attempt to download and install individual software through an already installed alternative application store. This action, despite having the legitimate purpose of ensuring cybersecurity for smartphone use or protecting information related to smartphone users, does not qualify as having a justifiable reason because that purpose can be achieved without requiring complex configuration modifications each time the user attempts to download and install individual software from an alternative application store they have already installed and started using. Instead, a pop-up can be displayed at the initial download and installation of the alternative application store, allowing the user to make the necessary configuration changes to use the alternative application store and download and install individual software, and those settings can remain active as long as the user does not choose to stop using the alternative application store, meaning there are other less competition-restricting means to achieve that purpose. Therefore, it violates Article 7 of the Act.

F. Desirable Practices by Designated Providers to Avoid Violations

To prevent actions that fall under Article 7, Item 1 and violate Article 7 of the Act, it is desirable for designated providers of basic operation software to undertake the following practices:

- If a designated provider imposes financial burdens, such as fees, on alternative application stores and individual software provided by such alternative application stores within the basic operation software, the designated provider notifies the amount of such financial burdens by means such as posting it on the designated provider's website. Additionally, the designated provider explains to providers of alternative application stores or third-party app providers how the level of financial burden imposed by the designated operator is reasonable in relation to the benefits derived by the providers of alternative app stores or third-party app providers from the basic operation software.

G. Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

Designated providers of basic operation software are required to report to the Japan Fair

Trade Commission on the status of their compliance with Article 7, Item 1, including the matters stipulated in Rules Article 36, Paragraph 2. Examples of other necessary information for confirming compliance with the Act under Item 4(c) of the same paragraph include the following:

1. The number and names of alternative application stores provided by other businesses through the designated provider's basic operation software.
2. If the designated provider establishes certain criteria and conducts reviews or examinations as conditions for other businesses to provide alternative application stores, the criteria for such reviews or examinations, the procedures for conducting them, and the name and content of any related terms and conditions.
3. If the designated provider imposes financial burdens such as fees on other businesses as conditions for them to provide alternative application stores, the calculation method of such financial burdens and the reasons for imposing them, and the name and content of any related terms and conditions.
4. If the designated provider imposes financial burdens such as fees on third-party app providers as conditions for them to provide individual software through alternative application stores, the calculation method of such financial burdens and the reasons for imposing them, and the name and content of any related terms and conditions.

(2) Item 2 (Prohibition of Hindering the Use of OS Functions)

A. Basic Approach

Article 7, Item 2 of this Act prohibits designated providers of basic operation software from preventing other businesses (businesses other than designated providers, etc.) from using OS functions with equivalent performance for the provision of individual software, when such OS functions are used by the designated provider, etc., to provide individual software. By prohibiting actions that prevent other businesses from using OS functions with equivalent performance as utilized by designated providers, etc., for the provision of individual software, this Item aims to promote competition regarding individual software.

B. Specific Understanding of Article 7, Item 2

(A) Functions Subject to the Provision

The functions subject to Article 7, Item 2 are OS functions that designated providers, etc., use to provide individual software.

a. OS Functions

OS functions include various functions related to smartphone operation controlled by the designated provider's basic operation software, such as audio functions like speakers and microphones, data communication functions, biometric authentication functions for smartphone users, location measurement functions, text input functions, functions to launch individual software, and pairing functions between smartphones and external connected devices. Basic operation software is defined as software (Article 2, Paragraph 2 of the Act) incorporated into a smartphone and configured to perform information processing primarily for controlling operations of the smartphone's central processing unit (CPU) and other smartphone operations. Since various smartphone operations are controlled by basic operation software, OS functions broadly encompass functions related to smartphone operation. It should be noted that basic operation software includes all software that falls under the definition of Article 2, Paragraph 2 of the Act, regardless of whether it constitutes a core part including what is generally called a kernel. For example, components other than the kernel and software positioned between the core part and individual software (generally called middleware) may also be included.

b. "Functions Used by the Designated Provider to Provide Individual Software"

The phrase "functions used by the designated provider to provide individual software" means to limit the functions subject to Article 7, Item 2 to OS functions that designated providers, etc., use to provide individual software in Japan (hereinafter referred to as "these OS functions"). Therefore, even if they are OS functions, those that designated providers, etc., do not use to provide individual software in Japan are not subject to this provision.

"Functions used by the designated provider, etc., to provide individual software" includes not only OS functions that designated providers, etc., currently use to provide individual software in the market, but also OS functions whose specifications have been concretized to a degree that allows other business operators to develop or improve individual software using them—such as beta versions made available for testing with public disclosure—as long as they are targeted for development or improvement by designated providers, etc., for the provision of individual software within Japan.

Furthermore, the ways in which designated providers, etc., "use OS functions for the provision of individual software" include the following:

(a) When OS functions are used for individual software itself provided by designated providers, etc.

For example, audio output functions are used for individual software providing music services (including music services provided through such individual software) itself. Also, for example,

location measurement functions are used for individual software providing maps (including navigation services provided through such individual software) itself.
(b) When OS functions are used for goods or services that are functionally integrated with individual software provided by designated providers, etc.
In this case, OS functions serve both the provision of the goods or services and the provision of the individual software itself. For example, a companion app used for operating smartphone peripherals such as smartwatches from the smartphone side is functionally integrated with the peripheral device. Therefore, the pairing function that connects the peripheral device and the smartphone is utilized for the provision of the companion app itself, as well as for the provision of the peripheral device.

(B) "Other Business Operators Using the Equivalent Performance to Provide Individual Software"

The intent of Item 2 is to ensure that OS functions are accessible to other businesses in a manner that does not significantly disadvantage their performance compared to designated providers, etc.'s use of the same functions for individual software provision, rather than merely allowing other businesses to use these OS functions for individual software provision. For example, if these OS functions are data transmission functions, their performance includes the maximum data volume that can be transmitted and the types of data. Other businesses must be able to use these OS functions with a maximum data volume and types of data that are not significantly inferior to those when designated providers, etc., use these functions.

Furthermore, it is sufficient if the OS functions enable other businesses to use them at a comparable level for individual software provision, so it does not necessarily require identical methods of access or use between designated providers, etc., and other businesses. For example, if there are multiple technical methods for using a particular OS function (e.g., in addition to industry-standard methods, there may be proprietary methods for data communication functions), even if other businesses are allowed to use that OS function for individual software provision using a technical method different from that used by designated providers, etc., it is sufficient if other businesses can use that OS function for individual software provision without significantly inferior performance compared to designated providers, etc.. However, for example, if other businesses are allowed to use that OS function for individual software provision using a technical method different from that used by designated providers, etc., but the performance is significantly inferior to that when designated providers, etc., use that OS function for individual software provision, it does not constitute "other businesses using the equivalent performance to provide individual software."

(C) Actions That "Prevent" the Use of OS Functions with Equivalent Performance by Other Businesses

Article 7, Item 2 of this Act refers to conduct that creates a high likelihood of making it difficult for other businesses to utilize these OS functions with equivalent performance for the provision of individual software. Such actions include conduct that prevents other businesses from utilizing these OS functions with equivalent performance for individual software provision (see C (A) below), as well as conduct that, while nominally permitting other businesses to utilize these OS functions with equivalent performance for individual software provision, creates a high likelihood of practically making it difficult for them to do so by imposing unreasonable technical constraints, contractual terms, or excessive financial burdens on those other businesses, or by steering smartphone users away from utilizing these OS functions or from granting permissions for the use of these OS functions to other businesses (see C (B) below).

For a designated provider's action to be considered as "preventing" the use of these OS functions with equivalent performance by other businesses, it is not necessary for other businesses to be completely unable to utilize these OS functions with equivalent performance for individual software provision. The determination of whether an action falls under this category is made based on the degree of likelihood that such a result will occur.

The degree of likelihood of causing difficulty for other businesses to use these OS functions with equivalent performance is assessed comprehensively based on factors such as: the nature of the designated provider's actions, the duration of such actions, the extent of impact on other businesses providing individual software using these OS functions, the degree of impact on smartphone users who use such individual software, etc.. For example, if access to these OS functions with equivalent performance is permitted without charge or restrictions, such actions would not be considered as "hindering" conduct under Article 7, Item 2. Furthermore, regarding actions where a designated provider imposes financial burdens such as fees as consideration for intellectual property rights such as patent rights, etc., when other businesses use these OS functions with equivalent performance, the judgment will be made in accordance with conventional practices under the Antimonopoly Act, as described in 2.2 above. If the action is recognized as an exercise of intellectual property rights, it will be determined that it does not violate Article 7 of the Act.

C. Hypothetical Scenarios

(A) Hypothetical scenarios of actions where a designated provider prevents other businesses

from utilizing these OS functions with equivalent performance for individual software provision, and thus falls under Article 7, Item 2 of the Act, include the following:

a. Preventing other businesses from using these OS functions via technical means, such as refusing to provide necessary Application Programming Interfaces (APIs) or other tools (hereinafter referred to as "APIs, etc.") that enable the use of these OS functions for individual software provision (including denying permissions for API use).

Hypothetical Scenarios: (Each function listed in the hypothetical scenarios is assumed to be an OS function. The same applies hereinafter in (2).)

- **Hypothetical Scenario 41:** A designated provider refuses to provide necessary APIs, etc., for other businesses to use message transmission/reception functions based on standards such as SMS (Short Message Service), which are used by designated providers, etc., to provide messaging apps.
- **Hypothetical Scenario 42:** A designated provider refuses to provide necessary APIs, etc., for other businesses to use NFC (Near Field Communication) functions, which are used by designated providers, etc., to provide payment apps that enable contactless payments.
- **Hypothetical Scenario 43:** A designated provider refuses to provide necessary APIs, etc., for other businesses providing similar services (e.g., search services) to use functions that enable efficient use of the designated provider's services (e.g., search services) provided in the designated provider, etc.'s individual software.
- **Hypothetical Scenario 44:** A designated provider refuses to provide necessary APIs, etc., for other businesses to use simple pairing functions with smartphones, which are used for smartwatches functionally integrated with companion apps provided by designated providers, etc..
- **Hypothetical Scenario 45:** A designated provider, who previously provided necessary APIs, etc., for other businesses to use these OS functions with equivalent performance in the provision of individual software, upon updating its basic operation software, continues to allow designated providers, etc., to use those OS functions for individual software provision, but ceases to provide those APIs, etc., to other businesses.

b. Contractually prohibiting other businesses from using these OS functions for the provision of individual software through terms of use or agreements.

Hypothetical Scenarios:

- **Hypothetical Scenario 46:** A designated provider prohibits other businesses from using

biometric authentication functions, which are used by designated providers, etc., to provide payment apps, for the provision of individual software in the terms of use or other contracts for the basic operation software.

- **Hypothetical Scenario 47:** A designated provider who also provides an application store through its basic operation software prohibits other businesses from using the function to display navigation screens even on the smartphone's lock screen, which is used by its subsidiaries to provide map apps, for the provision of individual software in the terms of use or other contracts for that application store.

c. Imposing technical restrictions or contractual terms, etc., that prevent other businesses from using these OS functions with equivalent performance for the provision of individual software.

Hypothetical Scenarios:

- **Hypothetical Scenario 48:** A designated provider allows photo apps provided by designated providers, etc., to upload data to cloud servers from the app even in the background (meaning the app is running even if it is not displayed on the smartphone screen) for a sufficient period, while allowing photo apps provided by other businesses to use this function for an insufficient period.
- **Hypothetical Scenario 49:** A designated provider allows voice call apps provided by designated providers, etc., to use voice call functions with protocols that offer superior communication speed, etc., while restricting voice call apps provided by other businesses to use only protocols that offer inferior communication speed, etc..
- **Hypothetical Scenario 50:** A designated provider restricts the scope of uses for data communication functions via Bluetooth between smartphones and smartphone peripherals such as smartwatches, which are functionally integrated with companion apps, for other businesses, compared to the scope of uses available to designated providers, etc..
- **Hypothetical Scenario 51:** A designated provider allows application stores provided by designated providers, etc., to use the function to automatically update apps in the background that are provided through the application store without restrictions on update cycles, etc., while imposing certain restrictions on update cycles, etc., for application stores provided by other businesses.
- **Hypothetical Scenario 52:** A designated provider, who previously provided necessary APIs, etc., for other businesses to use these OS functions with equivalent performance in the provision of individual software, upon updating its basic operation software, allows

designated providers, etc., to use those OS functions for individual software provision with improved performance compared to before, but despite being able to provide APIs, etc., for those OS functions with improved performance to other businesses, only allows them to use those OS functions for individual software provision with the previous performance.

(B) Hypothetical scenarios of actions where a designated provider, while permitting other businesses to utilize these OS functions with equivalent performance for individual software provision, creates a high likelihood of practical difficulty for other businesses to use these OS functions with equivalent performance for individual software provision, and thus falls under Article 7, Item 2 of the Act, include the following:

a. Imposing unreasonable technical constraints, contractual terms, or other conditions regarding the use of these OS functions on other businesses that use or intend to use these OS functions with equivalent performance for individual software provision.

Hypothetical Scenarios:

- **Hypothetical Scenario 53:** When it is normally necessary for other businesses to receive technical explanations, etc., regarding the use of these OS functions in addition to APIs, etc., from the designated provider to use these OS functions with equivalent performance for individual software provision, the designated provider only provides APIs, etc., but does not sufficiently provide technical explanations, etc., regarding the use of these OS functions.
- **Hypothetical Scenario 54:** A designated provider who also provides an application store through its basic operation software arbitrarily manipulates the search algorithm within that application store, causing individual software provided by other businesses that use these OS functions with equivalent performance to be positioned lower than the fair and non-discriminatory display order in the search results within the application store, or to be positioned in a location that makes discovery by smartphone users difficult, simply because the individual software uses these OS functions with equivalent performance.
- **Hypothetical Scenario 55:** A designated provider seeks consent from other businesses to unreasonable conditions regarding the use of these OS functions, which create a high likelihood of making it difficult for those other businesses to use these OS functions with equivalent performance for individual software provision (e.g., if the designated provider is a major recipient of goods or services related to the other business's important business, and the designated provider, without reasonable grounds, refuses to receive those goods or services from the other business, or restricts the quantity or

content of those goods or services received, in exchange for the other business using these OS functions with equivalent performance for individual software provision).

b. Imposing excessive financial burdens on other businesses that use or intend to use these OS functions with equivalent performance for individual software provision.

Hypothetical Scenarios:

- **Hypothetical Scenario 56:** A designated provider imposes financial burdens such as excessively high usage fees for these OS functions on other businesses, creating a significant practical obstacle for those other businesses to utilize these OS functions with equivalent performance (Note).

(Note) The level of fees that are likely to make it difficult for other businesses to use these OS functions with equivalent performance for individual software provision will be judged based on individual case-specific circumstances. Generally, the basic operation software of a designated provider is a common platform for other businesses to provide individual software, in addition to designated providers, etc. Therefore, ensuring the use of OS functions, which are functions controlled by the basic operation software, with equivalent performance is important for businesses that use OS functions to provide individual software. The amount of such financial burdens, payment terms, etc., will be considered.

c. If a designated provider adopts a system (hereinafter referred to as "application system" in (2)) where other businesses are required to submit prior applications to the designated provider to use existing OS functions for individual software provision, and the designated provider reviews, etc., the content of such applications before enabling other businesses to use the applied-for OS functions with equivalent performance for individual software provision, hypothetical scenarios include the following actions:

Hypothetical Scenarios:

- **Hypothetical Scenario 57:** Despite an eligible application having been submitted by another business, the designated provider excessively delays completing the necessary measures to enable the use of the applied-for OS functions with equivalent performance over an extended period (Note).

(Note) "Excessively delays completing the necessary measures over an extended period" refers to not completing the measures beyond a period that is objectively deemed reasonably necessary, depending on the content of the application. The standard period for this judgment

is generally expected to be around 6 to 18 months, depending on the extent of engineering efforts required by the designated provider to respond to the application. In any case, if the measures are still not completed after more than 24 months from the date the application was submitted, it can generally be said to fall under "excessively delays completing the necessary measures over an extended period." However, this does not apply if the designated provider can demonstrate objective and reasonable circumstances where, despite having appropriately and diligently taken all necessary actions to complete the measures within a period objectively deemed reasonably necessary (including appropriately prioritizing application processing and allocating sufficient personnel, etc., for that purpose), the completion of the measures could not avoid exceeding that period, or if an application was submitted for an OS function where the impact on competition for individual software resulting from the completion of the measures is deemed negligible (e.g., due to extremely limited demand), and the designated provider can demonstrate that the engineering efforts required to respond to that application are substantial.

d. Steering smartphone users away from utilizing individual software provided by other businesses that use these OS functions with equivalent performance, or from granting permissions for the use of these OS functions to those other businesses, when smartphone users use or intend to use such individual software.

Hypothetical Scenarios:

- **Hypothetical Scenario 58:** A designated provider implements technical specifications in its basic operation software that make it difficult for smartphone users to use these OS functions related to individual software provided by other businesses that use these OS functions with equivalent performance (including granting permissions for the use of these OS functions to those other businesses; hereinafter the same in d), such as unnecessarily complicating the setup process for such use.
- **Hypothetical Scenario 59:** When smartphone users attempt to use these OS functions related to individual software provided by other businesses that use these OS functions with equivalent performance, the designated provider displays a pop-up promoting the convenience of using these OS functions related to individual software provided by designated providers, etc., thereby steering users towards using these OS functions related to individual software provided by designated providers, etc..
- **Hypothetical Scenario 60:** Between the time smartphone users intend to use individual software provided by other businesses that use these OS functions with equivalent performance and the actual use of these OS functions, the designated provider engages

in actions or displays that induce users to abandon such use (e.g., presenting warnings that convey an exaggerated sense of risk associated with such use, repeatedly showing screens requesting confirmation of such use without reasonable grounds).

D. Hypothetical Scenarios of Justifiable Reasons

Based on the basic understanding of the applicability of justifiable reasons in (1) D above, hypothetical scenarios where justifiable reasons are typically recognized and do not constitute violations, and hypothetical scenarios where justifiable reasons are typically not recognized and constitute violations, are as follows:

(A) Hypothetical Scenarios Where Justifiable Reasons are Accepted and Not Considered Violations

Hypothetical scenarios of actions that are typically recognized as having justifiable reasons and are not considered violations of Article 7 include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 61:** When certain OS functions raise cybersecurity concerns, and it is difficult to resolve those concerns unless the ability to use such functions for individual software provision is limited to certain businesses, the designated provider may conduct reviews or examinations based on necessary standards for cybersecurity, etc., and if a business fails to meet those standards, the designated provider may restrict use of those specific OS functions. This action, while hindering the use of specific OS functions by preventing other businesses from using them with equivalent performance for individual software provision if they do not meet the review criteria set by the designated provider, contributes to ensuring cybersecurity, etc. Furthermore, if the review criteria and their application are limited to the necessary scope in light of their purpose, a justifiable reason is recognized, and it does not violate Article 7 of the Act.
- **Hypothetical Scenario 62:** When the designated provider offers APIs or other tools necessary for utilizing specific OS functions with equivalent performance, but imposes restrictions in the terms of use to ensure compliance with existing laws—such as the Act on the Protection of Personal Information— and prohibits the handling of smartphone user information in ways that violate the spirit of such legal provisions. This action, while imposing conditions on the use of specific OS functions and potentially hindering their use, contributes to the protection of information related to smartphone

users. Furthermore, if it merely restricts the handling of such information in ways that violate the spirit of existing laws, while providing APIs, etc., for the use of those OS functions, a justifiable reason is recognized, and it does not violate Article 7 of the Act.

- **Hypothetical Scenario 63:** If the basic operation software detects a significant deterioration in smartphone device performance due to the use of a specific OS function with equivalent performance, the designated provider restricts the use of that OS function through non-discriminatory technical settings or other means, to the extent necessary to restore the smartphone device's performance. This action, while restricting the use of a specific OS function when the basic operation software detects a significant deterioration in smartphone device performance, contributes to the prevention of abnormal operation of smartphones. Furthermore, if it merely restricts the use of that OS function to the extent necessary to restore the smartphone device's performance through non-discriminatory technical settings or other means, while providing APIs, etc., for the use of that OS function, a justifiable reason is recognized, and it does not violate Article 7 of the Act.

(B) Hypothetical Scenarios Where Justifiable Reasons Are Not Accepted and Constitute Violations

Hypothetical scenarios of actions that are typically not recognized as having justifiable reasons and are considered violations of Article 7 include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 64:** A designated provider, for a specific OS function, conducts reviews or examinations based on necessary cybersecurity standards for multiple businesses, granting access to OS functions with equivalent performance to those who meet the criteria, but then denies access to specific businesses —without conducting a proper review, etc. — in the name of cybersecurity concerns, despite having the purpose of ensuring cybersecurity, etc.. This action is typically deemed to be an attempt to exclude that other business and cannot be objectively evaluated as being conducted for the purpose of ensuring cybersecurity, etc. Therefore, a justifiable reason is not recognized, and it violates Article 7 of the Act.
- **Hypothetical Scenario 65:** A designated provider imposes a blanket prohibition on the use of specific OS functions by other businesses, without considering their initiatives or efforts, under the pretense of being necessary to achieve the purpose of protecting information related to smartphone users, even though it is not difficult to achieve the same purpose by limiting the eligible business operators to those who meet certain

criteria, allowing them to use OS functions with equivalent performance to provide individual software. This action, despite having the legitimate purpose of protecting information related to smartphone users, does not qualify as having a justifiable reason because that purpose can be achieved by setting objective and reasonable criteria from the perspective of protecting information and conducting reviews or examinations, and then allowing only those who meet the criteria to use specific OS functions with equivalent performance, meaning there are other less competition-restricting means to achieve that purpose. Therefore, it violates Article 7 of the Act.

- **Hypothetical Scenario 66:** A designated provider imposes a blanket prohibition on the use of a specific OS function by other businesses, without considering alternative means to provide parental control services, under the pretense of being necessary to achieve the purpose of safeguarding youth who use smartphones or preventing criminal activities conducted using smartphones, even though the OS function can be included in parental control services managed by parents. This action, despite having the legitimate purpose of safeguarding youth who use smartphones or preventing criminal activities conducted using smartphones, does not qualify as having a justifiable reason because that purpose can be achieved by alternative means, such as including it in parental control services managed by parents, meaning there are other less competition-restricting means to achieve that purpose. Therefore, it violates Article 7 of the Act.

E. Desirable Practices by Designated Providers to Avoid Violations

To prevent actions that fall under Article 7, Item 2 and violate Article 7 of the Act, it is desirable for designated providers of basic operation software to undertake the following practices:

- During the design phase of basic operation software, designated providers ensure that OS functions are structured in a way that allows other businesses to use them with equivalent performance for the provision of individual software. Even if other businesses can use OS functions with equivalent performance for the provision of individual software, if there is a delay compared to when designated providers, etc., use them for the provision of individual software, designated providers, etc., may gain a first-mover advantage in competition, putting other businesses at a disadvantage. Therefore, to prevent actions that fall under Article 7, Item 2 and violate Article 7 of the Act, it is useful for designated providers to design new OS functions developed after the enforcement of the Act, or existing OS functions that are modified, assuming that other businesses will use them with equivalent performance for the provision of individual software from the design stage of the basic operation software. Furthermore, it is

effective to actively disclose APIs, etc., without waiting for applications from other businesses, unless there are cybersecurity concerns, etc., thereby enabling other businesses to quickly and easily use OS functions with equivalent performance for the provision of individual software without delay from the time designated providers, etc., use them for the provision of individual software. It is desirable for designated providers to take such proactive measures from the perspective of complying with Article 7 of the Act.

F. Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

Designated providers of basic operation software are required to report to the Japan Fair Trade Commission on the status of their compliance with Article 7, Item 2, including the matters stipulated in Rules Article 36, Paragraph 2. Examples of other necessary information for confirming compliance with the Act under Item 4(c) of the same paragraph include the following:

1. If the designated provider implements measures such as an application system as conditions for other businesses to use these OS functions, the outline of the implementation method for such measures (if an application system is implemented, the method for submitting applications, information requested from other businesses during the application, each stage from application to completion of measures and their deadlines, considerations and review criteria for conducting reviews or examinations related to applications, method for providing APIs, etc., related to applications, status of system development for responding to applications (including API development), and status of explanation or disclosure to other businesses regarding the series of processes), and the content of related terms and conditions.
2. If the designated provider adopts an application system, the following numbers of cases:
   (a) The number of applications that the designated provider continued to respond to after the submission of the previous year's compliance report.

   (b) The number of applications received by the designated provider since the submission of the previous year's compliance report.

   (c) Out of the numbers of applications in (a) and (b), the number of applications for which the designated provider determined that the applied-for function falls under these OS functions (i.e., is subject to Article 7, Item 2 of the Act).

   (d) Out of the number of applications in (c), the number of applications for which the

designated provider had completed measures to enable the applicant to use the applied-for OS functions with equivalent performance as of the submission of this year's compliance report.

(e) For the applications in (d), the average number of days required for the designated provider from the acceptance of the application to the completion of the measures.

(f) Out of the number of applications in (c), the number of applications for which the designated provider is continuing to respond as of the submission of this year's compliance report.

(g) Out of the number of applications in (c), the number of applications for which the designated provider determined that a justifiable reason applied and therefore decided not to take measures to enable the applicant to use the applied-for OS functions with equivalent performance as of the submission of this year's compliance report.

4. Article 8: Prohibited Conduct by Designated Providers of Application Stores

(1) Item 1 (Prohibition of Restricting or Hindering the Use of Alternative Payment Management Services, etc.)

A. Basic Approach

Article 8, Item 1 of this Act prohibits designated providers of application stores from imposing conditions that prevent individual app providers from using alternative payment management services (i.e., payment management services other than those provided by the designated provider, including its subsidiaries; hereinafter referred to as "designated providers, etc." in this section) when offering individual software through the application store. It also forbids designated providers from obstructing individual app providers from enabling smartphone users to make payments using other methods without relying on payment management services. By prohibiting actions that restrict the use of alternative payment management services, etc. (meaning either alternative payment management services or other payment methods that individual app providers can offer to smartphone users without utilizing payment management services), this Act aims to enhance competition in individual software by allowing app providers to offer diverse payment services.

B. Specific Understanding of Article 8, Item 1

(A) Payment Management Services and Payment Methods

"Payment management services" in Article 8, Item 1 of the Act refer to services that enable

smartphone users to use payment methods while individual software is running. Specifically, these are services used by smartphone users when purchasing digital content such as items sold through individual software or making payments for subscription services, and they have a function that allows users to view their payment history, etc., in a list, commonly referred to as in-app purchase systems. Also, "payment methods" in the same item refer to all payment methods used by smartphone users to pay for goods or services, and specifically include various methods such as prepaid payment methods (payment by prepaid cards, etc.), credit card payments, bank transfers, and QR code-based cashless payments.

(B) Actions that make it a condition for using the application store that individual app providers do not use alternative payment management services

Article 8, Item 1(a) of the Act, which states that "…make it a condition for providing individual software through the application store that the individual application developer does not use any payment management service (meaning services that allow smartphone users to use payment instruments," refers to actions where an application store designated provider directly restricts the payment management services that can be used in the application store to those provided by the designated provider, etc. Such actions include the designated provider requiring, by contract or other means, that only payment management services provided by the designated provider, etc., be used for payment when providing goods or services through individual software, or prohibiting the use of alternative payment management services for payment.

(C) Actions that "Prevent" the Use of Alternative Payment Management Services, etc.

Actions that hinder the use of alternative payment management services, etc., refer to conduct that creates a high likelihood of making it difficult for individual app providers to utilize such services while offering individual software through a designated provider's application store. Such actions may include, among others: imposing unreasonable technical restrictions on individual app providers while allowing them to use alternative payment management services, placing excessive financial burdens on individual app providers for using alternative payment management services, etc., steering smartphone users away from utilizing alternative payment management services, etc.

The determination of whether a designated provider's action constitutes "preventing" the use of alternative payment management services, etc., does not require that it be completely impossible for individual app providers to use alternative payment management services, etc.

Instead, the determination is made based on the degree of likelihood that such a result will occur.

The degree of "difficulty" for use of alternative payment management services, etc. is assessed comprehensively based on factors such as: the nature of the designated provider's actions, the duration of such actions, the impact on individual app providers attempting to provide individual software using alternative payment management services, etc., the extent of impact on smartphone users utilizing such individual software, etc.

C. Hypothetical Scenarios

(A) Hypothetical scenarios of actions where a designated provider limits the payment management services available in its application store to those provided by the designated provider, etc., thus falling under Article 8, Item 1(a) of the Act, include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 67:** A designated provider, in the review items for reviews or examinations for using the application store, sets a condition that requires individual app providers to use only the payment management service provided by the designated provider, etc., for payment when providing goods or services through individual software.
- **Hypothetical Scenario 68:** A designated provider, in the terms of use for the application store, sets a condition that prohibits individual app providers from using alternative payment management services for payment when providing goods or services through individual software.

(B) Hypothetical scenarios of actions where a designated provider, while permitting the use of alternative payment management services, etc., in relation to its application store, substantially creates a high likelihood of difficulty for their use, and thus falls under Article 8, Item 1(b) of the Act, include the following:

a. A designated provider imposes unreasonable technical restrictions, contractual terms, or other conditions regarding the use of alternative payment management services, etc., on individual app providers who use or intend to use alternative payment management services, etc., in relation to its application store.

Hypothetical Scenarios:

- **Hypothetical Scenario 69:** A designated provider refuses to provide an app development

environment for individual app providers to offer individual software in its application store, when the individual app providers intend to use alternative payment management services, etc., for payment when providing goods or services through individual software.

- **Hypothetical Scenario 70:** If a designated provider requires individual app providers to submit applications, etc., for the use of alternative payment management services, etc., despite having received an eligible application and a reasonable period for reviews or examinations (taking into account the specific circumstances of the individual app provider) has passed, the designated provider does not provide a sufficient response to the application, etc., thereby preventing the provision of individual software using alternative payment management services, etc.
- **Hypothetical Scenario 71:** A designated provider manipulates the search algorithm within its application store to lower the search ranking of individual software that utilizes alternative payment management services or places such software in positions that make discovery by smartphone users more difficult, due to the individual software utilizing alternative payment management services, etc.
- **Hypothetical Scenario 72:** When an individual app provider can use both the designated provider, etc.'s payment management service and alternative payment management services, etc., and intends to use both, the designated provider processes the display for smartphone users such that buttons or text related to payments for alternative payment management services, etc., are displayed smaller or their colors are changed, compared to buttons or text related to payments for the designated provider, etc.'s payment management service.

b. A designated provider imposes excessive financial burdens regarding the use of alternative payment management services, etc., on individual app providers who use or intend to use alternative payment management services, etc., in relation to its application store.

Hypothetical Scenarios:

- **Hypothetical Scenario 73:** A designated provider, when individual app providers use alternative payment management services, demands fees or places financial burdens at a level that creates a high likelihood of making the use of such services practically difficult.

(Note) The level of fees that are likely to make the use of alternative payment management services, etc., difficult will be judged based on individual case-specific circumstances. For example, considerations will include the financial burdens such as fees required by designated providers, etc., from individual app providers when using payment management services

provided by designated providers, etc., and the financial burdens such as fees required by businesses providing alternative payment management services, etc., from individual app providers when using alternative payment management services, etc. (also taking into account whether efficient businesses providing alternative payment management services, etc., can continue their operations), and the financial burdens such as fees required by designated providers when using alternative payment management services, etc.

c. A designated provider steers smartphone users away from utilizing alternative payment management services, etc., when they use or intend to use alternative payment management services, etc., in relation to its application store.

Hypothetical Scenarios:

- **Hypothetical Scenario 74:** When an individual app provider can use both the designated provider, etc.'s payment management service and alternative payment management services, etc., and a smartphone user attempts to use alternative payment management services, etc., the designated provider, from the perspective of providing basic operation software and the application store, processes the display such that buttons or text related to payments for alternative payment management services, etc., are displayed smaller or their colors are changed, compared to buttons or text related to payments for the designated provider, etc.'s payment management service, thereby making it difficult for smartphone users to select alternative payment management services, etc.
- **Hypothetical Scenario 75:** A designated provider, as the provider of basic operation software and the application store, displays pop-ups promoting the convenience of its own payment management services whenever a smartphone user attempts to use alternative payment management services, thereby steering users toward its own payment management services.

D. Hypothetical Scenarios of Justifiable Reasons

Based on the basic understanding of the applicability of justifiable reasons in 3 (1) D above, hypothetical scenarios where justifiable reasons are typically recognized and do not constitute violations, and hypothetical scenarios where justifiable reasons are typically not recognized and constitute violations, are as follows:

(A) Hypothetical Scenario Where Justifiable Reasons are Accepted and Not Considered Violations

Hypothetical scenarios of actions that are typically recognized as having justifiable reasons

and are not considered violations of Article 8 include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 76:** A designated provider, in order to prevent criminal activities using smartphones and to protect smartphone user information to the necessary extent, establishes requirements that limit the use of alternative payment management services to those that properly handle payment information (such as credit card details) and ensure appropriate refund and cancellation procedures. This action, while limiting the alternative payment management services that individual app providers intend to use and thus hindering the use of alternative payment management services, etc., contributes to the prevention of criminal activities conducted using smartphones and the protection of information related to smartphone users. Furthermore, if the requirements for limiting alternative payment management services, etc., are limited to the necessary scope in light of their purpose, a justifiable reason is recognized, and it does not violate Article 8 of the Act.
- **Hypothetical Scenario 77:** A designated provider, from the perspective of providing basic operation software and the application store, enables settings (commonly referred to as parental control functions) to restrict the use of payment management services, including alternative payment management services, by minor smartphone users based on parental consent, in order to prevent unintended excessive charges or erroneous charges, which falls under safeguarding youth who use smartphones. This action, while restricting smartphone users from using alternative payment management services, etc., and potentially hindering individual app providers' use of alternative payment management services, etc., contributes to safeguarding youth who use smartphones. Furthermore, if the individual app providers who use alternative payment management services, etc., do not provide parental control functions equivalent to those of the designated provider, it is considered that there are no other less competition-restricting means to achieve this purpose. Therefore, a justifiable reason is recognized, and it does not violate Article 8 of the Act.
- **Hypothetical Scenario 78:** If an alternative payment management service, etc., does not implement appropriate measures for ensuring cybersecurity for smartphone use and protecting information related to smartphone users, and it is determined that using such alternative payment management service, etc., would lead to the leakage of smartphone users' credit card information, etc., the designated provider, from the perspective of ensuring cybersecurity for smartphone use and protecting information related to smartphone users, prohibits the provision of individual software that uses such

alternative payment management service, etc., in the application store. This action, while restricting individual app providers from using alternative payment management services, etc., and thus hindering their use, contributes to the protection of smartphone user information. Furthermore, if alternative payment management services, etc., do not implement measures that meet certain objective and reasonable standards for ensuring cybersecurity for smartphone use and protecting information related to smartphone users, it is considered that there are no other less competition-restricting means to achieve this purpose. Therefore, a justifiable reason is recognized, and it does not violate Article 8 of the Act.

(B) Hypothetical Scenarios Where Justifiable Reasons Are Not Accepted and Constitute Violations

Hypothetical scenarios of actions that are typically not recognized as having justifiable reasons and are considered violations of Article 8 include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 79:** A designated provider, citing cybersecurity concerns such as an increased risk of credit card information leaks due to cyberattacks, and concerns over criminal activities using smartphones, imposes a blanket prohibition on individual app providers using alternative payment management services without conducting proper reviews or examinations. This action, despite having the legitimate purpose of ensuring cybersecurity for smartphone use or preventing criminal activities conducted using smartphones, does not qualify as having a justifiable reason because that purpose can be achieved by setting objective and reasonable standards from the perspective of ensuring cybersecurity for smartphone use or preventing criminal activities conducted using smartphones and conducting reviews or examinations, and then allowing only those who meet the standards to use alternative payment management services, etc., when those services are provided by businesses that have taken sufficient countermeasures against cyberattacks, meaning there are other less competition-restricting means to achieve that purpose. Therefore, it violates Article 8 of the Act.
- **Hypothetical Scenario 80:** A designated provider, in order to prevent individual app providers from using alternative payment management services, prohibits the provision of individual software that uses such alternative payment management services in the application store, citing problems from the perspective of ensuring cybersecurity for smartphone use or protecting information related to smartphone users, even though the use of such alternative payment management services does not raise concerns from the

perspective of ensuring cybersecurity for smartphone use or protecting information related to smartphone users. This action, despite the designated provider claiming the purpose of ensuring cybersecurity for smartphone use or protecting information related to smartphone users, cannot be objectively evaluated as being conducted for that purpose, as the use of the alternative payment management service does not raise concerns from the perspective of ensuring cybersecurity for smartphone use or protecting information related to smartphone users. Therefore, a justifiable reason is not recognized, and it violates Article 8 of the Act.

E. Desirable Practices by Designated Providers to Avoid Violations

To prevent actions that fall under Article 8, Item 1 and violate Article 8 of the Act, it is desirable for designated providers of application stores to undertake the following practices:

- When imposing fees or other financial burdens on individual app providers using alternative payment management services, designated providers disclose the amount by posting it on their website or through other notifications. Additionally, they explain to such providers that the level of imposed financial burden is reasonable in light of the benefits individual app providers gain from the application store.

F. Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

Designated providers of application stores are required to report to the Japan Fair Trade Commission on the status of their compliance with Article 8, Item 1, including the matters stipulated in Rules Article 36, Paragraph 2. Examples of other necessary information for confirming compliance with the Act under Item 4(c) of the same paragraph include the following:

1. The number of individual software that uses alternative payment management services, etc. (limited to those identified by the designated provider through reviews or examinations, etc.) in the application store.
2. If the designated provider establishes certain criteria and conducts reviews or examinations as conditions for individual app providers to use alternative payment management services, etc., the criteria for such reviews or examinations, the procedures for conducting them, and the name and content of any related terms and conditions.
3. If the designated provider imposes financial burdens such as fees on individual app providers as conditions for them to use alternative payment management services, etc., the calculation method of such financial burdens and the reasons for imposing them, and

the name and content of any related terms and conditions.

(2) Item 2 (Prohibition of Hindering the Provision of Goods or Services Through Related Web Pages, etc.)

A. Basic Approach

Article 8, Item 2 of this Act prohibits designated providers of application stores from imposing conditions that prevent individual app providers from displaying pricing or other information about goods or services offered through web pages or other individual software outside their own software (hereafter, "related web pages, etc.") during the operation of their individual software (hereafter, "this individual software"). It also forbids designated providers from prohibiting individual app providers from including external links ("link-outs") that direct users to web pages outside the individual software. Additionally, designated providers may not prevent smartphone users utilizing individual software from accessing goods or services provided through related web pages, etc. By prohibiting actions that prevent transactions or payments conducted through related web pages, etc., this Act aims to enhance competition in individual software by allowing individual app providers to offer diverse services through such external platforms.

B. Specific Understanding of Article 8, Item 2

(A) Cases where goods or services are provided as stipulated by the Act

Article 8, Item 2 of the Act, which refers to cases where "…the individual application developer provides goods or services through the individual software provided by the individual application developer and provides the same goods or services through a web page or individual software other than such individual software," typically refers to cases where an individual app developer (provider) sells the same digital content, etc., both within its individual software (this individual software) and outside its software (related web pages, etc.).

For example, this applies when items consumed within a game provided as individual software are sold both within that individual software and within other individual software, or on a web page displayed in a browser. This also includes cases where the price of the item differs, or where bonuses are granted for coins consumed within the game, meaning it is not necessary for the content and price of the goods or services provided in this individual software and related web pages, etc., to be completely identical.

(B) "Cases specified by Cabinet Order"

To promote competition in individual software through the provision of diverse services related to transactions on related web pages, etc., in light of the intent of Article 8, Item 2, Article 3 of the Order stipulates that "cases specified by Cabinet Order as equivalent thereto" refer to cases where an individual app provider offers goods or services through related web pages, etc., that are utilized within this individual software but are not provided through this individual software itself.

Specifically, the following cases fall under "cases specified by Cabinet Order":

1. Cases where no digital content is sold, etc., within this individual software, but smartphone users purchase digital content on related web pages, etc., and then utilize it in this individual software (so-called reader apps, etc.). For example, for video streaming services, where users cannot enter into usage contracts within this individual software, but enter into usage contracts on the website of the business providing the video streaming service, and then by logging in with the contracted account or linking the account to this individual software, the video streaming service can be used within this individual software.
2. Cases where digital content is sold, etc., within this individual software, but non-identical goods or services are sold, etc., on related web pages, etc. For example, this applies when digital content (e.g., character skins that can be used in a game app) that is not sold within this individual software is sold exclusively on a web store.

(C) Display of Pricing and Other Information about Goods or Services Provided Through Related Web Pages, etc.

The "display of pricing and other information about goods or services provided through related web pages, etc." in Article 8, Item 2 of the Act includes not only the sales price on related web pages, etc., but also announcements of their existence, information on sales, special offers, and other marketing content related to the goods or services on related web pages, etc.

(D) Function to Browse Related Web Pages, etc., via This Individual Software

The function stipulated by the JFTC Rules in Article 8, Item 2 (function to browse related web pages, etc., via this individual software) refers to link-out capabilities. The Rules define it as the ability for users to obtain domain names or other location-related information of related

web pages, etc., by selecting displayed text, graphics, or other perceptible information on a smartphone screen, allowing them to access those web pages, etc.

"Text, graphics, or other perceptible information" broadly includes, for example, sentences expressing information about related web pages, etc., as well as images and buttons.

The "function to obtain domain names or other location-related information of related web pages, etc., and browse those related web pages, etc." assumes that by selecting the relevant information on the screen, a browser will launch and allow users to browse the web page.

(E) Actions that make it a condition for using the application store that pricing or other information about goods or services provided through related web pages, etc., is not displayed while this individual software is running

Article 8, Item 2(a) of the Act, which states that a designated provider "…make it a condition for providing such individual software through the application store that such information is not displayed while such individual software is executing (including attaching a condition that refuses or restricts the use of the feature that allows browsing of the related web pages, etc. through such individual software as specified in Fair Trade Commission Rules)," refers to actions where an application store designated provider directly restricts the display of external promotional information and the provision of link-outs in this individual software. Such actions include the designated provider prohibiting, by contract or other means, the display of external promotional information within this individual software, or prohibiting the inclusion of link-out capabilities to related web pages, etc., within this individual software.

(F) Actions that "Prevent" the Provision of Goods or Services Through Related Web Pages, etc.

Actions that prevent the provision of goods or services through related web pages, etc., refer to conduct that, while not directly prohibiting the display of external promotional information or the provision of link-outs in the terms of use within this individual software, creates a high likelihood of making it difficult to provide goods or services through related web pages, etc., including the display of external promotional information and the provision of link-outs. Such actions include imposing unreasonable technical restrictions on individual app providers, placing excessive financial burdens on them, or steering smartphone users away from obtaining goods or services through related web pages, etc. These actions constitute "preventing" the provision of goods or services through related web pages, etc., if they create a high likelihood of making such provision practically difficult.

The impact of such actions on the likelihood of making provisions difficult is assessed comprehensively based on various factors, including the nature of the designated provider's conduct, the duration of the conduct, the degree to which the conduct affects individual app providers offering goods or services through related web pages, etc., and the extent of impact on smartphone users utilizing the individual software.

C. Hypothetical Scenarios

(A) Hypothetical scenarios of actions where a designated provider prohibits the display of external promotional information or the provision of link-outs in its application store, thus falling under Article 8, Item 2(a) of the Act, include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 81:** A designated provider, as a condition for using the application store, prohibits individual app providers from displaying external promotional information, such as prices, discount amounts, or discount rates of digital content offered through related web pages, etc., or information on sales or special offers, within this individual software.
- **Hypothetical Scenario 82:** A designated provider, as a condition for using the application store, prohibits individual app providers from including link-out capabilities to related web pages, etc., where digital content is sold within this individual software.

(B) Hypothetical scenarios of actions where a designated provider, while permitting the display of external promotional information or the provision of link-outs in relation to its application store, substantially creates a high likelihood of difficulty in providing goods or services through related web pages, etc., and thus falls under Article 8, Item 2(b) of the Act, include the following:

a. A designated provider imposes unreasonable technical restrictions, contractual terms, or other conditions regarding the provision of goods or services through related web pages, etc., including the display of external promotional information and the provision of link-outs, on individual app providers who provide or intend to provide such goods or services in relation to its application store.

Hypothetical Scenarios:

- **Hypothetical Scenario 83:** A designated provider prohibits individual app providers from providing goods or services on related web pages, etc., through the terms of use, etc., of the application store.

- **Hypothetical Scenario 84:** A designated provider makes it difficult to provide goods or services on related web pages, etc., by preventing individual software of individual app providers that provide goods or services on related web pages, etc., from being displayed in a high position in the application store's ranking.
- **Hypothetical Scenario 85:** A designated provider refuses to offer APIs, templates, or other app development tools necessary for individual app providers to display external promotional information—such as sales or special offer details—or to provide link-out capabilities within their individual software.
- **Hypothetical Scenario 86:** A designated provider forces individual app providers to use payment management services or payment methods provided by designated providers, etc., as a condition for providing goods or services on related web pages, etc., or as a condition for displaying external promotional information or providing link-outs in this individual software, despite there being no necessity for the individual app providers and smartphone users.
- **Hypothetical Scenario 87:** A designated provider, without reasonable grounds, limits the number of displayed link-out destinations or does not allow payment web pages as link-out destinations (excluding pop-up displays that explain external website transitions when tapping the link).
- **Hypothetical Scenario 88:** If a designated provider requires individual app providers to submit applications, etc., for displaying external promotional information or providing link-outs in this individual software, despite having received an eligible application and a reasonable period for reviews or examinations (taking into account the specific circumstances of the individual app provider) has passed, the designated provider does not provide a sufficient response to the application, etc., thereby preventing the display of external promotional information or the provision of link-outs in this individual software.

b. A designated provider imposes excessive financial burdens regarding the provision of goods or services through related web pages, etc., including the display of external promotional information and the provision of link-outs, on individual app providers who provide or intend to provide such goods or services in relation to its application store.

Hypothetical Scenarios:

- **Hypothetical Scenario 89:** A designated provider, when individual app providers facilitate transactions through link-outs to related web pages, etc., demands fees or other financial burdens at a level that creates a high likelihood of making such transactions

practically difficult.

- **Hypothetical Scenario 90:** When external promotional information is displayed or link-outs are provided, or when goods or services are provided by individual app providers through related web pages, etc., the designated provider applies unfavorable conditions (e.g., refusing to use other systems or services provided by the designated provider) compared to cases where these are not provided, thereby imposing financial burdens such as additional response costs on individual app providers, and inducing them to abandon the provision of goods or services through related web pages, etc.

(Note) The level of fees that are likely to make it difficult to provide goods or services through related web pages, etc., will be judged based on individual case-specific circumstances. For example, for the provision of goods or services through related web pages, etc., via link-outs, the extent of benefits that individual app providers gain from the designated provider's application store will be considered, as well as the level of fees imposed by efficient businesses providing alternative application stores (limited to those adopting business models that operate application stores using fees collected from individual app providers) on individual app providers.

c. A designated provider steers smartphone users away from obtaining goods or services through related web pages, etc., including the display of external promotional information and the provision of link-outs, when smartphone users obtain or intend to obtain such goods or services, in relation to its application store.

Hypothetical Scenarios:

- **Hypothetical Scenario 91:** A designated provider, as the provider of basic operation software and the application store, processes the display of link-out buttons or text to worsen their visibility when smartphone users attempt to use link-outs, thereby making it difficult for users to use link-outs.
- **Hypothetical Scenario 92:** A designated provider, as the provider of basic operation software and the application store, displays a pop-up promoting the convenience of the designated provider, etc.'s payment management service and steering users towards using it, when external promotional information is displayed or link-outs are provided by individual app providers.

D. Hypothetical Scenarios of Justifiable Reasons

Based on the basic understanding of the applicability of justifiable reasons in 3 (1) D above,

hypothetical scenarios where justifiable reasons are typically recognized and do not constitute violations, and hypothetical scenarios where justifiable reasons are typically not recognized and constitute violations, are as follows:

(A) Hypothetical Scenario Where Justifiable Reasons are Accepted and Not Considered Violations

Hypothetical scenarios of actions that are typically recognized as having justifiable reasons and are not considered violations of Article 8 include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 93:** A designated provider, as a provider of basic operation software and an application store, displays a pop-up warning smartphone users that clicking on a link-out may redirect them to external websites that mimic legitimate ones in an attempt to deceive users or cause misunderstandings, and informs users that once redirected, the designated provider no longer controls the external website, because the designated provider cannot control the risk of smartphone users being redirected to such deceptive or misleading websites via link-outs. This action, while potentially causing smartphone users to abandon transitioning to external websites via link-outs and thus hindering the provision of goods or services on external websites, contributes to the prevention of criminal activities conducted using smartphones. Furthermore, if the content of the pop-up warning users about the risk of being involved in fraudulent activities if they transition to an external website via a link-out is factual, is not discriminatory towards individual app providers, is limited to the necessary scope in light of its purpose, and if the designated provider has no way to control such risks or no more effective way to convey the content to users, it is considered that there are no other means to achieve that purpose. Therefore, a justifiable reason is recognized, and it does not violate Article 8 of the Act.
- **Hypothetical Scenario 94:** A designated provider, as a provider of basic operation software and an application store, enables settings (commonly referred to as parental control functions) to restrict minor smartphone users from transitioning to external websites via link-outs and using payment on those websites, based on parental consent, from the perspective of safeguarding youth who use smartphones and preventing unintended excessive charges or erroneous charges. This action, while restricting minor smartphone users from transitioning to external websites via link-outs and thus hindering the provision of link-outs, contributes to safeguarding youth who use smartphones. Furthermore, if the businesses providing payment on external websites via

link-outs do not provide parental control functions equivalent to those of the designated provider, it is considered that there are no other means to achieve that purpose. Therefore, a justifiable reason is recognized, and it does not violate Article 8 of the Act.

(B) Hypothetical Scenarios Where Justifiable Reasons Are Not Accepted and Constitute Violations

Hypothetical scenarios of actions that are typically not recognized as having justifiable reasons and are considered violations of Article 8 include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 95:** If there are no restrictions on the content displayed as external promotional information or the destination websites accessed through link-outs, there is a risk that individual app providers may display pricing information that differs from the actual prices on external websites—including sale prices, discount amounts, and discount rates—or may mislead smartphone users by directing them to payment screens for goods or services different from what they intended to purchase. Under the justification of preventing unintended purchases by smartphone users—that is, from the perspective of preventing criminal activities using smartphones—a designated provider cannot impose a blanket prohibition, without conducting proper reviews, on including price information in external promotional content within individual software or on setting payment screens as the destination for link-outs. This action, despite having the legitimate purpose of preventing criminal activities conducted using smartphones, does not qualify as having a justifiable reason. This is because that purpose can be achieved by, for example, warning individual app providers and encouraging them to make improvements if there is a report that the price displayed in this individual software differs from the actual sales price on an external website, or by requiring individual app providers to confirm that the price information displayed in individual software is accurate and corresponds to the information on related web pages, etc., or by restricting link-outs only for individual software of individual app providers who are highly likely to design this individual software to mislead smartphone users to a different website than the link-out destination, meaning there are other less competition-restricting means to achieve that purpose. Therefore, it violates Article 8 of the Act.

E. Desirable Practices by Designated Providers to Avoid Violations

To prevent actions that fall under Article 8, Item 2 and violate Article 8 of the Act, it is desirable

for designated providers of application stores to undertake the following practices:

- If a designated provider imposes fees or other financial burdens on individual app providers who display external promotional information or provide link-outs in the application store, the designated provider notifies the amount of such financial burdens by means such as posting it on its website. Additionally, the designated provider explains to individual app providers who display external promotional information or provide link-outs that the level of financial burden imposed by the designated provider is reasonable in light of the benefits gained by the individual app providers from the application store.

F. Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

Designated providers of application stores are required to report to the Japan Fair Trade Commission on the status of their compliance with Article 8, Item 2, including the matters stipulated in Rules Article 36, Paragraph 2. Examples of other necessary information for confirming compliance with the Act under Item 4(c) of the same paragraph include the following:

1. The number of individual software in the application store where individual app providers display external promotional information (limited to those identified by the designated provider through reviews or examinations, etc.).
2. The number of individual software in the application store where individual app providers use link-outs (limited to those identified by the designated provider through reviews or examinations, etc.).
3. If the designated provider establishes certain criteria and conducts reviews or examinations as conditions for individual app providers to provide goods or services through related web pages, etc. (including those related to displaying external promotional information and providing link-outs), the criteria for such reviews or examinations, the procedures for conducting them, and the name and content of any related terms and conditions.
4. If the designated provider imposes financial burdens such as fees on individual app providers as conditions for them to provide goods or services through related web pages, etc. (including those related to displaying external promotional information and providing link-outs), the calculation method of such financial burdens and the reasons for imposing them, and the name and content of any related terms and conditions.

(3) Item 3 (Prohibition of Banning or Hindering the Use of Alternative Browser Engines)

A. Basic Approach

Article 8, Item 3 of this Act prohibits designated providers of application stores from making the browser engine provided by the designated provider, etc., a condition for individual app providers to use as a component of their individual software in the application store. Additionally, it forbids designated providers from preventing individual app providers from using alternative browser engines (i.e., browser engines other than those provided by the designated provider, etc.) as a component of their individual software. By prohibiting actions that prevent the adoption of alternative browser engines as components of individual software, this Act aims to enhance competition in individual software by allowing app providers to offer diverse browser engine choices. It should be noted that requiring the adoption of browser engines provided by designated providers, etc., in browsers as a condition for using the application store, or hindering the adoption of alternative browser engines (see C below for hypothetical scenarios), does not constitute a justifiable reason. On the other hand, as described in D below, justifiable reasons may be recognized for individual software other than browsers.

B. Specific Understanding of Article 8, Item 3

(A) Actions that make it a condition for using the application store that a browser engine provided by the designated provider, etc., is adopted.

Article 8, Item 3(a) of the Act, which states that "…make it a condition for providing individual software through the application store that the browser engine provided by the designated provider is to be a component of the individual software," refers to actions where an application store designated provider limits the browser engines that can be adopted in individual software provided through its application store to those provided by the designated provider, etc. Such actions include the designated provider requiring, by contract or other means, that individual software adopt the browser engine provided by the designated provider, etc., or prohibiting individual software that adopts alternative browser engines without exception.

(B) Actions **that "Prevent" the Adoption of Alternative Browser Engines**

Actions that prevent the adoption of alternative browser engines refer to conduct that creates a high likelihood of making it difficult for individual app providers to incorporate such engines into their individual software when providing it via a designated provider's application store. Such actions may include: imposing unreasonable technical restrictions on individual app providers while allowing them to adopt alternative browser engines, placing excessive financial burdens on individual app providers for adopting alternative browser engines, and steering smartphone users away from using individual software that incorporates alternative browser engines.

The determination of whether a designated provider's action constitutes "preventing" the adoption of alternative browser engines does not require that it be completely impossible for individual app providers to adopt alternative browser engines. Instead, the determination is made based on the degree of likelihood that such a result will occur.

The degree of likelihood of causing practical difficulty in adopting alternative browser engines is assessed comprehensively based on various factors, including: the nature of the designated provider's actions, the duration of such actions, the impact on individual app providers seeking to adopt alternative browser engines, and the extent of impact on smartphone users utilizing such individual software.

C. Hypothetical Scenarios

(A) Hypothetical scenarios of actions where a designated provider limits the browser engines that can be adopted in individual software provided through its application store to those provided by the designated provider, etc., thus falling under Article 8, Item 3(a) of the Act, include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 96:** A designated provider, in the reviews or examinations for providing individual software via the application store, sets a review item that requires the individual software to adopt the browser engine provided by the designated provider, etc.
- **Hypothetical Scenario 97:** A designated provider, in the reviews or examinations for providing individual software via the application store, sets a review item that prohibits individual software that adopts alternative browser engines without exception.

(B) Hypothetical scenarios of actions where a designated provider, while permitting the adoption of alternative browser engines in relation to its application store, creates a high likelihood of practical difficulty in adopting them, and thus falls under Article 8, Item 3(b) of the Act, include the following:

a. A designated provider imposes unreasonable technical restrictions, contractual terms, or other conditions regarding the adoption of alternative browser engines on individual app providers who adopt or intend to adopt alternative browser engines, in relation to its application store.

Hypothetical Scenarios:

- **Hypothetical Scenario 98:** A designated provider refuses to provide app development tools necessary for individual app providers to distribute their software through the designated provider's application store when they adopt an alternative browser engine.
- **Hypothetical Scenario 99:** A designated provider manipulates the search algorithm in the application store to lower the search ranking of individual software that adopts alternative browser engines or places such software in positions that make discovery by smartphone users more difficult, solely because it adopts an alternative browser engine.
- **Hypothetical Scenario 100:** When a designated provider requires individual app providers to submit applications, etc., for the adoption of alternative browser engines, despite having received an eligible application and a reasonable period for reviews or examinations (taking into account the specific circumstances of the individual app provider) has passed, the designated provider does not provide a sufficient response to the application, etc., thereby preventing the provision of individual software that adopts the alternative browser engine.

b. A designated provider imposes excessive financial burdens regarding the adoption of alternative browser engines on individual app providers who adopt or intend to adopt alternative browser engines, in relation to its application store.

Hypothetical Scenarios:

- **Hypothetical Scenario 101:** A designated provider imposes financial burdens such as excessively high fees on individual app providers who intend to adopt alternative browser engines, creating a high likelihood of making the adoption of alternative browser engines difficult.

c. A designated provider steers smartphone users away from using individual software that incorporates alternative browser engines when smartphone users use or intend to use such individual software, in relation to its application store.

Hypothetical Scenarios:

- **Hypothetical Scenario 102:** A designated provider, from the perspective of providing basic operation software and the application store, repeatedly displays pop-up messages, each time a smartphone user attempts to use individual software that adopts an alternative browser engine, stating that the designated provider, etc.'s browser engine is not adopted in that individual software and asking whether the user wishes to

continue using that individual software.

D. Hypothetical Scenarios of Justifiable Reasons

Based on the basic understanding of the applicability of justifiable reasons in 3 (1) D above, hypothetical scenarios where justifiable reasons are typically recognized and do not constitute violations, and hypothetical scenarios where justifiable reasons are typically not recognized and constitute violations, are as follows:

It should be noted that for individual software other than browsers, when it has the function of displaying web pages as one of its functions, differences in the function related to Browse web page information may arise depending on the adopted browser engine. However, it is necessary to consider that the number of individual software other than browsers is enormous, and using a common browser engine for them can enable rapid and effective countermeasures for ensuring cybersecurity, etc.

(A) Hypothetical Scenario Where Justifiable Reasons are Accepted and Not Considered Violations

Hypothetical scenarios of actions that are typically recognized as having justifiable reasons and are not considered violations of Article 8 include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 103:** In the situation of a very large number of individual software providers distributing non-browser software through the application store, a designated provider standardizes the browser engine used to display web pages through such software to its own browser engine by default. However, for individual app providers seeking to adopt alternative browser engines, the designated provider establishes certain cybersecurity-related requirements (for example whether or not they address vulnerabilities at the same level as the designated provider, or to confirm whether or not parental controls function) and conducts a prior review or examination to assess whether those requirements are met before deciding whether to allow the adoption of the alternative browser engine. This action, while imposing conditions that require the individual software to adopt the browser engine provided by the designated provider, etc., and in the sense that it requires certain requirements to be met when adopting an alternative browser engine, hinders the adoption of such alternative browser engines by individual app providers. On the other hand, the purpose of ensuring cybersecurity, etc., is legitimate. Furthermore, if the designated provider, etc., generally unifies vulnerability

countermeasures for displaying web pages using their browser engine, and if ensuring cybersecurity, etc., would be extremely costly or involve a significant shortage of personnel for security measures unless individual app providers who intend to adopt alternative browser engines are required to meet certain cybersecurity requirements and undergo prior reviews or examinations, it is considered that there are no other less competition-restricting means to achieve that purpose. Therefore, a justifiable reason is recognized, and it does not violate Article 8 of the Act.

(B) Hypothetical Scenarios Where Justifiable Reasons Are Not Accepted and Constitute Violations

Hypothetical scenarios of actions that are typically not recognized as having justifiable reasons and are considered violations of Article 8 include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 104:** An individual app provider develops its own browser engine and implements vulnerability management measures equivalent to those of the designated provider. Despite there being no cybersecurity concerns beyond those already present in software that adopts the designated provider's browser engine, the designated provider refuses to allow the individual app provider to adopt its own browser engine in its software under the justification of ensuring cybersecurity and protecting information related to smartphone users. This action does not qualify as having a justifiable reason because for individual software of individual app providers who develop their own browser engines and implement vulnerability management measures equivalent to those of the designated provider, there is no difference in terms of ensuring cybersecurity, etc., compared to individual software that adopts the designated provider's browser engine, meaning there is no legitimate purpose of ensuring cybersecurity, etc. Therefore, it violates Article 8 of the Act.

E. Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

Designated providers of application stores are required to report to the Japan Fair Trade Commission on the status of their compliance with Article 8, Item 3, including the matters stipulated in Rules Article 36, Paragraph 2. Examples of other necessary information for confirming compliance with the Act under Item 4(c) of the same paragraph include the following:

1. If the designated provider establishes certain criteria and conducts reviews or

examinations as conditions for individual software to adopt alternative browser engines, the criteria for such reviews or examinations, the procedures for conducting them, and the name and content of any related terms and conditions.

2. If the designated provider imposes financial burdens such as fees on individual app providers as conditions for individual software to adopt alternative browser engines, the calculation method of such financial burdens and the reasons for imposing them, and the name and content of any related terms and conditions.

(4) Item 4 (Prohibition of Forcing the Display of User Verification Methods)

A. Basic Approach

Article 8, Item 4 of this Act prohibits designated providers of application stores from making the display of the user verification method they provide a condition for individual app providers to distribute their software through the application store. By preventing designated providers from imposing this requirement, the Act ensures that individual app providers can choose their preferred user verification methods, promoting fair and open competition.

B. Specific Understanding of Article 8, Item 4

(A) User Verification Method

"User verification (meaning the identification of smartphone users by distinguishing him / her from other persons by means of codes or other information when the smartphone users use the individual software)" in Article 8, Item 4 of the Act refers to a method for identifying smartphone users. For example, in individual software that requires membership registration, it refers to a method for identifying smartphone users by requiring them to enter their email address, etc., and in addition, entering a password or biometric information such as fingerprint information as an alternative.

(B) Making the Display of User Verification Methods a "Condition for Providing Individual Software Through the Application Store"

If the terms of use of the application store do not state that displaying the user verification method provided by the designated provider, etc., is a condition for the user verification method related to individual software provided by individual app providers, it does not violate Article 8, Item 4.

On the other hand, even if it is not explicitly stated as a condition in the terms of use of the

application store that displaying the user verification method provided by the designated provider, etc., is required for the user verification method related to individual software provided by individual app providers, if, for example, during the app review or examination process, the designated provider requires individual software that does not display the user verification method provided by the designated provider, etc., to be modified to display it, this would effectively impose a requirement for distribution through the application store, violating Article 8, Item 4.

5. Article 9 (Prohibition of Self-Preferencing in Search Services by Designated Providers)

(1) Basic Approach

Article 9 of this Act prohibits designated providers of search engines and their subsidiaries (hereinafter referred to as "designated providers, etc." in this section) from giving preferential treatment to their own goods or services over competing goods or services without a legitimate reason when displaying search results that smartphone users request through the search service provided by the designated search engine. While providers of search services using search engines implement various innovations in displaying search results to enhance their appeal to smartphone users, which generally promotes fair and open competition in search services using search engines, giving preferential treatment to goods or services provided by designated providers, etc., over competing goods or services without legitimate reason in such search results undermines a fair competitive environment for those goods or services. Therefore, this provision aims to promote competition for those goods or services by prohibiting such preferential treatment.

(2) Specific Understanding of Article 9

A. Understanding "When Displaying Information on Goods or Services Sought by Smartphone Users Through Search"

(A) Regarding "Sought by Smartphone Users Through Search"

"Sought by smartphone users through search" refers to smartphone users conducting searches by manually or vocally entering search queries into a browser's address bar or a search box on a search service provider's website, or by clicking a hyperlink set to display results corresponding to a specific search query, with the aim of satisfying their demand to find information. For example, this refers to a smartphone user planning a trip to Tokyo and searching for accommodation by entering the search query "Tokyo Hotel" when looking for a place to stay.

(B) Regarding "When Displaying Information on Goods or Services Sought by Smartphone Users Through Search"

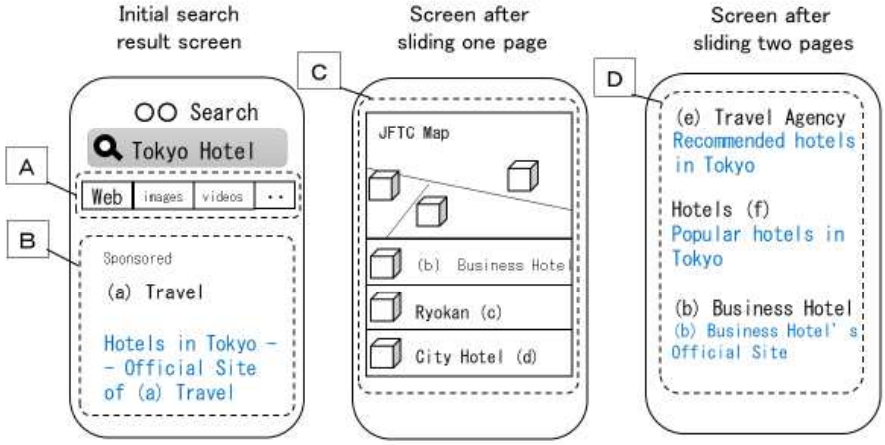
"When displaying information on goods or services sought by smartphone users through search" captures the scenario where information sought by smartphone users is displayed. That is, the screen showing the results of a search performed by a smartphone user is subject to Article 9 of the Act.

(C) Classification of Search Result Displays

General search result displays can be classified as follows:

- **Basic Search Results**: These are search results that display a list of links to the locations of an unspecified number of web pages containing the information sought through the search, ranked by the search engine according to the search query. This corresponds to part D in the figure below.
- **Separate Sections**: These display specific information in a format other than basic search results. This corresponds to part C in the figure below.
- **Search-Linked Advertising**: This primarily displays information related to goods or services desired by advertisers, determined through bidding, as advertisements to the user, to encourage purchases or consumption by smartphone users. This corresponds to part B in the figure below.
- **Tab-Form Links**: These are links provided in a tab format directly below the search box, leading to search services or web pages or individual software that display information sought by smartphone users, limited to specific fields or formats. This corresponds to part A in the figure below.

A: Links to search services, etc., provided in a tab format, limited to specific fields or formats.
B: Search-linked advertisements, noted with "Ad," "Sponsored," etc.
C: Separate frames displaying map services, hotel comparison services, etc., in special formats other than basic search results.
D: Links to numerous unspecified web pages, ranked and displayed according to the search query.



Among these, search-linked advertising (B in the graph) is subject to the Act on Improving Transparency and Fairness of Digital Platforms (Act No. 38 of 2020). If transparency and fairness in transactions related to search-linked advertising are sufficiently ensured by the designated provider based on the provisions of that Act, then scenarios that violate Article 9 of this Act are not anticipated.

On the other hand, a designated provider is in a position to decide on search-linked advertising, other advertisements, and the establishment of separate sections, etc.. Calling a certain display an advertisement does not unconditionally exempt it from Article 9. For example, even if something is labeled "Ad" or "Sponsored," if only information related to the designated provider's own goods or services is displayed, not as a result of fair and non-discriminatory processing as described in B (B) below, it may be recognized as being subject to Article 9, as it would constitute preferential treatment of the designated provider's goods or services over competing goods or services without legitimate reason.

(D) Regarding "Goods or Services"

"Goods or services" should not be interpreted in a particularly limited way. "Goods" include, for example, smartphone devices and their peripherals, as well as individual software. "Services" include, for example, search services (not only search services using a search engine as defined in Article 2, Paragraph 8 of the Act, but also broader search services such as so-called vertical search services that display information sought by smartphone users

limited to specific fields or formats). This also includes services provided in search results such as hotel comparison services, shopping comparison services, flight comparison services, and map information provision services, as well as hotel accommodation services and air transport services that are the subject of comparison services.

B. Understanding "Preferential Treatment of Goods or Services Provided by the Designated Provider, etc., Over Other Competing Goods or Services"

(A) Regarding "Other Competing Goods or Services" in Relation to Goods or Services Provided by the Designated Provider, etc.

Regarding preferential treatment related to goods or services provided by designated providers, etc., the comparison target is other goods or services that are in a competitive relationship with the goods or services provided by those designated providers, etc.. "Other goods or services in a competitive relationship" refers to goods or services of the same type from the perspective of smartphone users as the goods or services provided by the designated provider, etc..

Therefore, in determining the application of Article 9 of the Act, it will be necessary to identify the goods or services provided by the designated provider, etc., and confirm whether preferential treatment is given to those goods or services in relation to other competing goods or services.

(B) Regarding Preferential Treatment

Even if goods or services provided by designated providers, etc., which a designated provider offering search services using a search engine intends to make smartphone users aware of, purchase, consume, or use through their display in search results, are displayed in a position or by a method that is evaluated as being more easily recognized or selected by smartphone users compared to other goods or services in a competitive relationship with them, it does not constitute preferential treatment as stipulated in Article 9 of the Act if the setting of the search engine's search algorithm for displaying search information and the processing using it are fair and non-discriminatory (including cases where those goods or services are displayed within a separate section as a result of fair and non-discriminatory search algorithm settings and processing). This is considered a result of competition on the merits.

On the other hand, if information related to the designated provider's goods or services is displayed in a position or by a method that is evaluated as being more easily recognized or

selected by smartphone users, through arbitrary search algorithm settings or the establishment of separate sections that display only information related to the designated provider's goods or services (including cases where other goods or services in a competitive relationship with the designated provider's goods or services are displayed in a position or by a method that is evaluated as being less easily recognized or selected by smartphone users, thereby relatively making the designated provider's goods or services more easily recognized or selected), this constitutes preferential treatment as stipulated in Article 9 of the Act.

Furthermore, a display in a position evaluated as being more easily recognized or selected by smartphone users includes, for example, placement higher than the display order determined fairly and non-discriminatorily. A display by a method evaluated as being more easily recognized or selected by smartphone users includes, for example, manipulating font sizes or the visibility of text color in relation to background color.

(C) Regarding Processing Using Search Algorithms for Displaying Search Information

If the criteria of the search algorithm itself are unfair or discriminatory and set to favor the designated provider's goods or services, then the setting itself is recognized as preferential treatment of the designated provider's goods or services. Specifically, if a designated provider includes specific parameters in its search engine's algorithm that favor its own goods or services (e.g., elements that only apply to video services provided by that designated provider), thereby giving an advantage to its goods or services over other competing goods or services in the display of search results, this constitutes preferential treatment as stipulated in Article 9 of the Act.

Furthermore, the act causing preferential treatment of the designated provider's goods or services when displaying search information is not necessarily limited to actions taken at the time of displaying search results. Search services using a search engine are provided by first collecting information from web pages by a program called a crawler (crawling) and registering the collected information into a database (indexing) as a preparatory stage. Then, information from the index is referenced in response to the user's search query, and links to web pages are output in a ranked format based on their relevance to the search query, along with separate sections, etc.. For example, even if fair and non-discriminatory treatment is performed in the search algorithm for displaying basic search results for a certain search query, if only data related to the designated provider, etc., is crawled and indexed in the crawling and indexing process, which is a prerequisite for displaying basic search results, thereby treating the designated provider, etc.'s goods or services favorably, this constitutes preferential treatment

as stipulated in Article 9 of the Act.

(D) Regarding Separate Sections in Search Results Display

The method of displaying search results in search services is one of the competitive means among providers of search services using a search engine. Therefore, the establishment of a separate section in the display of search results does not immediately constitute preferential treatment as stipulated in Article 9 of the Act. Furthermore, if goods or services provided by the designated provider, etc., are displayed alongside other goods or services in a competitive relationship with them within a separate section, and these goods or services are displayed as a result of fair and non-discriminatory search algorithm settings and processing, it does not constitute preferential treatment as stipulated in Article 9 of the Act.

However, if only information related to the designated provider's goods or services is displayed as a separate section, and it is positioned higher or in a more prominent format than search results that would be displayed based on fair and non-discriminatory ranking, or conversely, if other goods or services in a competitive relationship with those goods or services are positioned lower or in a less visible format than search results that would be displayed based on fair and non-discriminatory ranking, this constitutes preferential treatment as stipulated in Article 9 of the Act.

Moreover, even if a separate section displaying only information related to the designated provider's goods or services is displayed along with basic search results that are ranked fairly and non-discriminatorily, separate sections are often set up to be more easily recognized or selected by smartphone users compared to basic search results, due to their size, color scheme, or other display methods. Therefore, establishing such a separate section and displaying only information related to the designated provider's goods or services in that separate section may itself constitute preferential treatment as stipulated in Article 9 of the Act.

Furthermore, there may be cases where a separate section is displayed with other businesses as the information source and this is indicated. However, if the display format suggests that the separate section is displayed as a service of the designated provider, etc., it will be subject to Article 9 of the Act.

It should be noted that if a mechanism is adopted for a separate section displaying only information related to the designated provider's goods or services that allows smartphone users to autonomously choose to display or hide it with simple operations, this will be a factor

to consider when determining whether the display of that separate section constitutes preferential treatment as stipulated in Article 9 of the Act.

(E) Hypothetical Scenarios of Preferential Treatment

Examples of search result displays by designated providers that constitute preferential treatment as stipulated in Article 9 of the Act include the following:

Hypothetical Scenarios:

- **Hypothetical Scenario 105:** Locking in place the display of a download prompt for the designated provider's app store at the top of search results when a user enters the name of a specific individual software as a search query.
- **Hypothetical Scenario 106:** Locking in place the display of information about a service of the designated provider that is of the same type as another service as an advertisement at the top of search results when a user enters the name of that other service as a search query.
- **Hypothetical Scenario 107:** Creating a separate section for displaying news, where only the designated provider's news service is shown, while ensuring that other web pages providing news content do not appear in that section.

C. Understanding the Concept of "Without Legitimate Reason"

(A) Basic Approach to Legitimate Reason

Even if an action constitutes preferential treatment as stipulated in Article 9 of the Act, it will not violate the provisions of that Article if there is a legitimate reason for such treatment (written as "justifiable reason" in the Act). The determination of whether a legitimate reason exists for preferential treatment is made in light of the purpose of such preferential treatment (the purpose should not merely be desirable for business operations, but should be justified from the perspective of Article 9, which aims to promote competition between the goods or services provided by the designated provider, etc., and other competing goods or services), and the availability and nature of other less competition-restricting alternative means to achieve that purpose.

It is difficult for external parties to accurately ascertain how search results are displayed, including the content of the search algorithm. Therefore, the designated provider must provide a concrete and detailed explanation of such "legitimate reason" to the Japan Fair Trade Commission through compliance reports under Article 14 of the Act, etc. (see (4) below).

(B) Understanding Related to the Quality of Search Services for Smartphone Users Regarding Legitimate Reason

Regarding preferential treatment, it is conceivable that an explanation will be provided concerning the improvement of the quality of search services for smartphone users, including the responsiveness and accuracy that smartphone users expect from search services using a search engine. For example, if the explanation for the improvement of search quality for smartphone users due to such preferential treatment is unclear or abstract, if the preferential treatment is performed with the intent to exclude other goods or services in a competitive relationship with the designated provider's goods or services, if other goods or services are unjustly treated in an inferior position, or if the preferential treatment is not reasonable and necessary for improving the quality, a legitimate reason is not recognized.

Furthermore, if the improvement in search service quality for smartphone users is not concretely and specifically demonstrated, and the explanation remains abstract, it becomes difficult to consider it when determining the existence of a legitimate reason. Also, while the improvement in quality may be explained in relation to a single change in the method of displaying search results, it may also be explained in relation to multiple sufficiently related changes. In any case, it becomes possible to consider the existence of a legitimate reason in the judgment only when the improvement in quality is concretely and specifically demonstrated.

Information for explaining such quality improvement may be obtained through tests conducted with smartphone users, and a concrete and detailed explanation of quality improvement may be provided based on the results of such tests. Designated providers providing such explanations are required to pre-determine the content to be measured by such tests, conduct these tests in major cases where the method of displaying search results is changed, and qualitatively analyze or quantify the results in an objectively verifiable manner. In this regard, such tests cannot be considered effectively tested unless they are carefully designed not to favor designated providers, etc.. Furthermore, if the content of the tests is not demonstrated in an objectively verifiable manner, it is difficult to determine whether they were effectively tested, making it difficult to consider them in the judgment of whether a legitimate reason exists.

(C) Regarding Restricting the Display of Specific Web Pages

In the provision of search services using a search engine, there may be cases where a specific web page is removed from search results, its display content is restricted, or its display ranking is lowered, due to reasons such as a high probability of harming the safety of smartphone

users. While such measures are taken to protect the safety of smartphone users, the goods or services provided on or through that web page may be treated in an inferior position, leading to a relative preferential treatment of the designated provider's goods or services that are in a competitive relationship.

In such cases, if the response to each web page, etc., is conducted unfairly or discriminately, such as continuing to display web pages related to the designated provider's goods or services that have similar problems, while preventing other businesses' web pages from being displayed in search results, a legitimate reason is not recognized. On the other hand, if there is a recognized need for measures to ensure the safety of smartphone users, and if there are no other less competition-restricting alternative means than such measures, a legitimate reason is recognized.

For example, preferential treatment carried out for the following purposes is generally recognized as having a legitimate reason:

Hypothetical Scenarios:

- **Hypothetical Scenario 108:** If it is discovered that a web page of another business providing a certain good or service has been hacked with malicious content due to security vulnerabilities, and for the purpose of ensuring cybersecurity for smartphone use, the web page is manipulated to not appear in search results until the issue is resolved, resulting in the web page providing the designated provider's competing goods or services being relatively displayed higher.
- **Hypothetical Scenario 109:** If a web page of another business providing a certain good or service contains information related to smartphone users without their consent, or includes deepfake videos of their faces, and for the purpose of protecting information related to smartphone users, the web page is manipulated to not appear in search results based on a request from the user, resulting in the web page providing the designated provider's competing goods or services being relatively displayed higher.
- **Hypothetical Scenario 110:** For the purpose of preventing the display of web pages that violate laws, if a web page selling intellectual property-infringing counterfeit goods is not displayed, resulting in the web page providing the designated provider's genuine goods being relatively displayed higher.

(D) Regarding Cases Where Goods or Services of the Designated Provider, etc., are Treated in a Higher or More Prominent Position Than Original Search Results

If, in basic search results, a web page related to the designated provider's goods or services is displayed higher than the original search results due to search algorithm settings, or if only displays related to goods or services provided by the designated provider, etc., are handled in a separate section, the existence of a legitimate reason will be judged in light of the purpose of such search algorithm settings or the establishment of such separate sections, and the availability and nature of other less competition-restricting alternative means to achieve that purpose.

For example, a purpose for establishing a separate section could be the need to provide accurate information in emergencies to ensure the safety of smartphone users. In such cases, preferential treatment carried out for the following purposes is generally recognized as having a legitimate reason:

Hypothetical Scenarios:

- **Hypothetical Scenario 111:** If, in a disaster, the designated provider, etc., displays information related to earthquakes or tsunamis, etc., and there is a high possibility of significant harm to the life or body of smartphone users if they cannot quickly browse accurately guaranteed information in the search results display, the designated provider, etc., displays its own information at the top, citing that it has been confirmed as information from a public institution, etc., for the purpose of ensuring the safety of users.

(3) Desirable Practices by Designated Providers to Avoid Violations

Article 9 of the Act targets search services using a search engine, which are services whose mechanisms are not easily verifiable by third parties. Therefore, ensuring transparency is important.

First, it is desirable for designated providers to disclose in a manner understandable to website operators, the main parameters used for setting the search algorithm that determines rankings, and the reasons for different treatment in search results between information related to the designated provider's goods or services and information related to other competing goods or services, in order to prevent actions that violate the provisions of the Act. To ensure that website operators can understand, it is desirable not only to simply list the parameters that determine display order, but also to explain the differences in importance between the parameters when actually determining display order. Furthermore, if there are changes to the parameters or their importance in determining display order, it is desirable to disclose the

content of such changes without delay.

Additionally, if only information related to the designated provider's goods or services is displayed as a separate section in search results, it is desirable to allow smartphone users to choose whether to display or hide potentially preferential displays, according to their wishes, from the perspective of ensuring smartphone users' autonomous choice.

If tests are conducted with smartphone users to evaluate the improvement in search service quality for smartphone users due to preferential treatment, it is desirable for designated providers to make the results public as much as possible, from the perspective of ensuring transparency.

Furthermore, the Act aims to promote fair and open competition related to specified software. In the display of search results for basic operation software, application stores, and browsers other than search services using a search engine, it is desirable to display search results that promote such competition from the perspective of that purpose. For example, in the display of search results corresponding to search queries seeking alternative application stores, displaying a list of alternative application stores in a separate section could be considered.

(4) Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

Designated providers of search engines are required to report to the Japan Fair Trade Commission on the status of their compliance with Article 9, including the matters stipulated in Rules Article 36, Paragraph 2. Examples of other necessary information for confirming compliance with the Act under Item 4(c) of the same paragraph include the following:

1. The following matters related to basic search results.
   A) Explanation regarding the main parameters of the algorithm that determines rankings (including explanations regarding the differences in impact of those parameters on the display of basic search results).
   B) If there have been changes to the main parameters of the ranking algorithm that have a significant impact on overall basic search results, other than measures for complying with Article 9 as stipulated in Rules Article 36, Paragraph 2, Item 1, since the submission of the previous year's compliance report, the outline of such changes and the presence or absence of tests conducted with smartphone users regarding those changes.
   C) If the designated provider's goods or services have been preferentially treated in search results due to the setting of the main parameters of the ranking algorithm, a

concrete and detailed explanation of the purpose and content of such preferential treatment and the existence of a legitimate reason for such preferential treatment.

2. The following matters related to separate sections (limited to those pre-notified by the Japan Fair Trade Commission to the designated provider).
   A) The name of each separate section. In addition, attach an example image of the display screen for each separate section with a serial number.
   B) Explanation regarding the conditions under which the separate section is displayed, such as typical search queries that trigger its display.
   C) The purpose of establishing the separate section.
   D) Whether the separate section displays only information related to the designated provider's goods or services.
   E) If smartphone users can choose to display or hide the separate section, the method of selection, such as by pressing the "×" mark displayed on the separate section or by operating from the settings screen.
   F) If the separate section has been modified since the submission of the previous year's compliance report, other than measures for complying with Article 9 as stipulated in Rules Article 36, Paragraph 2, Item 1, the outline of such modification and the presence or absence of tests conducted with smartphone users regarding that modification.
3. The following matters related to tab-form link displays (limited to those pre-notified by the Japan Fair Trade Commission to the designated provider).
   A) The name of each tab. In addition, attach an example image of the display screen for each tab.
   B) Explanation regarding the conditions under which the tab is displayed, such as typical search queries that trigger its display.
   C) The purpose of establishing the tab.
   D) If the tab has been modified since the submission of the previous year's compliance report, other than measures for complying with Article 9 as stipulated in Rules Article 36, Paragraph 2, Item 1, the outline of such modification and the presence or absence of tests conducted with smartphone users regarding that modification.

6. Article 10 (Measures Related to the Disclosure of Conditions for Acquiring Data)

(1) Disclosure of Conditions for Acquiring Data, etc., to Businesses

A. Basic Approach

Article 10 of this Act seeks to resolve the difficulty in externally verifying how designated providers (those designated for their basic operation software, application store, or browser;

hereinafter the same in this section) use acquired data by requiring them to disclose the conditions under which they obtain or use data (including causing their subsidiaries, etc., to use such data; hereinafter the same in this section), as well as the conditions for data acquisition by businesses using specified software (referring to basic operation software, application stores, or browsers; hereinafter the same in this section). This aims to ensure compliance with the prohibited conduct set forth in Article 5 regarding the unjust usage of acquired data.

Additionally, by enhancing transparency in transactions conducted through specified software by disclosing the conditions for data acquisition or usage by designated providers to both individual app providers, etc., utilizing specified software and smartphone users, and by making it easier for individual app providers, etc., to acquire data by disclosing the conditions for their data acquisition, Article 10 is expected to contribute to the promotion of innovation.

B. Regarding Data Covered by Disclosure

Based on the intent that Article 10, Paragraph 1, Items 1 to 3, aims to ensure compliance with Article 5, which prohibits the unjust usage of data acquired by designated providers, the data for which designated providers must disclose the conditions for acquisition or usage to individual app providers or website operators are specified in Rules Articles 19 to 21 as the data subject to Article 5, Items 1 to 3. It should be noted that disclosing the conditions for acquisition or usage of more types of data than those stipulated in each item of Article 5 is not prohibited.

C. Regarding Disclosure Methods

The methods of disclosure for the conditions of data acquisition, etc., to individual app providers or website operators are stipulated in Rules Article 18, Items 1 and 2, as being written in clear and simple language for other individual app providers or other website operators, and being easily accessible at any time both before and during the use of the basic operation software or application store provided by the designated provider by other individual app providers, or before and during the use of the browser provided by the designated provider by other website operators. In line with the basic understanding in A above, it is important that the conditions for data acquisition, etc., are easily understandable and verifiable by individual app providers or website operators. Therefore, it is required that the information is placed in an easily recognizable location on the designated provider's website, and if there are revisions to terms and conditions that significantly affect the business activities of individual app providers or website operators, the revision history is also posted as necessary, ensuring that

the information is always accessible in a way that is easy for individual app providers or website operators utilizing specified software to understand. Furthermore, it is desirable that the content of the data acquired, etc., be disclosed in a way that is easily understandable to individual app providers, website operators, and smartphone users, and that allows for easy external verification of the data acquisition, etc., status.

Additionally, since the Act anticipates the smartphone market in Japan, Rules Article 18, Item 3 stipulates that if the conditions for data acquisition, etc., are prepared in a language other than Japanese, a Japanese translation must be attached. It is desirable for the Japanese translation to be disclosed simultaneously with the disclosure of the conditions. However, if it is unavoidable that a Japanese translation cannot be attached at the time of disclosure, the designated provider is required to explicitly state a reasonable deadline at the time of disclosure and ensure that the Japanese translation is disclosed by that deadline (proviso of the same item).

D. Regarding Contents of What is Disclosed

Based on Article 10, Paragraph 1 of the Act, designated providers are obliged to disclose the conditions for data acquisition and usage, including the content of the data, as well as the conditions for data acquisition by individual app providers or website operators, in relation to data acquired through the use of specified software by individual app providers or website operators.

(A) Regarding Conditions for Data Acquisition by Designated Providers

Examples of the content of conditions for data acquisition by designated providers include the following:

- Content of data acquired through specified software and the purpose of acquisition.
- Method of acquiring the aforementioned data.

(B) Regarding Conditions for Data Usage by Designated Providers

a. Examples of the content of conditions for data usage by designated providers include the following:

- Content and purpose of usage of data acquired by the designated provider (or its subsidiaries, etc.).
- Data management framework for acquired data.

b. In line with the intent of Article 10, which aims to ensure compliance with Article 5 prohibiting the unjust usage of acquired data, a data management framework operated by a designated provider to prevent the use of acquired data for its own (or its subsidiaries', etc.) goods or services that are in a competitive relationship with goods or services provided by individual app providers or website operators, could include the following measures:

1. Organizational measures such as establishing a firewall between the data management department and the goods or services development department.
2. Technical measures such as access control to data in the data management department and goods or services development department.
3. Internal regulations regarding data storage periods in departments where data is shared (including sharing within the designated provider and with external parties if shared externally), departments that acquire data, and departments that receive shared data.
4. Internal regulations such as mechanisms (internal audits) that can detect and correct the possibility of unjust usage of acquired data in each decision-making process related to the development or provision of goods or services.
5. Measures that enable external or third-party verification, such as storing data access logs and records of the operation status of internal regulations, and evaluation of the data management framework by a third-party organization.
6. Establishment of a complaint consultation desk and publication of its contact information if established.

c. Article 10 of the Act does not oblige the establishment of a data management framework as described above. However, it is desirable to take such measures to prevent the use of data in violation of Article 5. If the aforementioned data management framework is established, it is required to be disclosed within a scope that does not hinder the business activities of the designated provider and related businesses. Through this disclosure, it is expected that compliance with Articles 5 and 10 of the Act can be confirmed.

(C) Regarding Conditions for Acquisition by Individual App Providers or Website Operators

Examples of the content of conditions for data acquisition by individual app providers or website operators include the following:

- Whether individual app providers or website operators can acquire data acquired by the designated provider in relation to individual software or websites they provide.
- Content of data if acquisition is possible.
- Method of acquisition and format of data provision if acquisition is possible.

- If an application is required for acquisition, the processing period for such application (period for responding to the application regarding data acquisition eligibility, period until data is provided if acquisition is possible, etc.).

Furthermore, it is desirable to disclose whether the designated provider can directly provide (directly transfer) data to a party designated by the individual app provider or website operator, without going through that individual app provider or website operator, and the method if it is possible.

(2) Disclosure of Conditions for Acquiring Data, etc., to Smartphone Users

A. Basic Approach

Article 10, Paragraph 2 of the Act aims to improve the situation where smartphone users have difficulty in recognizing what data is being acquired when using individual software or Browse websites through specified software, by disclosing to smartphone users utilizing specified software the conditions regarding the designated provider's data acquisition or usage. Through the promotion of rational and autonomous use or selection of specified software by those users, it aims to encourage compliance with Article 5 of the Act, which prohibits the unjust usage of data acquired by designated providers, and thereby protect the interests of individual app providers or website operators.

B. Regarding Data Covered by Disclosure

In light of the basic understanding in A above, the data for which designated providers must disclose the conditions for acquisition or usage to smartphone users are stipulated in each item of Rules Article 22 as data related to smartphone users and data generated or provided when smartphone users use individual software or browse web pages, among the data subject to each item of Article 5 of the Act.

C. Regarding Disclosure Methods

The methods of disclosure for the conditions of data acquisition, etc., to smartphone users are stipulated in Rules Article 23, Items 1 and 2, as being written in clear and simple language for smartphone users, containing content that allows smartphone users to easily understand the status of data acquisition and usage by designated providers, and being easily accessible at any time both before and during the use of specified software listed in Article 10, Paragraph 1, Items of the Act provided by the designated provider. In line with the basic understanding in A above, it is required that the information is placed in an easily understandable location when

operating the smartphone, and if there are revisions to terms and conditions that have a significant impact on smartphone users, the revision history is also posted as necessary, ensuring that the information is always accessible in a way that is easy for smartphone users utilizing specified software to understand. Furthermore, considering that smartphone users do not necessarily have sufficient specialized knowledge compared to individual app providers or website operators, it is required to disclose content that is easily understandable to those users.

Additionally, since the Act anticipates the smartphone market in Japan, Rules Article 23, Item 3 stipulates that if the conditions for data acquisition, etc., are prepared in a language other than Japanese, a Japanese translation must be attached. It is desirable for the Japanese translation to be disclosed simultaneously with the disclosure of the conditions. However, if it is unavoidable that a Japanese translation cannot be attached at the time of disclosure, the designated provider is required to explicitly state a reasonable deadline at the time of disclosure and ensure that the Japanese translation is disclosed by that deadline (proviso of the same item).

D. Regarding Contents of What is Disclosed

The content of disclosure to smartphone users is the same as that for information related to data usage by those users, as described in (1) D (excluding (C)) above.

(3) Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

Designated providers are required to report to the Japan Fair Trade Commission on the status of their compliance with Articles 5 and 10 of the Act, including the matters stipulated in Rules Article 36, Paragraph 2. Examples of other necessary information for confirming compliance with the Act under Item 4(c) of the same paragraph include the following:

1. Outline of data acquired by the designated provider through the use of specified software by individual app providers or website operators, and data used by the designated provider.
2. Explanation regarding the data management framework of the designated provider concerning acquired data, and the basis for the effectiveness of that data management framework in complying with Articles 5 and 10 of the Act.
3. Outline of the audit system and implementation status if the designated provider conducts internal audits or external audits by a third-party organization concerning the

data management framework in (2) (including cases where no problems were found in the audit or evaluations by a third-party organization).

4. Processing standards for data acquisition applications by individual app providers or website operators, and an outline of the status of data acquisition applications and their processing by individual app providers or website operators.

7. Article 11 (Measures Related to the Transfer of Acquired Data)

(1) Basic Approach

Article 11 of this Act obliges designated providers (those designated for basic operation software, application stores, or browsers; hereinafter the same in this section) to implement necessary measures to ensure that smartphone users' data – acquired through specified software (basic operation software, application store, or browser; hereinafter the same in this section) – can be seamlessly transferred to the user or a designated recipient upon the user's request. This provision aims to facilitate users switching to other business operators' services and promote competition among specified software.

(2) Designated Recipients by Smartphone Users

Article 11 includes not only smartphone users but also parties designated by smartphone users (hereinafter referred to as "third parties" in this section) as recipients for the seamless transfer of data. Examples of such third parties include other specified software providers to which the user is switching, OEM manufacturers (device manufacturers other than the designated provider that manufacture and sell smartphones with the designated provider's basic operation software incorporated), and businesses that provide individual software for data transfer, etc.. Methods for directly providing data to these businesses include cable connections, cloud services, and API-based methods.

(3) Methods for Seamless Data Transfer

A. Ensuring Data Transfer Availability

From the perspective of ensuring data transfer availability as a method for seamless data transfer, Rules Article 24, Item 1 stipulates that designated providers must ensure that smartphone users can request the transfer of transfer-eligible data (data prescribed in Rules Article 25 to Article 27; hereinafter the same in this section (3)) at any time. For example, if data transfer is only possible at very limited times, despite there being no reasonable grounds such as temporary service suspension necessary for ensuring cybersecurity, etc., it does not meet the requirements of this item. On the other hand, if a smartphone user engages in actions

contrary to the purpose of Article 11, such as frequently requesting data transfer and overloading the server regardless of the timing of switching specified software, it is permissible from the perspective of this item even if the transfer of transfer-eligible data is not permitted each time.

B. Ensuring Ease of Data Transfer Operations

From the perspective of ensuring ease of data transfer operations as a method for seamless data transfer, Rules Article 24, Item 2 stipulates that designated providers must ensure that smartphone users can transfer transfer-eligible data through simple operations. For example, if the operation to transfer transfer-eligible data cannot be completed solely through smartphone operations, or if it requires unnecessary multiple transitions between web pages, the measures do not meet the requirements of this item.

C. Ensuring Data Up-to-dateness and Format Versatility

From the perspective of ensuring data up-to-dateness and format versatility as a method for seamless data transfer, Rules Article 24, Item 3 stipulates that designated providers must ensure that the transfer-eligible data requested by smartphone users remains up to date and is formatted in a widely used format. For example, if smartphone users can only receive transfer-eligible data that is several months or more older than the current date, or if transfer-eligible data can only be received in a format that is difficult for other specified software providers to use, the measures do not meet the requirements of this item. On the other hand, for example, providing APIs that allow real-time access to transfer-eligible data requested by smartphone users to other specified software providers, smartphone manufacturers that provide individual software for data transfer, etc., or providing interoperable data formats that allow smartphone users to easily transfer data to such third parties, can be said to meet the requirements of this item.

D. Ensuring Reasonableness of Data Transfer Duration

From the perspective of ensuring reasonableness of data transfer duration as a method for seamless data transfer, Rules Article 24, Item 4 stipulates that the duration required to transfer transfer-eligible data does not exceed a reasonable period. For example, if transfer-eligible data is transferred beyond the standard period generally considered necessary after a smartphone user requests its transfer, despite the absence of technical constraints, etc., the measures do not meet the requirements of this item.

E. Ensuring Reasonableness of Data Transfer Fees

From the perspective of ensuring reasonableness of data transfer fees as a method for seamless data transfer, Rules Article 24, Item 5 stipulates that if a designated provider imposes fees for the transfer of transfer-eligible data, those fees must not exceed a reasonable range. For example, if no fees are set for the transfer of transfer-eligible data and it is performed free of charge, it can be said to meet the requirements of this item. On the other hand, for example, even if no fees are set for the transfer of transfer-eligible data, it is desirable to avoid requiring registration for some paid service provided by the designated provider as a prerequisite for requesting the transfer of transfer-eligible data.

F. Ensuring Cybersecurity, etc., for Data Transfers

From the perspective of ensuring cybersecurity, etc., for data transfers as a method for seamless data transfer, Rules Article 24, Item 6 stipulates that data transfers must implement encryption and other necessary security measures from the perspective of ensuring cybersecurity, etc., as stipulated in the proviso of Article 7 of the Act. It is desirable to adopt highly confidential methods for encrypting transfer-eligible data, such as end-to-end encryption. Furthermore, since transfer-eligible data may include sensitive information such as smartphone user account information and payment data, it is desirable for responses to be taken, such as adopting even more confidential methods depending on the type of transfer-eligible data.

It can also be said that necessary warnings issued by the designated provider to smartphone users requesting data transfer regarding the risk of information leakage, loss, or damage associated with the data transfer meet the requirements of this item.

Furthermore, when directly transferring transfer-eligible data to a third party, it is permissible from the perspective of this item for the designated provider to conduct a review from the perspective of whether the third party has sufficiently implemented measures for ensuring cybersecurity, etc.. If, as a result of such a review, it is determined that there is a problem from the perspective of ensuring cybersecurity, etc., regarding the transfer of transfer-eligible data to that third party, it is permissible from the perspective of this item for the designated provider not to transfer transfer-eligible data to that third party (i.e., to transfer transfer-eligible data only to the smartphone user).

On the other hand, if the aforementioned review of a third party is arbitrary, it becomes difficult to achieve seamless transfer of transfer-eligible data to that third party. Therefore, if a

designated provider conducts the aforementioned review, it is desirable to create and publicly disclose review items with reasonable content in advance, and to ensure fair and non-discriminatory operation based on those review items.

(4) Transfer-Eligible Data

Each item of Article 11 of the Act refers to "data acquired by the designated provider," and the purpose is to exclude data that is entirely impossible for the designated provider to transfer from the scope of transfer obligations, from the perspective of feasibility of compliance with the Act. Data stipulated in the Rules among "data acquired by the designated provider" is subject to transfer obligations, and specific examples are as described in A to C below. The scope of "data useful for using other specified software" (Rules Article 25, Item 3; Article 26, Item 3; and Article 27, Item 2) is determined after comprehensively considering smartphone user needs, the burden on the designated provider to enable data transfer, changes in technology in the specified software field, and the actual efforts of related businesses (including OEM manufacturers), etc..

A. Specific Examples of Data for Basic Operation Software

Examples of data related to basic operation software eligible for seamless transfer, as prescribed in Rules Article 25, include the following data acquired by the designated provider:

(A) Data related to phone calls and internet usage on smartphones equipped with the designated basic operation software:

- Contacts data
- Call history data
- eSIM data

(B) Data related to smartphone settings using smartphones equipped with the designated basic operation software:

- Display settings data
- Home screen layout data

(C) In addition to (A) and (B) above, data useful for using basic operation software provided by other businesses:

- Email account data
- Message data
- List of installed individual software data
- Photos, videos, and album data
- Calendar data

- Wallpaper data
- Password-related data

B. Specific Examples of Data for Application Stores

Examples of data related to application stores eligible for seamless transfer, as prescribed in Rules Article 26, include the following data acquired by the designated provider:

(A) Data related to individual software incorporated into smartphones through the designated application store:

- Download and purchase history data of paid individual software
- Download history data of free individual software

(B) Data related to smartphone users for using the designated application store:

- Account data such as email address, payment methods, and age verification information

(C) In addition to (A) and (B) above, data useful for using application stores provided by other businesses:

- Data input or registered by smartphone users

C. Specific Examples of Data for Browsers

Examples of data related to browsers eligible for seamless transfer, as prescribed in Rules Article 27, include the following data acquired by the designated provider:

(A) Data related to Browse web pages using the designated browser:

- Bookmark data
- Browsing history data

(B) In addition to (A) above, data useful for using browsers provided by other businesses:

- List of installed extensions data
- Credit card information data
- Password-related data

(5) Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

Designated providers are required to report to the Japan Fair Trade Commission on the status of their compliance with Article 11, including the matters stipulated in Rules Article 36, Paragraph 2. Examples of other necessary information for confirming compliance with the Act under Item 4(c) of the same paragraph include the following:

- An explanation of how ensuring data transfer availability, ease of data transfer operations, up-to-dateness of data and versatility of format, reasonableness of data transfer duration, reasonableness of data transfer fees, and cybersecurity for data transfers, etc., are sufficiently ensured for the necessary measures to seamlessly transfer data, along with supporting evidence that these are sufficiently ensured.

8. Article 12 (Measures Related to Default Settings, etc.)

(1) Basic Approach

Article 12 of this Act obliges designated providers of basic operation software or browsers to implement necessary measures to ensure that default settings related to their basic operation software or browsers can be changed through simple operations. It also obliges them to implement measures that contribute to smartphone users' selection, such as displaying multiple individual software options or service options of the same type that can be set as default. Furthermore, designated providers of basic operation software are obliged to implement necessary measures to obtain smartphone user consent when additionally installing individual software provided by the designated provider or its subsidiaries (hereinafter referred to as "designated providers, etc." in this section) onto the smartphone, and to enable users to delete such individual software through simple operations. This is because smartphone users tend to continue using individual software such as browsers and search apps (individual software used for entering search queries to receive search services using a specific search engine; hereinafter the same) that are installed and set as default on their smartphones, and to use search services that are set as default in browsers. Therefore, this provision aims to promote competition among such individual software or services by ensuring opportunities for selection for those users and making it easier for them to switch between individual software or services.

(2) Article 12, Item 1(a)

A. "Default Settings for Basic Operation Software"

"Default settings relating to the basic operation software" in Article 12, Item 1(a) refers to settings where specific individual software (sometimes referred to as "apps;" hereinafter the same in this section) is automatically selected and launched by the basic operation software (hereinafter simply referred to as "default settings" in this section (2) and (3)). Specifically, for example, when a smartphone user clicks a link (URL) to a web page displayed on the smartphone screen, a specific browser is launched by the control of the basic operation software, and the web page at that link is displayed, without the user having to actively select a specific browser each time.

In addition to the above example, such default settings also include cases where a part of the basic operation software's function itself launches specific individual software (for example, when text, images, or other displayed content on the smartphone screen are read by a part of the basic operation software's function, and that function launches a specific search app to display search results related to that displayed content). It should be noted that if individual software provided by designated providers, etc., does not launch as a default setting, the designated provider is not obliged to take the necessary measures related to Article 12, Item 1(a) of the Act for that individual software. Furthermore, the individual software that can be selected as a default setting only needs to include those installed on the smartphone.

B. Necessary Measures for Changing Default Settings

Regarding the measures to be taken by designated providers of basic operation software, Article 12, Item 1(a) stipulates that if individual software provided by the designated provider, etc., launches as a default setting, necessary measures must be taken to enable smartphone users to change that default setting through simple operations. Rules Article 28, Paragraph 1, stipulates three minimum requirements for such measures in each item.

(A) Ease of Finding the Operation Screen for Changing Default Settings

As the first requirement for necessary measures for changing default settings, Rules Article 28, Paragraph 1, Item 1 stipulates that the screen for changing default settings for individual software subject to default settings (hereinafter referred to as "operation screen" in this section (2) and (8) A) must be centralized in a single location or otherwise arranged in a way that ensures smartphone users can easily find it. For example, if it takes many operations or a considerable amount of time to reach the operation screen, the measures do not meet the requirements of this item.

Furthermore, for major individual software (e.g., phone apps, email apps, messaging apps, browser apps, map apps, wallet apps may be applicable) that are frequently used by smartphone users and for which users tend to continue using the default-set individual software unless the default settings can be changed with simple operations, it is required that a category where individual software subject to default settings is collectively displayed is provided in the smartphone's settings app, and that default settings can be changed centrally from that category, so that users can easily find the operation screen. However, if there is a more appropriate method for smartphone users to easily find the operation screen, adopting that method is also permissible from the perspective of this item.

(B) Explanation on the Operation Screen

As the second requirement for necessary measures for changing default settings, Rules Article 28, Paragraph 1, Item 2 stipulates that an explanation regarding the ability to change default settings must be provided on the operation screen. It is assumed that some smartphone users have sufficient knowledge about default settings, etc., related to smartphones, while others may not. Therefore, the content to be described on the operation screen must be such that any smartphone user can understand that they can change default settings on that operation screen.

(C) Changing Default Settings with Minimum Necessary Operations

As the third requirement for necessary measures for changing default settings, Rules Article 28, Paragraph 1, Item 3 stipulates that smartphone users must be able to change default settings with the minimum number of required operations. For example, if default settings can be changed only by operations such as tapping to select the icon of each individual software displayed as an option on the operation screen, selecting a radio button placed next to the icon of each individual software, or sliding a slide button placed next to the icon of each individual software to select it, it can be said to meet the requirements of this item. On the other hand, if changing default settings requires navigating through multiple screens or involves a large number of operations, it generally does not meet the requirements of this item.

Furthermore, regarding this requirement, it is also required that the operations for changing default settings as a whole are minimal, meaning that if operations for changing default settings are performed on the operation screen, the individual software set as default by the smartphone user will be automatically selected and launched by the basic operation software in situations where those default settings are used. For example, if changing the default setting for a search app changes the default setting for the search app launched via the browser, but does not simultaneously change the default setting for the search app launched when text, images, or other displayed content on the smartphone screen are selected to perform a search, it does not meet the requirements of this item.

(3) Article 12, Item 1(b)

Regarding the measures to be taken by designated providers of basic operation software, Article 12, Item 1(b) stipulates that measures that contribute to smartphone users' selection, such as displaying multiple individual software options of the same type that can be set as default for basic operation software, must be implemented. Rules Article 28, Paragraph 2,

stipulates four minimum requirements for the choice screen (meaning a screen that displays multiple individual software options of the same type that can be set as default (see Order Article 4), etc., and allows default settings to be made; hereinafter the same in this section (3) and (8) B) as such measures, in each item.

A. Matters Related to the Design of the Choice Screen

As the first requirement for the choice screen, Rules Article 28, Paragraph 2, Item 1 stipulates requirements for the selection of individual software options to be displayed on the choice screen.

(A) Matters Related to the Selection of Options

Rules Article 28, Paragraph 2, Item 1(a) stipulates that designated providers of basic operation software must ensure that multiple individual software options are displayed on the choice screen, selected based on objective and reasonable selection criteria (e.g., being among the top downloaded apps in the app store available on the designated provider's basic operation software provided for Japan) from the perspective of ensuring smartphone users' opportunities for selection. In this regard, the number of options to be displayed on the choice screen should be such that, assuming standard font sizes, etc., the entire list of options can be viewed without scrolling the smartphone screen, from the perspective of making it easy for smartphone users to compare options. In addition to this, to ensure smartphone users' opportunities for autonomous selection, it is required that a sufficient number of options be provided, taking into account the number of businesses providing individual software to be displayed on the choice screen, etc. Specifically, around four or five options are conceivable. On the other hand, providing only two options, including individual software provided by designated providers, etc., generally does not meet the requirements of this item (a).

Furthermore, the choice screen is not intended to promote specific individual software, and fairness in the selection of options is required. For example, if a designated provider requires payment of some consideration from a third-party app provider as a condition for including their individual software as an option on the choice screen, or if options are selected for display on the choice screen in descending order of the amount of consideration paid, it does not meet the requirements of this item (a).

In addition, for options on the choice screen, even individual software that is not installed on the smartphone at the time the choice screen is displayed is required to be included as an option on the choice screen if it meets the aforementioned selection criteria. It should be

noted that the approach to selecting options for individual software based on certain criteria and the number of options to display on the choice screen are considered to change over time. Therefore, it is desirable for designated providers to review these approximately once a year in response to such changes.

Furthermore, the proviso of Rules Article 28, Paragraph 2, Item 1(a) requires that, from the perspective of ensuring fairness among individual app providers providing individual software displayed as options on the choice screen, only one individual software per business operator may be displayed as an option on the choice screen.

(B) Display Items for Options

Rules Article 28, Paragraph 2, Item 1(b) stipulates that for options displayed on the choice screen, the name, logo, and description of the individual software must be displayed. For descriptions of individual software, it is assumed that descriptions displayed in the app store for that individual software or descriptions submitted by the third-party app provider providing that individual software will be used. If it is not appropriate to display all descriptions on the same screen due to smartphone screen constraints, etc., displaying descriptions in a pull-down format is permissible from the perspective of this item (b).

(C) Other Requirements for Choice Screen Design

Rules Article 28, Paragraph 2, Item 1(c) stipulates that the display order of options and other displays on the choice screen must not interfere with smartphone users' selection. For example, arbitrarily fixing the display order by taking advantage of order bias, where options displayed at the top (or bottom) are more likely to be selected, can hinder smartphone users' autonomous selection and does not meet the requirements of this item (c).

Furthermore, making a specific individual software more likely to be selected through the size of text or logos, the color of text in relation to the background color, or other display methods for options, or having a specific individual software pre-selected at the time the choice screen is displayed, can also hinder smartphone users' autonomous selection and does not meet the requirements of this item (c).

B. Choice Screen Display Timing

As the second requirement for the choice screen, Rules Article 28, Paragraph 2, Item 2 stipulates that smartphone users must be made to select a specific individual software from the options displayed on the choice screen promptly after the first activation of the

smartphone by the user. ″Promptly after the first activation″ refers to, for example, displaying the choice screen at the time of initial setup after the first activation of the smartphone, or displaying the choice screen at the time of the first launch of the individual software subject to the choice screen, and making users select a specific individual software from the options.

Furthermore, ″making the user select a specific individual software from the options displayed on the choice screen″ means that if the user continues to be in a state where a specific individual software is not selected, for example, by not promptly redisplaying the choice screen after the user has once skipped the selection on the choice screen, it does not meet the requirements of this item.

On the other hand, for smartphones that have already been activated by a smartphone user on the date of designation (or the enforcement date of the Act), it is required to display the choice screen within one year from the date of designation (or the enforcement date of the Act), for example, after a smartphone reboot due to a basic operation software update or at the time of the first launch of the individual software subject to the choice screen.

It should be noted that the proviso of Rules Article 28, Paragraph 2, Item 2, from the perspective of respecting smartphone users' selections made on the choice screen, exceptionally permits not displaying the choice screen on smartphones where the user has already selected a specific individual software from the options displayed on a choice screen on another smartphone, and the default settings for individual software subject to that choice screen on the user's other smartphone are inherited as default settings on the user's current smartphone at the time of first activation, etc..

C. Display of Explanation Screen for Choice Screen

As the third requirement for the choice screen, Rules Article 28, Paragraph 2, Item 3 stipulates that before making a selection on the choice screen, a screen (hereinafter referred to as ″explanation screen″ in this section (3)) displaying the type of individual software, the meaning and significance of default settings, an explanation that the user will be choosing individual software that will become the default setting on their smartphone, and an explanation of how users can change the default settings for selected individual software must be displayed. ″Explanation of how users can change the default settings for selected individual software″ refers to, for example, explaining that it can be changed at any time through the settings app.

Furthermore, it is assumed that some smartphone users have sufficient knowledge about default settings, etc., related to smartphones, while others may not. It is important for

smartphone users to make a selection after sufficiently understanding the implications of selecting individual software as a default setting, etc., to choose the most appropriate individual software for them. Therefore, the content described on the explanation screen must be such that any person can understand it.

D. Other Requirements for the Choice Screen

As the fourth requirement for the choice screen, Rules Article 28, Paragraph 2, Item 4 stipulates that, in addition to the requirements in A to C above, nothing must prevent smartphone users from configuring default settings through the choice screen. For example, if selecting individual software on the choice screen requires additional operations for it to launch as a default setting, depending on the number and complexity of such operations, it may constitute an action that hinders the user from setting default settings through the choice screen.

Specifically, this applies to cases where, when a smartphone user attempts to select uninstalled individual software on the choice screen, a pop-up appears stating that the individual software needs to be downloaded, requiring the user to close the choice screen, manually launch the app store, download and install the individual software, and then return to the choice screen to complete the operation. It also applies to cases where, if individual software provided by designated providers, etc., is selected on the choice screen, the choice screen is no longer displayed, but if individual software other than that provided by designated providers, etc., is selected on the choice screen, the choice screen is repeatedly displayed until individual software provided by designated providers, etc., is selected, thereby steering the smartphone user to select a specific individual software.

(4) Article 12, Item 1(c)

Regarding the measures to be taken by designated providers of basic operation software, Article 12, Item 1(c) stipulates necessary measures to obtain smartphone user consent when additionally installing individual software provided by designated providers, etc., onto the smartphone. Rules Article 28, Paragraph 3, stipulates two minimum requirements for such measures in each item.

First, Rules Article 28, Paragraph 3, Item 1 stipulates that the name and functional overview of the individual software to be additionally installed (meaning to be additionally installed; hereinafter the same in this section (4)) must be shown to the smartphone user. Rules Article 28, Paragraph 3, Item 2 stipulates that the smartphone user's consent regarding the additional

installation of individual software must be confirmed. The overview of the individual software shown to the smartphone user must be detailed enough for the user to determine whether or not to give consent. For confirming the presence or absence of consent for additionally installing individual software provided by designated providers, etc., onto the smartphone, the designated provider is required to select and implement the most appropriate timing and method for confirming the user's intent.

(5) Article 12, Item 1(d)

A. Specific Understanding of Article 12, Item 1(d)

"Delete" in Article 12, Item 1(d) refers to uninstalling individual software from a smartphone. "Individual software that is indispensable for smartphone operation, such as individual software that operates smartphone settings, and which other businesses cannot technically provide" specifically refers to individual software closely linked to basic operation software, such as individual software that operates smartphone settings (e.g., settings app, phone app).

In addition, "operation equivalent to deletion" refers to, for example, making the individual software inactive, such as allowing smartphone users to choose to delete the individual software's cache or user data to free up smartphone device storage.

B. Necessary Measures for Deleting Individual Software from Smartphones Through Simple Operations

Regarding the measures to be taken by designated providers of basic operation software, Article 12, Item 1(d) stipulates necessary measures to enable smartphone users to delete individual software provided by designated providers, etc., from their smartphones through simple operations. Rules Article 28, Paragraph 4, stipulates two minimum requirements for such measures in each item.

First, Rules Article 28, Paragraph 4, Item 1 stipulates that the screen for deleting individual software provided by the designated provider must be made easily discoverable. For example, if a pop-up for deletion appears when long-pressing the individual software's icon, it can be said to meet the requirements of this item.

Furthermore, Rules Article 28, Paragraph 4, Item 2 stipulates that smartphone users must be able to delete individual software with the minimum necessary operations on the aforementioned screen. Through the aforementioned pop-up, for example, it is required that deletion can be completed with the minimum necessary steps, including explanations of the

effects of deletion.

(6) Article 12, Item 2(a)

A. "Default Browser Settings"

"Default browser settings" in Article 12, Item 2 refers to settings where a specific search service or other service is automatically selected and provided by the browser (hereinafter simply referred to as "default settings" in this section (6) and (7)). Specifically, for example, when a smartphone user enters a search query in the browser's address bar, a specific search service is selected and provided by the browser's control, without the user having to actively select a specific search service each time.

B. Necessary Measures for Changing Default Settings

Regarding the measures to be taken by designated providers of browsers, Article 12, Item 2(a) stipulates that if services provided by the designated provider or its subsidiaries are provided as default settings, necessary measures must be taken to enable smartphone users to change those default settings through simple operations. Rules Article 28, Paragraph 5, which applies mutatis mutandis to Article 28, Paragraph 1, stipulates three minimum requirements for such measures in each item. The understanding of these three requirements is the same as in (2) B above.

(7) Article 12, Item 2(b)

Regarding the measures to be taken by designated providers of browsers, Article 12, Item 2(b) stipulates that for services related to default browser settings as defined in Order Article 5, measures that contribute to smartphone users' selection, such as displaying multiple options of the same type of service that can be set as default, must be implemented. Rules Article 28, Paragraph 6, which applies mutatis mutandis to Article 28, Paragraph 2, stipulates four minimum requirements for the choice screen (meaning a screen that displays multiple service options of the same type that can be set as default, etc., and allows default settings to be made; hereinafter the same in this section (7) and (8) D) as such measures, in each item. The understanding of these four requirements is the same as in (3) above.

It should be noted that for designated providers of both basic operation software and browsers that are obliged to display a choice screen under Article 12 for both, from the perspective of avoiding redundant selection efforts for smartphone users, if, for example, the search service related to the search app selected by the user on the search app choice screen under Article

12, Item 1(b) is also reflected as a default setting in the designated provider's browser, it is permissible from the perspective of this item not to display the search engine choice screen as a designated provider of browsers again to that user, treating it as if the search engine choice screen as a designated provider of browsers has already been displayed.

(8) Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

Designated providers of basic operation software or browsers are required to report to the Japan Fair Trade Commission on the status of their compliance with Article 12, including the matters stipulated in Rules Article 36, Paragraph 2. Examples of other necessary information for confirming compliance with the Act under Item 4(c) of the same paragraph include the following:

A. Regarding Article 12, Item 1(a)

1. If the designated provider of basic operation software establishes criteria or conditions for individual software to enable default settings related to basic operation software, an outline of those criteria.
2. An explanation of the main matters used to determine the display order of individual software options subject to default settings on the operation screen for changing default settings related to basic operation software (including whether advertising expenses or other financial payments from third-party app providers to the designated provider may influence the display order).

B. Regarding Article 12, Item 1(b)

1. Detailed selection criteria for individual software options to be displayed on the choice screen, an explanation of the reasonableness of those selection criteria, and if the selection criteria have been changed, the content of the change and the reasons for it.
2. Status regarding the scope of target devices for which the individual software choice screen is displayed.

C. Regarding Article 12, Item 2(a)

- An explanation of the main matters used to determine the display order of service options subject to default settings on the operation screen for changing default settings related to the designated provider's browser (meaning a screen that allows changing default settings for services subject to default browser settings) (including whether

advertising expenses or other financial payments from other businesses to the designated provider may influence the display order).

D. Regarding Article 12, Item 2(b)

1. Detailed selection criteria for service options to be displayed on the choice screen for services related to default browser settings, an explanation of the reasonableness of those selection criteria, and if the selection criteria have been changed, the content of the change and the reasons for it.
2. Status regarding the scope of target devices for which the choice screen for services related to default browser settings is displayed.

9. Article 13 (Measures Related to Changes in Specifications and Usage Conditions of Designated Software)

(1) Basic Approach

Article 13 of this Act obliges designated providers of basic operation software, application stores, or browsers to implement necessary measures to ensure that other individual app providers and website operators (hereinafter referred to as "individual app providers" and "website operators," respectively, and collectively referred to as "other businesses" in this section 9) can seamlessly respond when changes are made. This applies to the specifications or conditions of use (hereinafter referred to as "specifications, etc.") or to instances where the use of the designated provider's specified software (referring to basic operation software, application stores, or browsers, collectively referred to as "specified software" in this section 9) is entirely or partially rejected during the provision of such specified software to other businesses (hereinafter collectively referred to as "changes in specifications, etc." in this section 9).

If a designated provider fails to implement necessary measures to ensure that other businesses can seamlessly adapt to changes in specifications, etc., it may cause unexpected disadvantages for those other businesses. Therefore, by obliging designated providers to implement such measures in a way that ensures transparency and fairness, this provision aims to secure a fair competitive environment among other businesses utilizing specified software.

(2) Content of Measures that Designated Providers Must Implement Under Article 13

The content of necessary measures that designated providers must implement to ensure that other businesses can seamlessly adapt to changes in specifications, etc., is stipulated in each item of Rules Article 29, corresponding to the category of specified software prescribed in

each item of Article 13 of the Act.

A. Measures to be Taken by Designated Providers of Basic Operation Software

For designated providers of basic operation software, Rules Article 29, Item 1 stipulates that they must implement the following measures:

1. Measures to disclose specifications, etc.
2. When changing specifications, etc., measures to ensure a reasonable period and disclose the content and reasons for the change
3. When entirely rejecting use, measures to ensure a reasonable period and disclose the intent and reasons for the entire rejection of use
4. When partially rejecting use, measures to disclose the content and reasons for the partial rejection of use
5. Measures to establish a system for handling complaints and other matters related to changes in specifications, etc.

The recipients of measures (3) and (4) above are limited to individual app providers that the designated provider of basic operation software directly permits to use and continuously use the basic operation software. For example, individual app providers who provide individual software through alternative application stores that have not been pre-reviewed by the designated provider regarding the use of basic operation software are not included as recipients of the measures.

B. Measures to be Taken by Designated Providers of Application Stores

For designated providers of application stores, Rules Article 29, Item 2 stipulates that they must implement the same measures as (1) to (5) in A above, and the recipients of these measures are individual app providers.

C. Measures to be Taken by Designated Providers of Browsers

For designated providers of browsers, Rules Article 29, Item 3 stipulates that they must implement the following measures: 1) measures to disclose specifications, 2) measures to ensure a reasonable period and disclose the content and reasons for changes when changing specifications, and 3) measures to establish a system and procedures necessary for considering opinions and other circumstances of website operators related to the setting or changes of specifications. The recipients of these measures are website operators.

D. "Specifications" and "Conditions for Use"

"Specifications" refers to the mechanism of data processing, etc., but is limited to those that "have circumstances equivalent to significantly affecting the business activities of businesses utilizing specified software and are deemed necessary to be disclosed," and excludes those that "may harm the interests of smartphone users if disclosed". Furthermore, industry standards formulated and published by industry associations in which designated providers also participate, for example, are not included in "specifications" here.

"Circumstances equivalent to significantly affecting the business activities of businesses utilizing specified software and are deemed necessary to be disclosed" include, for example, specifications of a browser that, if changed, would significantly alter the layout of web pages displayed in that browser, or that determine the readability of web pages or the operability for smartphone users Browse those web pages, as well as those whose change would prevent website operators from obtaining information obtained from displaying web pages, when they use such information for their business activities. On the other hand, specifications that do not determine the display of web pages or the operation for smartphone users Browse them, such as specifications changed due to bug (meaning an error or defect in a program) fixes, do not fall under this category. Furthermore, specifications that contain information protected as intellectual property rights of the designated provider and whose disclosure may infringe those rights also do not fall under this category. "May harm the interests of smartphone users if disclosed" refers to, for example, information related to the algorithm for display ranking in application store search results, which, if disclosed, may be abused to manipulate the mechanism for determining display ranking, resulting in search results not reflecting smartphone users' actual evaluations, thereby potentially harming smartphone users' interests.

It should be noted that "changes in specifications" are considered to occur more frequently than "conditions for use," such as incidental changes due to bug fixes. Minor changes in specifications are excluded from the disclosure obligation under Article 13 of the Act.

"Conditions for use" refers to general conditions stipulated in the designated provider's terms and conditions or contracts that other businesses need to meet to use the designated provider's specified software. Unlike "specifications," "conditions for use" are the basis of the transactional relationship between the designated provider and other businesses. Therefore, from the perspective of ensuring transparency and fairness in transactions, "conditions for use" are subject to the disclosure obligation under Article 13 of the Act without specific exceptions.

E. "Entire Rejection of Use" and "Partial Rejection of Use"

As described in A above, the entire rejection of use or partial rejection of use of specified software (hereinafter collectively referred to as "rejection of use" in this section 9) is considered to be directed at individual app providers. "Entire rejection of use" refers to measures such as suspending the individual app provider's developer account. "Partial rejection of use" refers to measures such as suspending some individual software provided by the individual app provider, or suspending some functions of basic operation software or an application store.

(3) Measures to Disclose Specifications, etc.

Rules Article 30 stipulates the methods and required items for disclosure when a designated provider implements measures to disclose specifications, etc..

A. Disclosure Methods

The methods for disclosing specifications, etc., are stipulated in Rules Article 30, Paragraph 1 as follows:

1. Using clear and simple language
2. Being easily accessible at any time
3. If the disclosed information (excluding program information and other specification-related information for which Japanese translation is not expected in Japan) is not prepared in Japanese, attaching a Japanese translation

From the perspective of (1) and (2), it is required not to use proprietary terms used only internally by the designated provider or to frequently use ambiguous expressions. It is also required not to disclose information only at certain times or to limit the scope of information disclosure to only some other businesses.

Furthermore, if terms of use containing conditions for use are voluminous, important information for other businesses using specified software may be buried within them. Therefore, it is desirable to take measures that allow other businesses to easily find the information they are looking for, such as displaying important information from the terms of use on a consolidated web page for other businesses, such as a help page or blog, and providing a search function on that web page.

From the perspective of (3), for designated providers operating globally, the original text of specifications, etc., is often prepared in languages other than Japanese, while most other businesses operating in Japan are expected to be domestic companies. Therefore, to ensure transparency and fairness between designated providers and other businesses, a Japanese translation of the disclosed specifications, etc., is required as a general rule. However, for technical information described in programming languages, etc., or other specification-related information for basic operation software for which Japanese translation is not expected in Japan, a Japanese translation is not required.

It should be noted that preparing Japanese translations of specifications, etc., may take time due to their large volume or complex content. Therefore, it is conceivable that it may be unavoidable to not attach a Japanese translation to the original text of specifications, etc., prepared in a language other than Japanese. Even in such cases, the designated provider is required to explicitly state a deadline at the time of disclosure and to attach the translation by that deadline. At this time, any deadline is not acceptable; it is desirable to explicitly state a reasonable deadline necessary for preparing the Japanese translation.

B. Disclosure Items

The matters subject to disclosure by designated providers (hereinafter referred to as "disclosure items") are stipulated in Rules Article 30, Paragraph 2, Item 1 for basic operation software and in Item 2 for application stores. These disclosure items are stipulated as matters that should be "included" in the conditions for use and disclosed, from the perspective of contributing to the improvement of transparency and fairness for other businesses using specified software. Therefore, if there are any other matters that fall under specifications, etc., they are included as disclosure items.

Some of these disclosure items are intended to improve transparency from the perspective of other businesses and protect other businesses' interests regarding the designated provider's efforts to comply with other provisions of the Act. Designated providers are required to comply with the entire Act by disclosing the matters stipulated in each item of Rules Article 30, Paragraph 2.

Among these disclosure items, the content and reasons for requesting individual app providers to purchase designated goods or receive paid services provided by the designated provider in conjunction with the use of specified software (Rules Article 30, Paragraph 2, Items (b)) are required to be disclosed even if the designated provider forces the use of specific services without relying on terms of use, etc..

Furthermore, for business related to application stores, the main matters used to determine the ranking when information related to goods or services is displayed with a ranking (Rules Article 30, Paragraph 2, Item 2 (f)) include not only the ranking of results displayed for information sought by smartphone users through search, but also the main matters used to determine the ranking when the designated provider displays rankings or recommended rankings by category without search. In addition, these display rankings have a significant impact on smartphone users' purchasing behavior, etc., and individual app providers typically make modifications to individual software, etc., assuming that smartphone users will act rationally regarding the main matters for determining such display rankings. Therefore, it is desirable for designated providers to disclose the main matters for display rankings to smartphone users as well.

Similarly, emphasized displays such as recommendations also have a significant impact on smartphone users' purchasing behavior, etc., and therefore, the main matters used to determine the content of such displays (Rules Article 30, Paragraph 2, Item 2 (g)) are also required to be disclosed.

Rules Article 30, Paragraph 2, Item 2 (h) requires the disclosure of the content and conditions for withholding all or part of the payment that the designated provider should make to individual app providers as consideration for goods or services provided by individual app providers. Since withholding payment can significantly impact individual app providers' cash flow, if the designated provider actually withholds payment, it is desirable to disclose the content and reasons for such withholding to the individual app provider who is the recipient of the withholding. It should be noted that depending on the content or reasons for the withholding, the withholding itself may violate Article 6 of the Act.

(4) Measures Related to Disclosure When Changing Specifications, etc., and Rejecting Use

Rules Article 31 for changes in specifications, etc., Rules Article 32 for entire rejection of use, and Rules Article 33 for partial rejection of use (hereinafter collectively referred to as "each Article" in this section (4)) stipulate the methods and timing of disclosure, including ensuring a reasonable period, and exceptions to disclosure obligations, etc., when a designated provider changes specifications, etc., or rejects use, and implements measures to disclose items stipulated in each item of Rules Article 29 (b).

A. Disclosure Items

The disclosure items when a designated provider changes specifications, etc., are stipulated in

each item of Rules Article 29 (b) as the content and reasons for the change. The content of the change is required to include information on the changed parts and the specifications, etc., after the change. For example, for application stores, considering the circumstances of individual app providers, if the intent of the change cannot be understood by merely disclosing information on the changed parts and the specifications, etc., after the change, it is conceivable to also disclose information on the specifications, etc., before the change as part of the content of the change, to show which parts were changed and how.

The disclosure items when a designated provider entirely rejects use are stipulated in Rules Article 29, Item 1 (c) and Item 2 (c) as the intent and reasons for the entire rejection of use. The disclosure items when a designated provider partially rejects use are stipulated in Rules Article 29, Item 1 (d) and Item 2 (d) as the content and reasons for the partial rejection of use. For example, for application stores, considering the circumstances of individual app providers, it is required to disclose these items concretely and accurately enough for individual app providers to file objections or implement improvement measures for prompt account recovery. Furthermore, in cases of rejection of use due to specific violations of terms of use, it is desirable to disclose the relevant clauses of the terms of use.

It should be noted that, based on the obligation to establish a complaint handling system and procedures under Rules Article 34, designated providers are required to respond diligently to inquiries from individual app providers whose use of basic operation software or application stores has been rejected due to account suspension, etc.. Furthermore, if the rejection of use was based on an incorrect judgment, it is desirable to take measures that give full consideration to the interests of individual app providers, such as considering the necessity of compensating for losses incurred by individual app providers during the period of inability to use the software.

B. Disclosure Methods and Timing

The methods and timing of information disclosure by designated providers are stipulated in Paragraph 1 of each Article.

Regarding disclosure methods, Paragraph 1, Item 1 of each Article stipulates that when a designated provider changes specifications, etc., or rejects use, it must disclose necessary information using clear and simple language for other businesses. Designated providers are required to disclose necessary information to other businesses to the extent that it is possible to foresee what specific actions other businesses need to take due to changes in specifications, etc., or rejection of use, or to fully understand the nature of the disadvantages incurred by other businesses.

Furthermore, if terms of use containing conditions for use are revised, it is desirable to disclose the revised parts in an easily understandable manner, such as by providing a comparison table, so that the important revised parts are clear to other businesses using specified software.

In addition, regarding the information to be disclosed, Paragraph 1, Item 2 of each Article stipulates that if requested by other businesses, the content translated into Japanese must be disclosed without delay. Since the disclosure of Japanese translations is a prerequisite for correctly understanding the content of changes in specifications, etc., and the reasons for rejection of use, it is desirable to ensure smooth two-way communication in Japanese, for example, by assigning Japanese-speaking staff to inquiry desks for changes in specifications, etc., and rejection of use, rather than merely providing unilateral notifications via documents or emails.

Finally, regarding the timing of disclosure, Paragraph 1, Item 3 of each Article stipulates that disclosure must be made:

1. For changes in specifications, by the day that ensures a reasonable number of days depending on the content of the change.
2. For changes in conditions for use, by 15 days before the day of the change (or by the day that ensures a reasonable number of days expected for the work or adjustments if other businesses are expected to require more than 15 days for such work or adjustments) (however, it can be a shorter period if there is consent from the individual app provider).
3. For entire rejection of use, by 30 days before the day of rejection.
4. For partial rejection of use, by the time of rejection.

Designated providers are required to disclose information to other businesses while ensuring each period stipulated in the Rules. Among these, regarding "a reasonable number of days depending on the content of the change" in (1), if the content of the change in specifications has a significant impact on other businesses, it is required to disclose information with sufficient time in advance.

Furthermore, it is desirable for measures to be taken that give consideration to the business operations of other businesses, such as disclosing information with ample time in advance of the disclosure timing stipulated in the Rules, especially when particularly necessary in individual cases. In particular, for partial rejection of use in (4), which includes individual software suspension measures, as it has a significant impact on individual app providers, it is desirable for it to be disclosed early, considering the impact on individual app providers, rather than

immediately before the partial rejection of use is carried out.

C. Exceptions to Disclosure Obligations, etc.

Exceptions to information disclosure obligations, etc., are stipulated in Paragraph 2 of each Article.

First, for cases where 1) the content of changes in conditions for use is extremely minor, 2) it is based on laws and regulations and it is necessary to promptly change specifications, etc., or 3) it is necessary to promptly change specifications, etc., for ensuring cybersecurity, etc., or to respond to infringement activities using fraud or other dishonest means, or activities clearly contrary to public order or morality, it is sufficient to disclose the content and reasons for the change without delay. For example, for (1), cases where other businesses do not need to take countermeasures such as modification work and their business activities are not affected are considered extremely minor. For (2), cases where administrative agencies, based on laws and regulations, issue dispositions, etc., requesting designated providers to promptly change specifications, etc., and designated providers need to comply, are conceivable. For (3), cases where measures are taken to ensure cybersecurity, etc., such as preventing data leakage, loss, or damage, are conceivable.

Furthermore, for entire rejection of use, exceptions are stipulated for cases where 1) individual app providers repeatedly violate conditions for use and there is a risk of hindering the operation of the specified software business, 2) individual app providers are likely to be involved with organized crime groups, etc., 3) it is based on laws and regulations and disclosing the reason may harm the legitimate interests of the designated provider, smartphone users, or other parties, 4) it is based on laws and regulations and it is necessary to promptly make the rejection, or 5) it is necessary to promptly make the rejection for ensuring cybersecurity, etc., or to respond to infringement activities using fraud or other dishonest means, or activities clearly contrary to public order or morality. In cases (1) and (2), it is sufficient to disclose the intent of entire rejection of use without delay. In case (3), it is sufficient to disclose the intent of entire rejection of use by 30 days before the date of rejection. In cases (4) and (5), it is sufficient to disclose the intent and reasons for entire rejection of use without delay. Among these, for (1), for example, cases where individual app providers repeatedly apply for individual software with the same content that violates the terms of use of the designated provider's application store, thereby hindering review operations in that application store, are conceivable.

Furthermore, for partial rejection of use, similar provisions to the exceptions for entire rejection of use are stipulated.

It should be noted that entirely rejecting the use of specified software, such as by performing immediate account suspension measures without prior notification, or partially rejecting the use of specified software, such as by performing individual software suspension measures without prior notification, has a significant impact not only on individual app providers but also on smartphone users who use individual software. Therefore, when a designated provider entirely rejects use or partially rejects use, the designated provider is required to carefully judge the applicability of each of the aforementioned exceptional circumstances. Furthermore, even in cases where an exception appears to apply, it is desirable to thoroughly consider the necessity and reasonableness of applying the exception, and if necessary, to provide prior notification for entire rejection of use or partial rejection of use as a general rule.

In addition, even in cases where each of the aforementioned exceptional circumstances ((1), (2), (4), and (5)) applies, it is required to disclose information related to changes in specifications, etc., or entire rejection of use or partial rejection of use "without delay". In light of the purpose of Article 13 of the Act, which is to prevent unforeseen disadvantages for individual app providers, if a designated provider fails to disclose such information for a long period without reasonable grounds, it violates Article 13 of the Act.

(5) Measures for Handling Complaints and Establishing Other Systems

Measures for handling complaints and establishing other systems are stipulated in Rules Article 34, Paragraphs 1 to 3, corresponding to the category of specified software prescribed in each item of Article 13 of the Act.

Designated providers of basic operation software or application stores are stipulated to implement measures for 1) establishing a system to ensure that changes in specifications, etc., are conducted fairly, 2) establishing a system for handling complaints and resolving disputes, 3) appointing a domestic administrator, and 4) taking measures to sufficiently consider the opinions and other circumstances of other businesses. However, for designated providers of basic operation software, in measures (2), (3), and (4), (a) website operators and (b) individual app providers other than those that the designated provider directly permits to use and continuously use the basic operation software are excluded from the recipients of the measures.

Furthermore, for designated providers of browsers, it is stipulated that they must implement only measures (1) and (4) (however, limited to those related to the setting or changes of specifications).

A. Establishing a System to Ensure that Changes in Specifications, etc., are Conducted Fairly

Changes in specifications, etc., by designated providers must be conducted fairly, and designated providers are required to establish a system and procedures to ensure this. Designated providers are required to 1) establish an appropriate mechanism to ensure consistent and fair judgments when making changes in specifications, etc., and to establish an appropriate mechanism to ensure appropriate responses that consider the interests of other businesses as necessary, taking into account the impact on other businesses, etc., and 2) establish an appropriate mechanism to improve fairness related to changes in specifications, etc..

Examples of responses related to (1) include establishing objective and clear judgment criteria and establishing a review system and procedures for making appropriate judgments in accordance with those criteria to ensure consistent and fair judgments when designated providers entirely reject use or partially reject use of specified software. It also includes establishing mechanisms to ensure appropriate responses that go beyond the scope required by Rules Articles 30 to 33, as necessary, considering the disadvantages incurred by individual app providers, etc.. Examples of responses related to (2) include establishing a system and procedures for conducting ex-post verification and operational improvement regarding the operation of the review system and procedures in (1).

It should be noted that designated providers of basic operation software or application stores are prohibited from engaging in unjust discriminatory treatment or otherwise unfair treatment towards individual app providers based on Article 6 of the Act. Therefore, the establishment of necessary systems and procedures to ensure that changes in specifications, etc., related to specified software are conducted fairly also contributes to compliance with Article 6 of the Act.

B. Establishing a System for Handling Complaints and Resolving Disputes

Designated providers are required to establish a system and procedures necessary for handling complaints and resolving disputes, including disclosing methods for submitting complaints, etc., to individual app providers, in order to appropriately respond to complaints, etc., from individual app providers regarding changes in specifications, etc.. Designated providers are required to 1) establish a system and procedures to appropriately and promptly process and resolve the causes of complaints and disputes, depending on their importance and complexity, and 2) establish an appropriate mechanism to improve fairness related to changes in specifications, etc., based on complaints and disputes.

For example, for (1), establishing basic policies, response manuals, and workflow charts for appropriately and promptly processing complaints from individual app providers, and establishing a contact point (including a responsible department, person in charge, and contact information) for accepting complaints or requests for consultation externally are conceivable. For (2), it is conceivable to analyze the content, number, increase/decrease in number, and reasons for complaints and disputes received through the designated complaint form established by the designated provider, and to utilize the information obtained through such analysis for changes in specifications, etc..

C. Appointment of Domestic Administrator

Designated providers are required to appoint a person who manages the necessary operations in Japan to maintain close contact with individual app providers and other relevant parties (hereinafter referred to as "domestic administrator") so that they can efficiently grasp the diverse circumstances of a large number of relevant parties located in Japan and take appropriate actions based on their opinions and knowledge.

It is desirable for the domestic administrator to establish a mechanism that allows for appropriate coordination between the designated provider and individual app providers and other relevant parties as necessary. From this perspective, for example, it is conceivable to appoint relevant department personnel as assistants to the domestic administrator to enable appropriate coordination, and to establish a system that allows for sufficient communication with other businesses and other relevant parties.

D. Measures to Sufficiently Consider Opinions and Other Circumstances of Other Businesses

Designated providers of basic operation software or application stores are required to appropriately grasp the opinions, etc., of individual app providers and to implement necessary measures to sufficiently consider the opinions and other circumstances of individual app providers. Designated providers are required to 1) establish a mechanism to understand the opinions and other circumstances of individual app providers, and 2) establish an appropriate mechanism to effectively utilize the opinions and other circumstances of individual app providers for the provision of specified software.

For example, as a response from both (1) and (2) perspectives, it is conceivable to establish a mechanism for sufficiently hearing and understanding the opinions of individual app providers and other relevant parties regarding changes in specifications, etc., and to reflect the results in operations related to changes in specifications, etc., as necessary. In this regard, since

small-scale individual app providers may be too busy dealing with changes in specifications, etc., to have time for consultations, and may wish to remain anonymous due to fear of retaliation, and since consolidating opinions from individual app providers may lead to more efficient consultations, it is conceivable for designated providers to respond not only to individual companies but also to requests for consultations and opinions from organizations.

Furthermore, for designated providers of browsers, who are exempt from the obligation to appoint a domestic administrator as described in (C) above, it is particularly necessary to sufficiently consider the opinions, etc., of domestic website operators, for example, if changes in browser specifications significantly affect the business activities of website operators who use information obtained from displaying web pages for their business activities, by preventing them from obtaining such information.

(6) Matters to be Reported to the Japan Fair Trade Commission to Confirm Compliance with the Act

Designated providers of basic operation software, application stores, or browsers are required to report to the Japan Fair Trade Commission on the status of their compliance with Article 13, including the matters stipulated in Rules Article 36, Paragraph 2. Examples of other necessary information for confirming compliance with the Act under Item 4(c) of the same paragraph include the following:

1. URL of the web page displaying the specifications and conditions for use subject to disclosure under Rules Article 30 (latest Japanese translation).
2. Content implemented through the system and procedures established based on Rules Article 34 (including an outline of opinions, etc., submitted by individual app providers and website operators, and the designated provider's responses and outcomes for those submissions).

IV. Understanding Compliance Reports

(1) Basic Approach to Compliance Reports from the Perspective of Seamless and Appropriate Application of the Act

For the seamless and appropriate application of the Act, it is crucial to ensure that the Japan Fair Trade Commission can reliably grasp the measures taken by designated providers to prevent actions that violate the prohibited conduct stipulated in Articles 5 to 9 (hereinafter referred to as "prohibited provisions" in this Section 4) and to comply with the measures to be taken stipulated in Articles 10 to 13 (hereinafter referred to as "measures provisions" in

this Section 4). Furthermore, if actions suspected of violating prohibited provisions or non-compliance with measures provisions are found by designated providers, it is necessary for the Japan Fair Trade Commission to conduct investigations against those designated providers as quickly as possible.

From this perspective, designated providers are required to specifically explain in the report submitted to the Japan Fair Trade Commission based on Article 14, Paragraph 1 of the Act (hereinafter referred to as "compliance report"), in addition to the content of measures taken to prevent actions violating prohibited provisions and to comply with measures provisions, other necessary matters for confirming compliance with these provisions of the Act, accompanied by supporting evidence, including explanatory materials from the designated provider, that substantiates the content described in the compliance report.

In particular, regarding justifiable reasons from the perspective of ensuring cybersecurity, etc., when an action is suspected to violate the provisions of this Act, it is important to efficiently grasp the facts of the case and the designated provider's claims. Therefore, the designated provider is required to provide a reasonable and specific explanation demonstrating that its actions qualify as a justifiable reason.

The Japan Fair Trade Commission will confirm the content of compliance reports submitted by designated providers and, as necessary, request reports or issue orders for reports based on Article 40 of the Antimonopoly Act to obtain more detailed information regarding the content of the compliance report, thereby confirming the designated provider's compliance status with the Act. If necessary for confirming such compliance status, the Japan Fair Trade Commission may, as described in Section 5 below, seek opinions from relevant government ministries and agencies and may also hear opinions from businesses other than designated providers, etc..

Furthermore, the Japan Fair Trade Commission will publicly disclose compliance reports, excluding descriptions related to the secrets of businesses, including designated providers, based on Article 14, Paragraph 2 of the Act. At that time, the Japan Fair Trade Commission will determine whether the content described in the compliance report constitutes a business secret, while appropriately reflecting the designated provider's explanation.

(2) Specific Content to be Reported in Compliance Reports

A. Matters Related to the Outline of the Designated Provider's Business

For the purpose of accurately understanding the designated provider's business related to the

provision of specified software, etc., and for reference in confirming compliance with the Act, Article 14, Paragraph 1, Item 1 stipulates that matters related to the outline of the designated provider's business must be reported, and specific reporting matters are stipulated in Rules Article 36, Paragraph 1. That is, for each specified software, designated providers are required to report the following to the Japan Fair Trade Commission in the compliance report:

(A) Content of terms and conditions and other conditions for use related to the provision of specified software, etc.
(B) For the content of conditions for use in (A) above, changes (excluding minor changes) from the previous report and an explanation of the purpose of such revisions
(C) Content of specifications related to specified software (excluding search engines) (limited to those that have a significant impact on the business activities of businesses using specified software)
(D) For the specifications in (C) above, changes (excluding minor changes) from the previous report and an explanation of the purpose of such changes

B. Matters Related to Measures Taken to Comply with Articles 5 to 13 of the Act

From the perspective of grasping matters related to measures for preventing actions violating prohibited provisions and complying with measures provisions, and confirming the designated provider's compliance status with the Act, Article 14, Paragraph 1, Item 2 stipulates that matters related to measures taken to comply with Articles 5 to 13 must be reported, and specific reporting matters are stipulated in Rules Article 36, Paragraph 2. Designated providers are required to report to the Japan Fair Trade Commission on matters related to measures taken to comply with Articles 5 to 13, in the compliance report, taking into account the content of "Matters to be reported to the Japan Fair Trade Commission to confirm compliance with the Act" described for each article in Section 3 above.

C. Other Necessary Matters for Confirming Compliance Status with the Act

In addition to (1) and (2) above, from the perspective of confirming compliance status with the Act, designated providers are required to report the following matters to the Japan Fair Trade Commission in the compliance report:

A. Main Content of Discussions Held with Stakeholders, etc., Regarding the Implementation of Necessary Measures for Compliance with the Act

For measures necessary to prevent actions violating prohibited provisions and to comply with measures provisions, mechanisms for considering opinions and other matters, including

consultations with stakeholders such as individual app providers and smartphone users, are effective. Designated providers are expected to conduct such consultations with stakeholders from the design stage of such measures. Such consultations with stakeholders, etc., include, for example, consultations with individual app providers regarding the use of functions related to basic operation software, and consultations with individual app providers regarding conditions for using application stores.

Regarding reports on consultations with stakeholders, etc., if they are conducted as part of the implementation of measures necessary to prevent actions violating prohibited provisions and to comply with measures provisions, since they are relevant information for the Japan Fair Trade Commission to confirm compliance status with the Act, designated providers are expected to report matters related to compliance, such as the progress of the consultations.

B. Other Matters of Reference Regarding Compliance Status with the Act

If an exclusion order under Article 18 of the Act or a recommendation or order under Article 30 of the Act (hereinafter collectively referred to as "exclusion order, etc." in this section B) is issued to a designated provider, it will basically also require reporting on the implementation status of measures taken based on that exclusion order, etc.. However, in the compliance report, designated providers are required to report any matters that should be reported regarding measures to be taken based on that exclusion order, etc., other than the implementation status of measures to be reported based on that exclusion order, etc..

Furthermore, if the Japan Fair Trade Commission certifies an exclusion measures plan applied for by a designated provider based on Article 23 of the Act or an exclusion measures assurance plan based on Article 27 of the Act (hereinafter collectively referred to as "commitment plan"), the designated provider will take necessary measures in accordance with that commitment plan (for commitment plans, please refer to the "Policy on Commitment Procedures under the Smartphone Software Competition Promotion Act" formulated from the perspective of ensuring transparency in their operation and predictability for businesses). In the compliance report, designated providers are required to report any matters that should be reported regarding measures to be taken based on that commitment plan, other than the implementation status of measures to be reported based on that commitment plan.

In addition, if a designated provider deems that there are matters that should be described in the compliance report in light of its purpose, it is desirable to describe those matters in the compliance report. Furthermore, if the Japan Fair Trade Commission, in communication with designated providers related to the application of the Act, deems that there are matters that

should be described by the designated provider in the compliance report in light of its purpose, it will convey to the designated provider that those matters should be described in the compliance report and, as necessary, revise the rules that stipulate the items to be described in the compliance report.

V. Approach to Coordination with Relevant Government Ministries and Agencies

(1) Basic Approach to Cooperation with Relevant Government Ministries and Agencies

In applying the Act, it is necessary to promote competition while ensuring cybersecurity, etc., which requires close cooperation between the Japan Fair Trade Commission and relevant government ministries and agencies. It is important for the Japan Fair Trade Commission to make judgments on individual cases while taking into account opinions from relevant government ministries and agencies that have specialized knowledge on cybersecurity and other related concerns, for the effective application of the Act.

(2) Specific Flow of Cooperation

A. Regarding Cooperation on Justifiable Reasons under Article 7 and Article 8

For the application of the proviso of Article 7 or Article 8, considering the importance of ensuring cybersecurity, etc., cooperation will be carried out based on Article 43, Paragraphs 1 and 3 of this Act, as follows:

(A) The Japan Fair Trade Commission shall, when deemed necessary, request opinions from relevant government ministries and agencies regarding whether the actions of a designated provider fall under the proviso of Article 7 or Article 8.
(B) Upon receiving a request under (A), relevant government ministries and agencies shall examine the matter from a specialized perspective and may provide opinions to the Japan Fair Trade Commission on the applicability of the proviso of Article 7 or Article 8. Furthermore, even in the absence of a formal request under (A), relevant government ministries and agencies may provide opinions to the Japan Fair Trade Commission if they deem it necessary based on the claims made by the designated provider, etc., or other considerations. Additionally, if necessary, the Japan Fair Trade Commission may confirm the contents of the opinions with the designated provider and provide an opportunity for the provider to express its views.
(C) The Japan Fair Trade Commission shall fully consider the opinions of relevant government ministries and agencies under (B) before determining whether there is a violation of Article 7 or Article 8.

(D) The Japan Fair Trade Commission and relevant government ministries and agencies shall mutually establish contact points to facilitate communication and coordination related to the above cooperation (these contact points will also be used for communication and coordination as described in (2) below).

B. Other Cooperation

In addition, it is conceivable that designated providers may make claims regarding prohibited conduct or measures to be taken, other than those related to the application of the proviso of Article 7 or Article 8. In such cases, the Japan Fair Trade Commission shall, based on Article 43, Paragraph 2 of the Act, request opinions from relevant government ministries and agencies when deemed necessary for the enforcement of the Act. The relevant government ministries and agencies that receive such requests shall examine the matter from a specialized perspective and may provide opinions to the Japan Fair Trade Commission from the perspective necessary for the enforcement of the Act. Furthermore, even in the absence of a request for opinions from the Japan Fair Trade Commission, if a relevant government ministry or agency deems it necessary based on the claims made by the designated provider, etc., it may provide opinions to the Japan Fair Trade Commission based on Article 43, Paragraph 4 of the Act.

ENDS