Guidelines on Shared Data with Limited Access

January 23, 2019

Ministry of Economy, Trade and Industry

Table of contents

Introduction

1. Characteristics of the Guidelines

The Guidelines are based on opinions including those by the Unfair Competition Prevention Subcommittee, Intellectual Property Committee, Industrial Structure Council (responsible for considering introducing the present program) (hereinafter, "the Unfair Competition Prevention Subcommittee"), that "easy-to-understand guidelines presenting ideas behind each requirement and specific examples of applicable actions, etc. should be created" with regard to "unfair competition" related to shared data with limited access, a concept introduced as a result of the revision of the Unfair Competition Prevention Act in 2018.

The Guidelines were drafted by the Working Group for Formulation of Draft Guidelines on Unfair Competition Prevention, then deliberated by the Unfair Competition Prevention Subcommittee, a group of industry representatives, experts, and other members. The Guidelines present a definition of shared data with limited access, requirements that fall under unfair competition, and other matters. However, the Guidelines are not legally binding.

It is natural, therefore, that specific issues related to the Unfair Competition Prevention Act will eventually be comprehensively judged by the competent courts together with other considerations according to the relevant specific circumstances.

Also note that the Guidelines are to be reviewed when and as appropriate in view of how they will be implemented after the revised Act comes into effect.

● Excerpt from "Interim Report: Study to Promote Data Utilization" by the Unfair Competition Prevention Subcommittee, Intellectual Property Committee, Industrial Structure Council

7. Efforts to improve predictability through formulation of guidelines, etc.

To clarify the details of each provision before enforcement of a new system, a study should be conducted by the Working Group for Formulation of Draft Guidelines on Unfair Competition Prevention. Then, easy-to-understand guidelines, or materials, etc. (hereinafter "the guidelines") that provide information including the reasoning behind requirements for items related to and including technical management and examples thereof, and examples that do or do not fall under actions taken for the purpose of wrongful gain or causing damage under the category of significant violation of the principle of good faith, should be created. In addition, even after the system is enforced, the guidelines should be reviewed in a timely and appropriate manner, while monitoring the status of implementation of the system. It is also important for business operators to promote education and awareness-raising activities based on their regulations formulated in-house. From the perspective of promoting such activities, formulation of guidelines, etc. should be prepared so that the business operators can conduct such activities more easily.

I. General

1. Characteristics of the Unfair Competition Prevention Act

The Unfair Competition Prevention Act (Act No. 47 of 1993 as revised in 2018; hereinafter, "the Act") defines actions and behaviors that involve unlawful use of the results of technical development, product development, or other accomplishments achieved by someone else, as unfair competition.

More specifically, the Act regards the theft of brand indication, imitation of configurations, unauthorized acquisition of trade secrets, and other actions falling under the category of unfair competition as subject to civil injunction (Article 3 of the Act) and as an extraordinary rule for tort law.

Moreover, any unfair competition that infringes public welfare considerably and that is entrusted merely to a civil claim between the parties is regarded as subject to criminal punishment.

2. Unfair competition related to shared data with limited access (as revised in 2018)

Against the backdrop of the Fourth Industrial Revolution with the progress of IoT, big data, artificial intelligence, and other information technology, data is becoming an increasingly valuable source of corporate competitiveness. Weather data, map data, machine operational data, consumption trend data, and similar information are being shared and used to create new enterprises, resulting in the creation of high value that can drive the Japanese economy. To realize an industrial society of "Connected Industries", where various kinds of such data are combined to create new value, we need an environment that rewards the efforts of data creators, collectors, analyzers, and controllers.

However, useful data is easy to duplicate and, once illegally obtained, can be immediately redistributed in its entirety, meaning that investors may lose the chance to recoup their investments. Therefore, there have been calls for the introduction of legal measures against such illegal conduct in order to reassure data providers.

Under these circumstances, in view of the fact that data is to be widely provided as a product, shared within consortium, and to be supplied to third parties by business operators through transactions or other operations, the Act defines shared data with limited access (Article 2-7 of the Act) and defines unauthorized acquisition, use, and disclosure of shared data with limited access as unfair competition (Articles 2-1-11 to 2-1-16 of the Act).

To ensure that data is used securely, we also considered the possibility that the revised law may not be popular with some users. We therefore set forth a provision that defines certain actions as being exempt from the law regarding unfair competition with shared data with limited access (Article 19-1-8 of the Act).

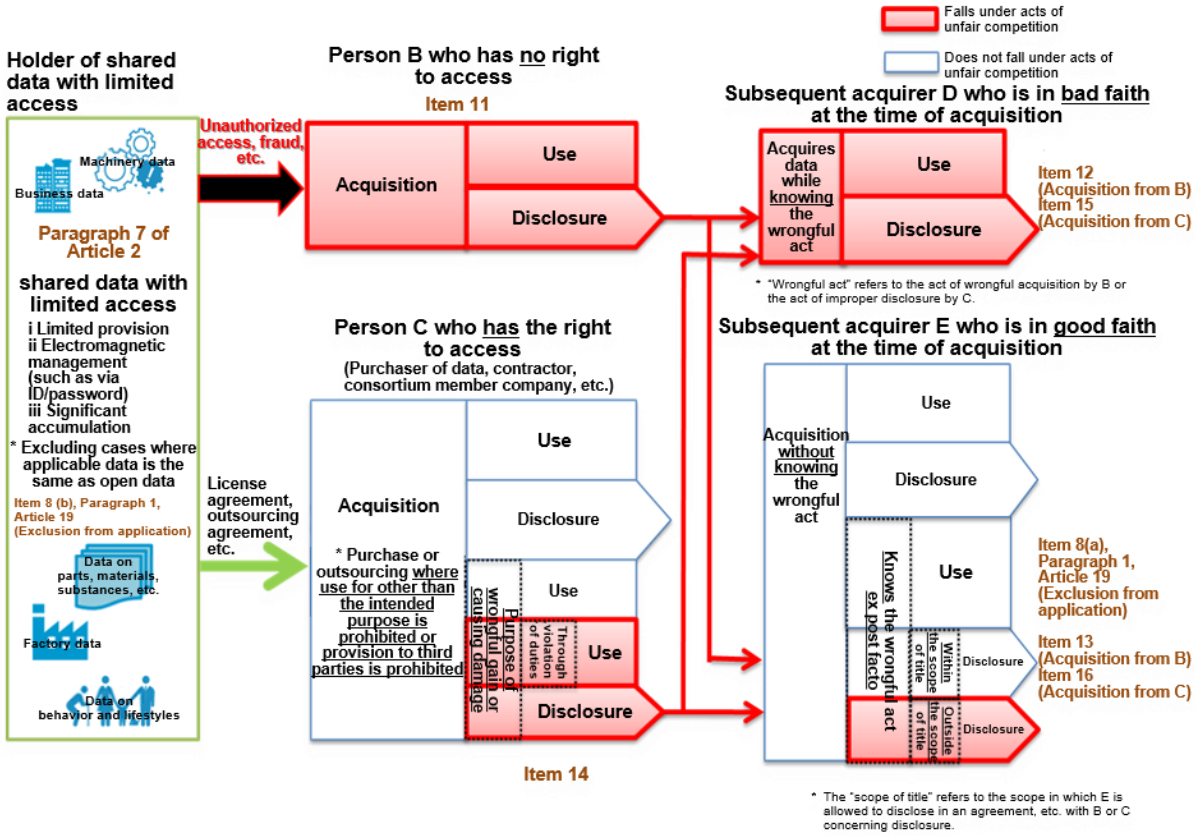
Unauthorized acquisition, use, disclosure, etc. of shared data with limited access are subject to civil measures (claims for injunctions, claims for compensation for loss or damage). However,

as there have been few cases of this kind to date, such conduct is not yet defined as criminally punishable in order to avoid excessive negative effects on business operators.

Shared data with limited access, similarly to trade secrets, consists of "technical or business information" and that the unauthorized acquisition thereof and similar actions are regarded as unfair competition. However, objects for protections are different between shared data with limited access and trade secrets. Even if similar statements are used in these two cases, therefore, they should be interpreted according to the spirit of the provisions made.

*These Guidelines do not affect the interpretation of provisions regarding trade secrets.

Unfair competition regarding shared data with limited access



(1) Definition of shared data with limited access

Article 2

(7) The term shared data with limited access as used in this Act means technical or business information that is accumulated to a significant extent and is managed by electronic or magnetic means (meaning an electronic form, magnetic form, or any other form that is impossible to perceive through the human senses alone; the same applies in the following paragraph) as information to be provided to specific persons

on a regular basis (excluding information that is kept secret).

(2) Unfair competition regarding shared data with limited access

1) Category of unauthorized acquisition

Article 2 (1) The term "unfair competition" as used in this Act means any of the following:

(xi) the act of acquiring shared data with limited access by theft, by fraud, by duress, or by other wrongful means (hereinafter referred to as an "act of wrongful acquisition of shared data with limited access"); or the act of using or disclosing shared data with limited access acquired through an act of wrongful acquisition of shared data with limited access;

2) Category of significant violation of the principle of good faith

Article 2 (1) The term "unfair competition" as used in this Act means any of the following:

(xiv) the act of using or disclosing shared data with limited access disclosed by an undertaking holding that data (hereinafter referred to as the "holder of shared data with limited access"), for the purpose of wrongful gain or causing damage to that holder of shared data with limited access (using the relevant data for that purpose is limited to an act conducted in breach of the duties regarding the management of that data);

3) Category of subsequent acquisition

(Category of subsequent acquisition in bad faith at the time of acquisition)

Article 2 (1) The term "unfair competition" as used in this Act means any of the following:

(xii) the act of acquiring shared data with limited access with the knowledge that there has been an intervening act of wrongful acquisition of shared data with limited access, or the act of using or disclosing shared data with limited access acquired in such a way;

(xv) the act of acquiring shared data with limited access with the knowledge that the disclosure of that data is an act of improper disclosure of shared data with limited access (meaning, in the case described in the preceding item, the act of disclosing shared data with limited access for the purpose as provided for in the same item; the same applies hereinafter) or that there has been an intervening act of improper disclosure of shared data with limited access with regard to the relevant shared data with limited access, or the act of using or disclosing shared data with limited access acquired in such a way;

(Category of subsequent acquisition in good faith at the time of acquisition)

Article 2 (1) The term "unfair competition" as used in this Act means any of the following:

(xiii) the act of disclosing shared data with limited access after having acquired it and learning that there had been an intervening act of wrongful acquisition of shared data with limited access;

(xvi) the act of disclosing shared data with limited access after having acquired that data

and learning that the relevant acquisition falls under an act of improper disclosure of shared data with limited access or that there had been an intervening act of improper disclosure of shared data with limited access;

(3) Exclusion from Application

(Exclusion from Application)

Article 19 (1) The provisions of Articles 3 through 15, Article 21 (excluding the part under Article 21, paragraph (2), item (vii)), and Article 22 do not apply to the act prescribed in the relevant of the following items for the classification of unfair competition set forth in that item:

(viii) unfair competition set forth in Article 2, paragraph (1), items (xi) through (xvi) - any of the following acts:

(a) the act by a person that has acquired shared data with limited access through a transaction (limited to a person that, at the time of acquiring the shared data with limited access, was without knowledge that the disclosure of that data was an act of improper disclosure of shared data with limited access or that there had been an intervening act of wrongful acquisition of shared data with limited access or an act of improper disclosure of shared data with limited access with regard to that data), of disclosing the shared data with limited access within the scope of title acquired through the transaction; or

(b) the act of acquiring shared data with limited access in which the information accumulated to a significant extent is the same as any information that has been made available to the public without compensation, or the act of using or disclosing such acquired shared data with limited access;

II. Shared data with limited access

Article 2

7. The term shared data with limited access as used in this Act means ***technical or business information*** *that is* ***accumulated to a significant extent and is managed by electronic or magnetic means*** *(meaning an electronic form, magnetic form, or any other form that is impossible to perceive through the human senses alone; the same applies in the following paragraph) as information to be* ***provided to specific persons on a regular basis (excluding information that is kept secret)***.

*Whether each requirement is applicable or not will be judged when an instance of unfair competition in question is performed or is about to be performed.

1. "Provided to specified persons on a regular basis" (Limited provision)

The term shared data with limited access used here assumes big data and similar data that is widely provided as a product, data shared within a consortium, and other information to be provided to third parties by a business operator or other entity through a transaction or other operation.

The object of this requirement is therefore to protect data that is provided to specific target users under certain conditions.

- Shared data with limited access therefore does not include data that is widely supplied free of charge to a wide range of people, without specification or limitation (explained in detail in Section 6).

(1) "On a regular basis"

In the case where any such data is provided repeatedly and continuously, or it is objectively known that the holder of specific data intends to provide such data repeatedly and continuously even if no such data has actually been provided yet, this requirement is applicable. This requirement is to be applicable basically when providing such data to anyone on business.

Specific examples that are in principle considered to be "on a regular basis"

- If the holder of specific data is supplying such data repeatedly (including cases where such data is provided to two or more people, one piece of data being provided once to each person, and cases where such data is supplied in customized form to each customer)
- If the data holder has placed a notice on a website or the like that they will begin to sell such data from the next month
- If the data holder is providing such data to members of a consortium within the consortium

Any data provided free of charge or provided by an individual can be regarded as provided "on a regular basis" if it can be regarded as part of an action that is conducted repeatedly and continuously. There is a possibility that person or entity providing such data, however, may not definitively fall under the category of "a person whose business interests have been infringed on" or "are likely to be infringed on," who is the one entitled to "claims for an injunction" (Article 3 of the Act) or "claims for compensation for loss or damage" (Article 4 of the Act).

(2) "Provided to specified persons"

"Specified persons" refers to those who will be provided with data under certain conditions. If specified, these persons will satisfy this requirement regardless of the number of persons actually provided with data.

Specific examples that are in principle considered to fall under the category of "specified persons"

- Those paying to receive data that is provided to anyone who pays the fee
- Those joining a data sharing consortium that only qualified people can belong to

2. "Accumulated to a significant extent by electronic or magnetic means" (Significant accumulation)

The spirit of the requirement of significant accumulation is to protect electronic data such as big data and similar information that is accumulated as far as it remains useful. Note that the requirement of "electronic or magnetic means" is defined in view of the characteristics of electronic data as the target.

(1) "To a significant extent"

Shared data with limited access, which is provided on a regular basis, applies to those which are valuable, as considered conventionally, through accumulation by electronic or magnetic means while "to a significant extent" is to be determined according to the nature of the specific data. In a judgment, the value to be generated by accumulating specific data by electronic and magnetic means, the possibility of its use, its transaction price, and the labor, time, expenses, and other costs spent on collecting and analyzing it will be considered.

A part of accumulated collection of the holder's data would generate value in their accumulation, the possibility of their use, their transaction prices, and the labor, time, expenses, and other costs spent on collecting and analyzing them, and then, the said data is considered to be accumulated to a significant extent.

Specific examples that are in principle considered to satisfy "significant accumulation"

- Data where, if a business operator that is accumulating nationwide, positional information on mobile phones extracts and sells any data for a specific area (such as for the Kasumigaseki area, Tokyo), then the data for that particular area too is considered to have transactional value by being accumulated by electronic and magnetic means
- Any portion of data in a database created based on the traveling history of a vehicle that has become valuable by being accumulated by electronic and magnetic means even if the data is not provided to customers
- Data from the analysis of large amounts of previously accumulated meteorological data that is summarized in patterns in typhoon movement affecting specific regions, created through investments in labor, time, capital and other expenses
- A collection of data that is required to run a specific program that was created by investing labor, time, expenses, and other costs to analyze and examine the data

3. "Managed by electronic or magnetic means" (Electromagnetic management)

The requirement of electromagnetic management is meant to ensure both predictability for a third party other than specified persons and the stability of economic activities, by clarifying to outside parties the intention to control data as something to be provided to specified persons when the holder of the data provides the data, as Article 2-7 of the Act sets forth "that … is managed by electronic or magnetic means … as information to be provided to specific persons."

(1) Electromagnetic management

For the electromagnetic management requirements to be satisfied, it is necessary to ensure that a third party protects the intention of the holder of any data to control the data as something to be provided exclusively to specified persons.

The specifics of the management measures and the degree of management vary with the nature of the data and other circumstances, but the data needs to be controlled in ways that allow a third party to easily understand how the data is managed.

Applicable measures need to be engineered and implemented that prevent anyone other than the data holder and those who have received any such data from the relevant holder (specified persons) from accessing the data, that is, a technology that limits such access.

Access is generally limited by user authentication by using so-called two- or three-factor authentication which consists of such elements as ID and a password (Something You Know); an IC card, a specific terminal, and a token (Something You Have); and biometric information (Something You Are) (this applies to cases where, in encrypting data, a measure is taken that allows access for specified persons alone, such as by ensuring that the encrypted data are decrypted after user authentication). Moreover, utilizing leased lines for transmission is

similarly considered to fall under the category of access-limiting technology.

1) Authentication technology

Permissible methods include the use of one of the authentication technologies listed below, a combination of any two of them, or a combination of an authentication technology with an encryption technology.

Specific examples of "authentication technology"

- ID, password, IC card, token, biometric authentication (facial features, fingerprint, vein, iris, sonogram, etc.), electronic certificate, IP address[1]
- Product activation (including antilocking)

Specific examples of "encryption technology" used in combination with authentication technology

- Encryption of data, encryption of communication, and encryption of websites and email communication
- Encryption that prevents non-subscribers from viewing images

Specific examples that are in principle considered to satisfy the "electromagnetic management" requirements

- Limiting access with user authentication procedures including ID and password
- Limiting access by using two or more authentication technologies, such as ID, password, and/or fingerprint and/or facial authentication, etc.
- A method that involves encrypting data, then limiting access with the help of facial authentication technology
- A method that involves limiting access with the help of user authentication by means of ID and password over VPN[2]

2) Leased line

One conceivable access-limiting technology is the use of a leased line that blocks interference by a third party who is someone other than the specified person(s).

---

[1] This refers to the unique combination of numbers assigned to each computer that connects to the internet. (From the Information Security Website for Japanese Nationals run by the Ministry of Internal Affairs and Communications at http://www.soumu.go.jp/main_sosiki/joho_tsusin/security_previous/index.htm)

[2] VPN (Virtual Private Network): This [is] a method of using a typical subscriber's telecommunication line as if it were a leased line. It is creatively designed to maintain safety by means of authentication or encryption technology. (Excerpts from "A Leaflet for Measures to Combat Information Leaks by Encryption" by the Information-technology Promotion Agency, Japan (IPA) available at https://www.ipa.go.jp/security/antivirus/documents/12_crypt.pdf)

3) Where electromagnetic management does not apply

"Electromagnetic management" is considered not to apply when a measure is taken that prevents duplication of specific data but access to the data is not controlled.

> **Specific examples that are in principle not considered to satisfy the "electromagnetic management" requirement"**
>
> - When data recorded onto a DVD allow access but not duplication

4. Technical or business information

Article 2-7 of the Act stipulates that what it protects is "technical or business information."

(1) The concept of "technical or business information"

"Technical or business information" applies to a wide range of information in use (or meant for use). More specifically, "technical information" includes map data*, machine operational data, data sets (learning data sets)[3] for developing (learning) AI-based[4] software, learned models[5] obtained from such learning, and other information. "Business information" involves consumption trend data, market research data, and other information.

*"Data" in the Guidelines includes text, image, audio, video, and similar information.

On the other hand, the Act does not explicitly define or specify certain information as illegal or harmful information that violates public order and/or morality, which can be regarded as similar to the above. However, in view of the objectives of the Act ("fair competition among undertakings" and "contributing to the sound development of the national economy"), such information presumably does not fall under the category of technical or business information to be protected.

Moreover, a person that is entitled to file for injunctions (Article 3 of the Act) and/or loss or damage(Article 4 of the Act) is defined as "a person whose business interests have been infringed on" or "a person whose business interests are likely to be infringed on." Providers of data or information violating public order and morality, when considered in view of the

---

[3] This refers, as opposed to raw data, to secondary processed data generated to facilitate an analysis with the target learning method by removing or otherwise pretreating missing values, outliers, and other values, adding label information (correct solution data) and other separate data, or combining them and converting or processing them (from "AI Guidelines").

[4] Similarly to Contractual Guidelines on the Use of Artificial Intelligence and Data: Artificial Intelligence (June 2018) (hereinafter, "AI Guidelines") (http://www.meti.go.jp/press/2018/06/20180615001/20180615001-3.pdf), "AI technology" in these Guidelines means machine learning or a series of software technologies related thereto. The AI Guidelines describes "machine learning" as "one of the learning methods for discovering certain rules in some data and realizing the estimation, prediction, or other operation on unknown data accordingly."

[5] This refers to an "inference program" incorporating learned parameters [parameters (factors) obtained from learning by means of a set of learning data] (from "AI Guidelines").

objectives of the Act, do not fall under the category of a person whose business interests have been infringed on or are likely to be infringed on.

Specific examples that are in principle considered to fall under the category of information that is illegal or violates public order and morality

- Child pornography in image data format
- Ads for narcotics and other illegal drugs in data format
- Instances of slander or libel in data format, etc.

5. "Excluding information that is kept secret"

The "information" in the phrase "excluding information that is kept secret (secrecy)" is "trade secrets (Article 2-6 of the Act)." "Trade secrets" are information that is reasonably controlled by business operators as secret, while shared data with limited access are information designed to be provided exclusively to specific outsiders satisfying certain conditions.

This provision is intended to note such differences as those between "trade secrets" and shared data with limited access and to avoid overlaps between them by excluding "information that is kept secret" distinguishing "trade secrets" from shared data with limited access.

(1) Secrecy management

Secrecy management is specified as follows: "it is necessary that the intent to maintain confidentiality within of a specific company regarding a specific trade secret that it owns has been clarified to its employees by using appropriate confidentiality measures, thereby allowing the employees and other workers to recognize the said intention of confidentiality.[6]" Satisfying this requirement requires at least that the holder shows intention to control the said secret as confidential information. Shared data with limited access, too, may be electromagnetically controlled by ID, password, or other means, subjected to a measure that imposes on their provider "the obligation of non-disclosure to a third party*," and similar measures. If, however, these measures are limited to those designed to ensure profit or the like, and if they are implemented under a policy that allows the data to be known to any party that satisfies the objectives, then these measures are not based on the intention to keep such information confidential and therefore neither can the intention be objectively recognized. In such cases, therefore, such data presumably does not fall under the category of something "that is kept secret" in "excluding information that is kept secret" which is set forth in the definition of shared data with limited access in Article 2-7 of the Act.

*In agreements and other documents related to the provision of shared data with limited access, this concept may be defined with "non-disclosure to a third party" or other term different from

[6] Quoted from the Management Guidelines for Trade Secrets available at: http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20150128hontai.pdf

"disclosure."

Specific examples that are in principle considered to be "kept secret"

- When a business operator commissions part of its production process to an outside business operator and obligates the latter outside business operator to keep specific data confidential and then provides the latter with a medium containing the said data
- When, in a consortium of a limited number of members (only several of them) for joint research and development, a member corporation provides experimental data required for a specific research project to other members within the consortium, and if it obligates the other members to keep the data confidential and affixes an ID and a password to each such member that gives them access to the said data

Specific examples that are in principle not considered to be "kept secret"

- If a provider of a members-only database to which one can subscribe in exchange for a fee gives each of its members an ID and a password that give them access to specific data (in that case, the obligation of "non-disclosure to a third party" would not make the relevant data fall under the category of something that is "kept secret")
- When a consortium to which any member of a specific industry can become a member merely by applying collects data from its members, then uses a unique ID and password authentication system to provide each member with access to specific data (in that case, the obligation of "non-disclosure to a non-member" does not fall under the category of something "kept secret")

Note that secrecy management or the lack thereof may be judged differently according to the situation even when the same item of data is involved. For example, data that used to be electromagnetically managed by employees obligated to keep such data confidential with such obligations as "non-disclosure to a third party" can be separately protected as "trade secrets." One conceivable case is where a data holder finds value in sharing the data with a third party and begins supplying the data or finds and undertakes a business opportunity to sell the data to third parties for a specified fee. In that case, even if the internal management style of a company remains unchanged before and after the sale of specific data, it can be considered that the moment the data holder clarifies their intention to sell the data, their intention to keep them secret is lost and the said data ceases to fall under the category of something that is "kept secret." On the other hand, in these cases, the sale of such data may be abandoned before any of the data is ever sold. In such a case, the moment the data provider stops selling such data to a third party (someone outside the data provider) and announces its intention to keep the data

confidential again, and if the said data still satisfies the requirement of not being publicly known and other relevant requirements, then the data will be protected as "trade secrets" similarly to before the start of the sale thereof.

6. Information that is "the same as any information that has been made available to the public without compensation (open data)," which is excluded from application (Article 19-1-8b)

> *(Exclusion from Application)*
> *Article 19 (1) The provisions of Articles 3 through 15, Article 21 (excluding the part under Article 21, paragraph (2), item (vii)), and Article 22 do not apply to the act prescribed in the relevant of the following items for the classification of unfair competition set forth in that item:*
> *(viii) unfair competition set forth in Article 2, paragraph (1), items (xi) through (xvi)*
> *- any of the following acts:*
> *(b) the act of acquiring shared data with limited access in which the information accumulated to a significant extent is* ***the same as any information that has been made available to the public without compensation****, or the act of using or disclosing such acquired shared data with limited access;*

Data legally provided free of charge to a wide range of users without specification or limitation (hereinafter, "open data") is, accessible to anyone. The act of using or disclosing identical data to the open data regardless of whether it is labeled shared data with limited access is therefore exempted from Article 3 of the Act and similar provisions.

(1) "Information that has been made available to the public without compensation"

The term "without compensation" assumes that there is no need to pay a fee (free of charge) to receive data. This term "without compensation" is not considered to apply when, even if no money needs to be paid, the recipient must provide the recipient's own data in exchange for the data, or when data is provided to purchasers of a product accompanying the data, or in any other case where some kind of exchange of data is required in response to the economic value of the data.

Specific examples that in principle fall under the category of something "without compensation"

- When, at the time of data provision, money is not paid, but a specific license provision requires that "when a recipient of any data item wishes to quote it, they should indicate the source"
- When, at the time of data provision, no monetary payment is required in relation to the data itself, but when payment is required for the actual expenses of the

CDs or physical storage device containing the data, or the related shipping fees, or other expenses are incurred

- Data which anyone can access free of charge through the internet and for which the business operator earns money from advertisements

Moreover, "available to the public" means that the data is accessible to many unspecified people. This applies, for example, where anyone is free to access specific data published on a website. As described above, "information that has been made available to the public without compensation" applies also to any information accessible to many unspecified people although with certain obligations on use (such as that to specify the source explicitly), not only to information accessible on a wholly unconditional basis.

Specific examples that are in principle considered to apply to "information that has been made available to the public without compensation"

The shaded portion in the table below falls under the category of "information that has been made available to the public without compensation."

Among the information that can be provided to outside parties	For a fee	Free of charge
Unavailable to the public (accessible only to specified persons)	- Directories of customers shared with affiliates - Data provided for a fee within a consortium where shipping data is shared. - Map data for automated driving for paying subscribers - Typical court decisions on paying subscribers in data format - Articles shared on news websites limited to paying subscribers - Data provided within a consortium that people can join on condition that they provide data that they have saved for themselves - Map updates in data format provided only to purchasers of car navigation systems	- Data accessible to members of a relevant industrial organization - Images in data format uploaded on file-sharing websites accessible only to those who know the special URL - Information on jobs offered on information websites for job seekers to free-of-charge subscribers
Available to the public (accessible to anyone)	- Industrial research reports commercially sold in data	- Statistics provided by governments in data format

	format on CD-ROM (with its data not designed with user authentication technology based on ID, password, or similar methods)	- Shelter data provided by map suppliers in data format - Data freely accessible on the internet, but whose source is required to be referenced in every quote - Data that anyone can receive upon request free of charge and regarding which one only needs to pay the shipping fee and other expenses - Data viewable by anyone free of charge on the internet and for which the website owner earns money from ads on the website - Data for learners freely accessible and usable on the internet but for which the results of their use need to be made useful to the public

(2) "The same"

"The same" means that the data is the same as "open data."

For example, "open data" which is simply and mechanically rearranged is considered to remain virtually the same.

If, however, part of the shared data with limited access is virtually the same as "information that has been made available to the public without compensation," then that part will be exempt from the Act.

Specific examples that are in principle considered to be "the same"

Open data: statistics provided in data format by governments

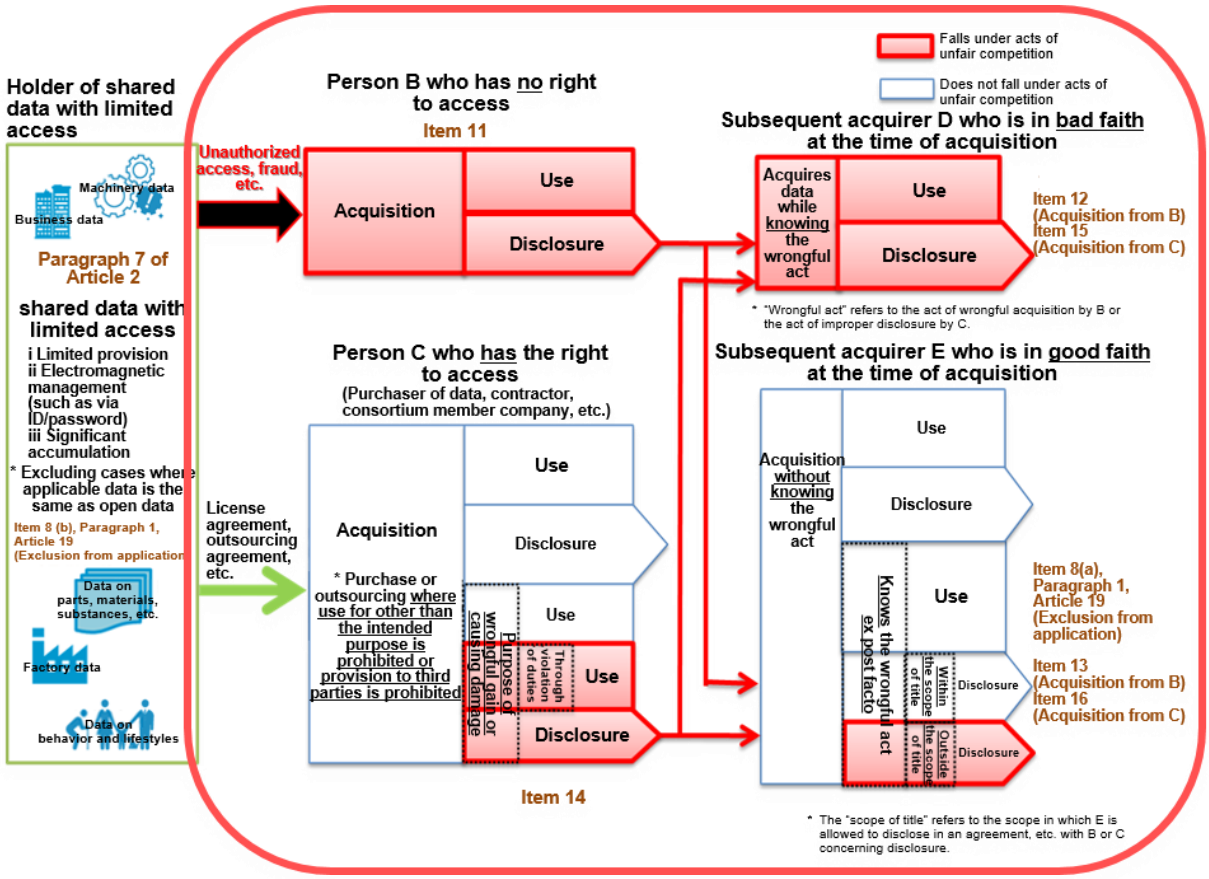
- When all the statistics are provided as they are without modification
- When statistics, whether in part or whole, are rearranged simply and mechanically (such as by rearranging a set of chronological data into ascending numerical order), or part of the statistics are removed simply and mechanically (such as by extracting only the data in and after 2010)
- When data provided is a combination of open data released by different governments or at different times existing statistics with other open data provided by a government (such as by linking the GDP growth rate of 2017 with

the GDP growth data of 2018 in chronological order)

"Shared data with limited access which is the same as any information that has been made available to the public without compensation" applies to any data in electronic format if the said data is the same as any "open data" which has been made available on paper only to the public without compensation.

III. Acts of "unfair competition" (general)

As for actions concerning shared data with limited access, in order to ensure a good balance in protection between the holders of shared data with limited access and users of the data, malicious actions such as the act of infringing directly on the profit of the holder of shared data with limited access are defined as "unfair competition" in order to promote the distribution and use of data on the whole (Articles 2-1-11 to 2-1-16 of the Act). Under these instances of "unfair competition," the acts of "acquisition," "use," or "disclosure" are defined.



1. The objects of the actions ("acquisition," "use," and "disclosure")

Articles 2-1-11 to 2-1-16 of the Act specify acts of "unfair competition" within the categories

of acts of "acquisition," "use," or "disclosure" of shared data with limited access. The objects of these actions need to be shared data with limited access. Shared data with limited access is set forth as information that is "accumulated to a significant extent and is managed by electronic or magnetic means … as information to be provided to specific persons on a regular basis" (Article 2-7 of the Act). It is therefore required that the object of "acquisition," "use," or "disclosure" be the whole of shared data with limited access provided by the holder of shared data with limited access or a part that satisfies accumulation to a significant extent(where the said part is judged to prove valuable in view of the value produced by accumulating it, the possibility of its use, its transaction price, and the labor, time, expenses, and other costs involved in collection and analysis).

If, however, portions that are not "accumulated to a significant extent" are acquired separately over time, eventually totaling "a significant extent", then the series of acts of acquisition together may be considered together and be subject to evaluation as "unfair competition."

*The same shared data with limited access as information that has been made available to the public without compensation is not subjected to filing for injunctions, damages or other compensation, or other disposition, even if acquired, used, or disclosed (Article 19-1-8b of the Act).

*For the above, see II. shared data with limited access.

2. "Acquisition"

"Acquisition" refers to obtaining control over data. Among the actions falling under this category are the act of owning data itself within a storage medium or the like containing the data, taking photos of a display screen image showing the data, and any other actions by yourself or a third party of possessing or maintaining control of the data in a manner that does not entail the movement of a storage medium or the like containing the data to a different location.

Specific examples that are in principle considered to fall under the category of "acquisition"

- The act of copying a data item stored on a server or medium onto your own PC or portable memory devices including USB memory
- When your environment allows you to use data in a domain or the like in the cloud related to your own account (in which case your case may fall under the category of "acquisition" even if you do not download your data onto your own PC or portable memory devices including USB memory)
- The act of copying any data stored in your company's internal server onto another medium
- The act of requesting someone else to send an email with an electronic file of data

attached to it and then the act of receiving the file (on the presupposition that the said file is not access-restricted or otherwise restricted and, if simply by opening the email, you will be able to know the contents of the data), or of forwarding the said email to a third party and having them receive it (the act of having a third party "acquire" it)

*Note that if you have obtained only an ID and a password with which you can access the data (and you have not received the data itself), then this case is not considered to fall under the category of "acquisition," but if it is highly probable that you may have "acquired" it, that is, if a data holder's "business interests are likely to be infringed on" (Article 3 of the Act), then the data holder can claim a preventive injunction on such "acquisition."

- The act of printing data out on paper and removing the paper from the vicinity
- The act of taking pictures and videos of PC or other display screen images showing data

3. "Use"

"Use" is the act of using data. More specifically, it presumably includes the act of using data in its preparation, analysis, and other operations.

Specific examples that are in principle considered to fall under the category of "use"

- The act of conducting research and development by using acquired data
- The act of manufacturing a commodity or preparing a program by using acquired data
- The act of analyzing and examining data in order to prepare a learning data set[7] for developing (learning) software based on AI technology[8] from acquired data
- The act of using acquired data in developing software based on AI technology
- The act of classifying and rearranging acquired data in an easy-to-search manner in order to prepare a new database
- The act of processing acquired data by data cleansing[9] or other techniques
- The act of combining acquired data with your own data collected elsewhere and building a database
- The act of engaging in sales and marketing by using acquired data

*Note that even in such stages as those where data acquired is only saved as it is, and if it is highly probable that the data will be subsequently "used" or "disclosed" in a manner violating the Act, that is, if a data holder's "business interests are … likely to be infringed on" (Article 3 of the Act), then it will

7 See II. 4.

8 See II. 4.

9 "Data cleansing" refers to correcting and otherwise handling differences in notation in order to improve data consistency or quality.

be possible for the data holder to file a preventive injunction with regard to "use" or "disclosure." As a result, the person responsible may be requested to delete any data saved.

If a product created from the use of acquired data (a learned model generated by causing a device to learn from data, such as a commodity or the like developed based on the data) is evaluated as something no longer the same as the original shared data with limited access, the act of using, transferring, or otherwise handling it does not fall under the category of unfair competition.
However, if any such product is evaluated as virtually equivalent to data acquired by the relevant product, or evaluated as containing something virtually equivalent to such data, such as in the case of a database containing acquired data as it is, then the act of using the said product is considered to fall under the category of "use" of acquired data.

4. "Disclosure"

"Disclosure" refers to placing data in a state where a third party can see or access it. It is unnecessary for a third party to actually see or access it, nor is it considered to be necessary for the party at the other end of the "disclosure" to actually "acquire" the data*.
*For example, posting data on a website accessible to anyone presumably falls under the category of disclosure.
Also note that the act of disclosing a database or other product generated by using acquired data falls under the category of "disclosure" of the original data, similarly to the case of "use," if the said product is considered to be virtually equivalent to the original data or to contain something virtually equivalent.

Specific examples that are in principle considered to fall under the category of "disclosure"

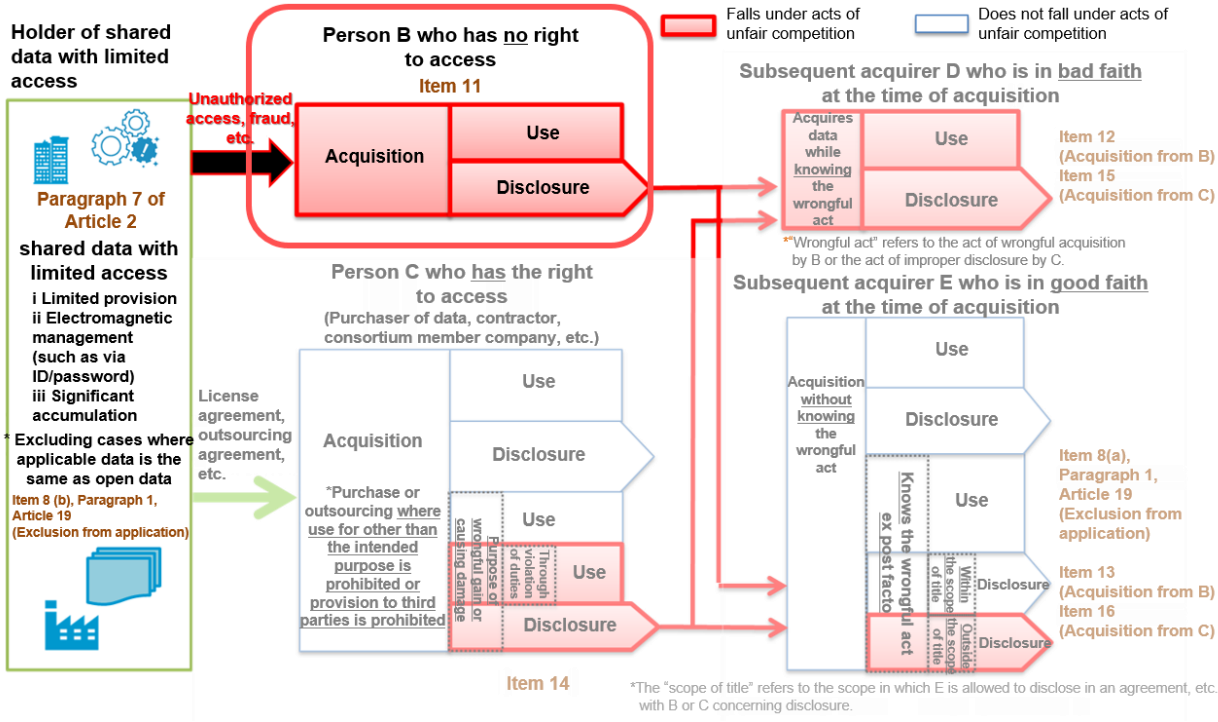
- The act of handing a data-containing medium (including paper) to a third party
- The act of posting data on a website accessible to a third party
- The act of emailing an electronic file containing data to a third party (regardless of whether the email is opened or not)
- The act of establishing a third party's right of access to acquired data in Excel format in a server where the data is saved under a PDF format
- The act of saving data on a server, then notifying a third party in writing or orally of the password with which to access the said website together with the URL of that server
- The act of displaying large quantities of data on the display or screen of a tablet, Smartphone, or other terminal, then giving a third party access to the same

Note that if a product that is obtained by using acquired data (a learned model generated by causing a device to learn the data, a commodity developed by using the data, or the like) is evaluated as no longer the same as the original shared data with limited access, then the said transfer or other action will not fall under the category of unfair competition.

IV. The category of unauthorized acquisition

Article 2 (1) The term "unfair competition" as used in this Act means any of the following:

(xi) the act of acquiring shared data with limited access ***by theft, by fraud, by duress, or by other wrongful means*** *(hereinafter referred to as an "act of wrongful acquisition of shared data with limited access"); or the act of using or disclosing shared data with limited access acquired through an act of wrongful acquisition of shared data with limited access;*



Among the actions falling under the category of "unfair competition," the category of unauthorized acquisition of shared data with limited access (hereinafter, the category of unauthorized acquisition") is set forth in Article 2-1-11 of the Act. This category of unauthorized acquisition regulates such acts as that of acquiring shared data with limited access by malicious means ("by theft, by fraud, by duress, or by other wrongful means").

1. "By theft, by fraud, by duress, or by other wrongful means"

Among "theft, fraud, duress, or other wrongful means," "theft," "fraud," and "duress" are cited as examples of wrongful means. "Other wrongful means" refers not only to actions falling under the category of theft, fraud, and other criminally punishable acts but also to actions that use methods that violate public order or morals which are conventionally considered to be equally illegal.

That is, these "other wrongful means" are expected to include violations of the Act on Prohibition of Unauthorized Computer Access (hereinafter, "the Unauthorized Computer

Access Prevention Act"), violations of the Penal Code such as using computer viruses and using inappropriate methods to circumvent restricted access measures including disabling or disrupting ID, password, encryption or other security methods, in violation of standards of public order and morality.

Specific examples that are in principle considered to fall under the category of acquisition by "wrongful" means

- The act of stealing USB or other memory devices where data is saved
- The act of entering the premises of the data holder, printing data out on paper, or copying and saving it on your own portable memory devices including USB memory, and removing it from the premises
- The act of impersonating a rightful data recipient, sending an email to the data holder, instructing the latter to store the data in a server that you manage, and in so doing mislead the data holder into believing that the email is from a person legitimately authorized to store the data on your server
- The act of sending a computer virus to the data holder and obtaining the data saved in a closed server that their company manages through those means
- The act of breaking into a PC of another company via a network without authorization in order to test if your own company's product works on it properly, nullifying the password, and acquiring the data in the process of studying the mutual technical compatibility or other characteristics of the product with those of the other company
- The act of acquiring data by impersonating someone who is authorized to access specific data and acquiring a password with which to access the data

*Note that if you have acquired an ID and a password with which to access specific data (without acquiring the data itself), and if the action is not considered to fall under the category of "acquisition," then a data holder may seek a preventive injunction to prevent "acquisition" if "acquisition" is highly probable and the data holder's "business interests … are likely to be infringed on" (Article 3 of the Act).

2. Cases presumably not falling under the category of "unauthorized acquisition"

If, for example, the objectives of a specific operation are found to be rightful under other Acts (such as in the case of a legitimate operation under the Copyright Act), then the said operation will, in view of the rightfulness thereof, not be considered to fall under "the act of acquiring shared data with limited access by theft, by fraud, by duress, or by other wrongful means" (unless there is a violation of the Penal Code, the Unauthorized Computer Access Prevention Act, or other act).

Specific examples that are in principle not considered to fall under "acquisition" by "other wrongful means"

- The act, by a repair agent for gaming machines or similar machinery, of making a backup copy, to a necessary degree, of shared data with limited access which is stored in the consoles, in the process of maintenance, repair, or replacement of a gaming machine or terminal, and to unprotect the machine in a manner that does not violate the Unauthorized Computer Access Prevention Act and restore to its original state after a repair or the like, e.g. cases where the repair agent has not acquired all the licenses from the machinery manufacturer although an agreement made at the machine's time of sale did not explicitly specify whether it was prohibited to undo the protection.
- The act of unprotecting a specific product without connecting it to a network in a manner that does not violate the Unauthorized Computer Access Prevention Act and acquiring a specific range of shared data with limited access that is required in order to ensure the correct performance of the specific rival product purchased in the market in the process of studying its mutual technical compatibility or other characteristics with a product manufactured by a competitor, including cases where it is not always possible to obtain the consent of all the companies with whom mutual compatibility needs to be ensured although an agreement made at the time of sale of the product did not explicitly specify whether it was prohibited to unprotect the machine.

*Note that if a specific business merely avoids electromagnetic control of the data and does not intend to acquire the data, this practice presumably does not fall under "acquisition" under this item.

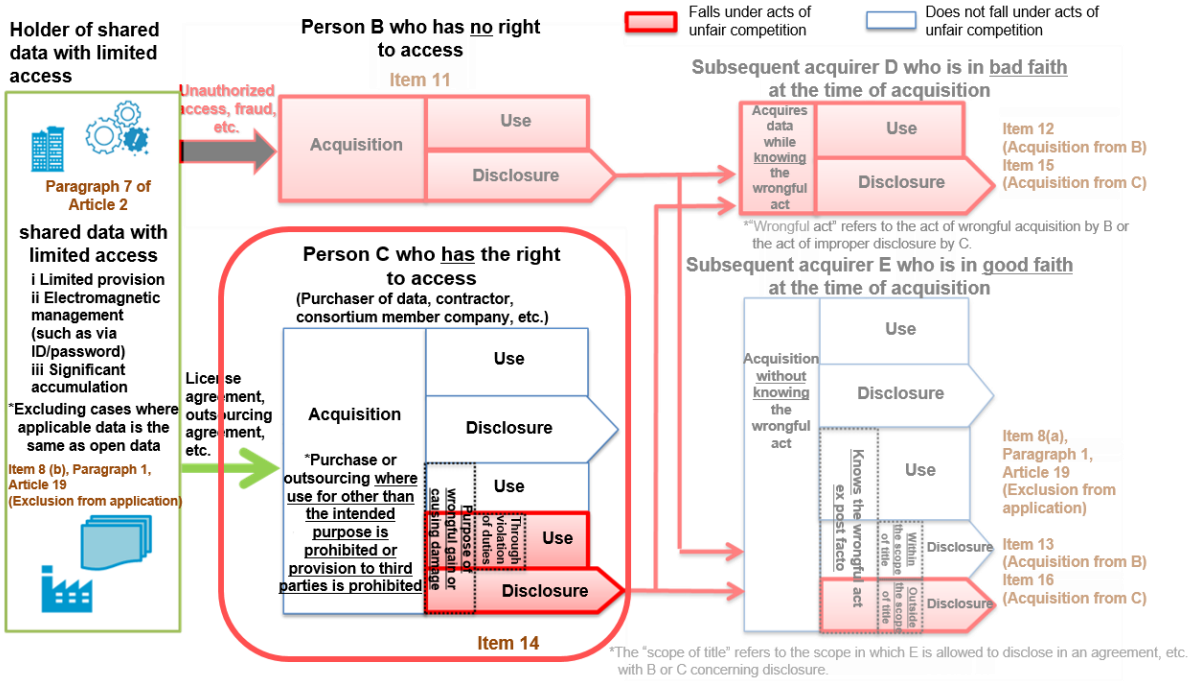
*If unprotection is explicitly tolerated or unprotection is conducted upon request or with consent, then such a practice will fall under the acquisition of shared data with limited access under Article 2-1-14).

- The act, by a server operator who is separate from the data holder, of decrypting an encryption key urgently without the prior consent of the data holder when a threat such as virus infection, flooding, or other risk occurs that may result in the loss of the server where encrypted data is accumulated for specified persons and making a backup copy in another server.
- The act of acquiring shared data with limited access without the authorization of the data holder in order to check the data and to take the necessary measures against a virus or other potential source of harm.
- The act, by the purchaser of a specific product manufactured by a 3D printer, of using a 3D scanner to obtain shape data from the product, which is shared data with limited access.

V. Category of significant violations of the principle of good faith

Article 2 (1) The term "unfair competition" as used in this Act means any of the following:

(xiv) the act of using or disclosing shared data with limited access disclosed by an undertaking holding that data (hereinafter referred to as the "holder of shared data with limited access"), ***for the purpose of wrongful gain or causing damage to that holder of shared data with limited access*** *(using the relevant data for that purpose is* ***limited to an act conducted in breach of the duties regarding the management of that data****);*



Of all actions falling under “unfair competition,” the act of using or disclosing it to a member, employee, or other workers of an outsourcing partner, licensee, or consortium in a manner that violates the terms set out by the holder of shared data with limited access, for the purpose of wrongful gain or causing damage to the holder, is defined as “unfair competition” under Article 2-1-14 of the Act, because the said act is a malicious act significantly violating the principle of good faith.

“Shared data with limited access disclosed by an undertaking holding that data” refers to cases where the said data is acquired from the holder in a manner other than wrongful acquisition, such as the receipt of shared data with limited access under an agreement.

Moreover, wrongful use is subjected to an aggravating requirement to the effect that it is “limited to an action conducted in breach of the duties regarding the management of the shared data with limited access,” thereby limiting cases falling under “unfair competition.”

That is, “unfair competition” includes “uses satisfying requirements 1) and 2)” and “the act of disclosure satisfying requirement 1)” specified below:

1) "for the purpose of wrongful gain or causing damage to the holder of shared data with limited access (for the purpose of wrongful gain or causing damage)
2) Actions taken in breach of the duties regarding the management of the shared data with limited access.

1. For the purpose of wrongful gain or causing damage to that holder of shared data with limited access

For the use or disclosure of acquired data by the person to whom the holder of shared data with limited access has disclosed specific data (hereinafter, "the rightful acquirer") to fall under "unfair competition," it is necessary that there be a purpose of wrongful gain or causing damage*.

The purpose of wrongful gain or causing damage is a subjective requirement that limits the scope to cases where the act of using or disclosing data rightfully acquired from the holder of shared data with limited access under a license agreement, business commissioning agreement, or related contract, still falls under "unfair competition" beyond mere contract violations, in order to avoid excessively affecting appropriate business activity.

Consequently, when determining whether requirements for the purpose of wrongful gain or causing damage are satisfied, the premise is that it is obvious for both parties concerned that the relevant act of use or disclosure is not permitted by the holder of shared data with limited access, and that the violating party, as a rightful acquirer of shared data with limited access, are aware of such fact. Note that any such act of use or disclosure for a rightful purpose should be interpreted as not falling under "unfair competition."

*Note that any use only by a rightful acquirer is also subject to a requirement that it should be "conducted in breach of the duties regarding the management of the shared data with limited access" (to be explained later in 2.).

(1)If there is considered to be a purpose of wrongful gain or causing damage

If the requirements (i) and (ii) below are satisfied, that is, when it is obvious to both parties concerned that the relevant act of use or disclosure is not permitted by the holder of shared data with limited access, and that as the rightful acquirer, the other party is aware of such fact and still attempts to use or disclose the acquired data for the purpose of wrongful gain either for themselves or for a third party, or of causing damage to the data holder, then the action is considered to have a purpose of wrongful gain or causing damage.

	Use	**Disclosure**
(i)	If it is obvious from the contents of the agreement or the like that you are obligated not to use a specific data item in a particular manner,	If it is obvious from the contents of the agreement or the like that you are obligated not to disclose a specific data item to a third party[*1],

	and if you are aware of it,
(ii)	and yet, in violation of the said obligation, the party uses or discloses the acquired data for the purpose of wrongful gain for themselves or a third party or of causing damage to the data holder[*2]

Case (iii), however, is considered not to contain the purpose of wrongful gain or causing damage.

(iii)	If a rightful purpose is involved

*1 As for the range of "third parties" to whom disclosure is to be prohibited, it is desirable for an agreement to clarify whether they include one's subsidiaries, affiliates, or other entities. Some agreements and similar documents may use "non-provision to a third party" or other terms different from "disclosure to a third party."
*2 "The purpose of wrongful gain" is considered to involve not only the purpose of engaging in competitive enterprise but also the purpose of seeking wrongful gain over a wider range in a manner violating public order or morality or the principle of good faith. Consequently, rendering services that directly compete with the holder of shared data with limited access can be a factor in determining the purpose of wrongful gain, but is not a necessary requirement.
Note that "the purpose of causing damage to the holder (the purpose of causing damage)" refers to the purpose of causing property damage, compromising confidence or reputation, or other corporeal or incorporeal wrongful damage, but without the necessity of generating actual damage.

Specific examples where you are in principle considered to have "the purpose of wrongful gain or causing damage"

- If shared data with limited access is acquired under a license agreement that prohibits its disclosure to a third party, and some of the said data is disclosed to clients through a company's service while being aware that its disclosure to a third party is prohibited
- If shared data with limited access is acquired under a license agreement that prohibits its disclosure to a third party, and the data is disclosed on a website in order to cause damage to the data holder while being aware that its disclosure to a third party is prohibited
- If shared data with limited access that is acquired on condition of use only for specific commissioned analysis, and the data is used for developing a new in-house product without authorization, despite the knowledge that it violates the condition

(2) If there is considered to be no purpose of wrongful gain or causing damage

If a specific action is considered to be permitted under the particular agreement, you are

considered not to have the purpose of wrongful gain or causing damage. If, on top of that, there is a conflict in the interpretation of the agreement and a specific operation is eventually determined to constitute a contract violation, then the following categories can be considered to have no purpose of wrongful gain or causing damage:

1) Categories not considered to fall under "awareness of obligation" [Table (1) (i)]

(a) If it is unclear in the agreement that there is an obligation not to use shared data with limited access for an unspecified purpose or to disclose it to a third party

(a 1) If there is a conflict over the interpretation of the agreement regarding the range of permitted use or disclosure

If the range of permitted use or disclosure is unclear to the concerned party under the agreement*, and if they think that they are allowed to use or disclose specific data in the relevant manner and have actually used or disclosed it, then they are considered not to have the purpose of wrongful gain or causing damage in principle even if the said manner is judged to have exceeded the range permitted under the agreement.

*To avoid any such incident, the data holder should explicitly specify in the agreement the range of permitted use and disclosure.

Specific examples where you are in principle considered "not to have the purpose of wrongful gain or causing damage"

*The premise is that, although unclear in the phrasing used in the agreement, the operation in question has been considered to have been an unpermitted form of use or disclosure.

- If shared data with limited access is acquired on condition that it be used in a specific system configuration and yet, in view of the industry's trade practices where system upgrades occur frequently, the data is used in a system configuration that deviates from the relevant regulations
- If shared data with limited access is acquired under a license agreement that prohibits its disclosure to a third party, and the data is disclosed to a data analysis/processing agency to be returned under the assumption that, if this is done exclusively for the data used, the said operation can be regarded as internal and then the said operation is within the scope of the license

(a 2) If there is a conflict over the contractual interpretation of procedures after the termination of a contract or how to handle a contract renewal

If you are unclear about when to terminate the relevant contract, whether to renew it, what its terms and conditions should be, and other matters under the relevant contract, and if you have continued to use or disclose the data under the contract as before, expecting that the contract will be renewed, then it cannot be concluded that, even if the contract is deemed to have been terminated while the relevant use or disclosure continued, you intended to obtain "a wrongful gain." You are therefore in principle presumed not to have intended to obtain a wrongful gain and/or cause damage.

Specific examples where you are in principle considered "not to have the purpose of wrongful gain or causing damage"

*The premise is that, although unclear in the phrasing used in the agreement, the operation in question has been considered to have been an unpermitted form of use or disclosure.

- If the relevant license agreement is unclear about whether or how to renew the relevant contract, and if you have continued to use the shared data with limited access, intending to keep paying royalties to the data holder after the termination of the contract
- If you have provided your clients with shared data with limited access purchased from its holder as incorporated into a database of your own making, and if at the time of contract renewal concerning the shared data with limited access, you have negotiated its pricing with its holder in the hope of upgrading the data to be acquired, but, because the negotiations have been prolonged, you have kept the data disclosed between the termination of the contract and the contract renewal

(a 3) For actions taken while negotiating a contract

In such actions you are in principle not considered to have intended to obtain a wrongful gain and/or cause damage in that you eventually expected your use or disclosure to come within the scope of the contract, if you used or disclosed the data under the assumption that you expected your action to be justified ex post facto under circumstances where the contract will naturally be established or you thought your action was implicitly permitted, in negotiating the contract, even if afterwards the contract eventually was not established.

Specific examples where you are in principle considered "not to have the purpose of wrongful gain or causing damage"

*The premise is that your use or disclosure has been deemed to be in a manner not permitted by the holder.

- If, in the stage where you are considering receiving a license, you assume that shared data with limited access acquired from the holder as a sample is within the permitted scope of use and go on to use it to determine its usability for your company's business
- If you proceed to disclose a database of shared data with limited access that was previously accessible only to consortium members to nonmember companies who have begun to sign up for the consortium, believing that their future membership implies permission to do so

(b) If you are unaware of your obligation

If you are unaware of your obligation of non-use for any unspecified purpose and of non-disclosure to a third party, then you may be held responsible for failing to fulfill your obligations in violation of the contract but will be considered not to have intended to obtain a wrongful gain and/or cause damage. However, if an employee or other worker were to actually use or disclose shared data with limited access within the organization despite being unaware of their said obligation, but the person in charge or other representative who specified a possible range of use or disclosure was aware of the inappropriate nature of the activity, then the said person in charge or other representative is considered to have been aware of the said obligation before use or disclosure of the said data and may be deemed to have intended to obtain a wrongful gain and/or cause damage.

Specific examples where you are in principle considered "not to have the purpose of wrongful gain or causing damage"

*The premise is that your use or disclosure is deemed to have been in a manner not permitted under the agreement

- If you have acquired data with such conditions as the objectives of use, non-disclosure to a third party, and other requirements under a license agreement, but nevertheless, one of your employees discloses such data to a customer while unaware of the conditions

2) A category considered not to fall under "the purpose of wrongful gain for oneself or a third party or causing damage to the holder of shared data with limited access in violation of its own obligation" [Table (1) (ii)];

(a) Violation caused by negligence

Even if you are aware of your obligation of non-use for any unspecified purpose and non-disclosure to a third party, and if your use or disclosure of the said data exceeds the scope permitted under the agreement negligently, you may be held responsible

for having failed to fulfill your obligations under contract terms, but will be considered not to have intended to obtain a wrongful gain and/or cause damage.

Specific examples where you are in principle considered "not to have the purpose of wrongful gain or causing damage"

*The premise is that your use or disclosure has been deemed to be in a manner not permitted under the agreement.

- If you are aware that you are licensed to use shared data with limited access solely for the purpose of using it for developing software A based on AI technology, and yet you have mistaken software B for software A and proceed to use the data for teaching software B
- If, as a corporate employee, you have acquired shared data with limited access under a license agreement that states non-disclosure to a third party, and even despite awareness thereof, a clerical error results in disclosing the data to another company
- If any shared data with limited access that you have acquired under a license agreement that states non-disclosure to a third party is leaked due to unauthorized access or the like by an outside party to your corporate server, resulting in disclosure of the data to a third party

(b) An action taken on behalf of the holder of shared data with limited access

If you are violating the agreement specifically for the benefit of the holder of shared data with limited access, and if the action is protected to a certain degree under the Civil Code as management of business (Article 697 of the Civil Code), even though you are aware of the violation, your action may not be regarded as violating the Act and will be considered not to have been intended in order to obtain a wrongful gain and/or cause damage.

Specific examples where you are in principle considered "not to have the purpose of wrongful gain or causing damage"

*The premise is that your use or disclosure is deemed to have been in a manner not permitted under the relevant agreement.

- If you consign shared data with limited access whose disclosure to a third party is prohibited under a relevant consignment agreement to ensure safety in data storage
- When you knowingly employ more efficient methods than specified in the relevant consignment agreement to save resources in processing the shared

data with limited access obtained for that purpose in order to aid the data holder

(c) In any other presumably unavoidable case

If you are obliged to keep using or disclosing shared data with limited access because you cannot contact the holder of shared data with limited access or for any other reason that is found to be attributable to the responsibility of the holder of shared data with limited access, then you are considered not to have intended to wrongful gain and/or cause damage.

Specific examples where you are in principle considered "not to have the purpose of wrongful gain or causing damage"

*The premise is that your use or disclosure is deemed to have been in a manner not permitted under the relevant agreement.

- If, after the termination of the agreement, you send a written offer to renew your agreement to the holder of shared data with limited access by content-certified mail, and have not received a reply from the holder of shared data with limited access in the one month afterwards, and consequently keep using the shared data with limited access for developing software based on AI technology to avoid suspending your business.

3) The category presumed to fall under "where there is a justifiable purpose for such actions" [Table (1) (iii)]

If you are doing something that falls under the category of being conducted urgently to protect data, or if such is required under law, or if you are required to submit any such data to authorities in order to determine the presence or absence of a crime or prosecution, or if any other reason related to public welfare is recognized that exceeds the protectable interests of the holder, then your provision of any such data to the required degree is considered not to have been intended to obtain a wrongful gain and/or cause damage.

Specific examples where you are in principle considered "not to have the purpose of wrongful gain or causing damage"

*The premise is that your use or disclosure is deemed to have been in a manner not permitted under the relevant agreement.

(a) If urgently necessary to protect the data

- If there arises an urgent need to maintain your data storage equipment, but you had no other data storage equipment within your company, so that you have to disclose the shared data with limited access to a subsidiary to which you are not licensed to disclose the data, for the purpose of temporary storage
- If you disclose virus-infected shared data with limited access to a third-party company in order to detect the virus, for decontamination, or other purpose, in order to prevent the virus from spreading, despite the fact that disclosure to a third party is prohibited

(b) If under law

- If you must disclose shared data with limited access in response to a search under a warrant issued by a judge
- If you must disclose shared data with limited access in response to a survey under the law
- If you must disclose shared data with limited access to create a report under the law

(c) To protect human life or for any other reason or cause that falls under "for the sake of public welfare"

- If you disclose shared data with limited access to a local government, to whom you are not allowed to disclose traffic information, in order to help guide traffic to safety in the case of a disaster
- If you disclose data about human flows in commercial facilities to a third party, to whom you are not allowed to disclose such data, in order to protect human lives

2. Actions "taken in breach of the duties regarding the management of the shared data with limited access"

If you (a rightful acquirer) have only used data acquired lawfully (that is, without disclosing it), then making it "unfair competition" requires that you have since intended to obtain a wrongful gain or cause damage (1) as described above, and that you have "taken action in breach of the duties regarding the management of the shared data with limited access" (2).

In this category, the data acquisition itself occurred lawfully. To ensure that the data is properly distributed, therefore, it is crucial not to allow the acquirer's business activities to be negatively affected. And then, this requirement has been stipulated only for malicious acts.

(1) If there presumably are "duties regarding the management of the shared data with limited access"

For it to be presumed that "duties regarding the management of the shared data with limited access" exist, in view of the fact that this requirement is regarded as an aggravating requirement separately from the purpose of wrongful gain and causing damage (1), it is necessary that there be presumed duties for the sake of the holder of shared data with limited access, instead of being a mere agreement concerning data.

More specifically, that "duties regarding the management" exist, refers to cases where there is a relationship of consignment and entrustment between the concerned parties in which the duties are fulfilled on behalf of the holder. The presence or absence thereof is determined by examining actual circumstances.

If, for example, you undertake data processing for the holder of shared data with limited access, there is presumed to be a relationship of consignment and entrustment. On the other hand, if you have purchased data or the like for yourself (e.g. to develop a new product), then there is presumed to be no relationship of consignment and entrustment.

Note that if your intention (as a rightful acquirer) to do something on behalf of the holder of shared data with limited access is combined with the intention to do so for yourself, and if it is considered to be an action on behalf of the holder, then "duties regarding the management of the shared data with limited access" are considered to exist.

Moreover, if "duties regarding the management of the shared data with limited access" are determined not for each agreement but for each target data item, and if they constitute an action taken for the holder of "shared data with limited access" concerning a data item, then, even if you (the acquirer) are handling other data not managed for the holder of "shared data with limited access", the "duties regarding the management of the shared data with limited access" will presumably not be denied concerning the relevant data.

Specific examples concerning the presence or absence of "duties regarding the management of the shared data with limited access" under various agreements

The following are conceivable agreements for providing shared data with limited access. The examples given below presuppose that you intend to wrongful gain and/or cause damage and use the shared data with limited access in a manner not permitted under the relevant agreement.

Note that the title of a specific agreement alone is not enough to establish what "duties regarding the management of the shared data with limited access" are included in the agreement.

Moreover, who is to become the data holder will be determined in each specific project depending on the specific business model or other circumstance concerning the management of the data that is targeted by the unauthorized actions.

Typical agreement type	An example presumably involving "duties regarding the management of the shared data with limited access" (where there is an action that is found to be "conducted for the benefit of the holder of "shared data with limited access")	An example where there are no "duties regarding the management of the shared data with limited access"
Consignment agreement	In the case of analysis with "shared data with limited access" under commission from the holder of shared data with limited access (an example presumably involving "duties regarding the management of the shared data with limited access" in that there occurs a duty of diligence regarding data management for the consignor due to being commissioned to analyze data)	— (In a consignment contract regarding shared data with limited access, there is commonly presumed to be a confidential relationship where the consignee is to do work for the consignor. In that case, therefore, you cannot easily assume that there are no "duties regarding the management of the shared data with limited access".)
Franchise agreement	When under a franchise agreement, a franchise branch that is both a franchisee and a sub-franchiser uses data acquired from the franchise headquarters in its own franchise business (a case where the franchise branch manages its own franchisee not as a mere franchisee but for the franchise headquarters, so that there are presumed to be "duties regarding the management of the shared data with limited access")	When under a franchise agreement a franchisee uses data acquired from its franchiser for its own franchise business (An example where there are not presumed to be "duties regarding the management of the shared data with limited access" unless there are circumstances showing that the franchisee is to manage the data not merely as a franchisee but particularly for the sake of its franchiser)

Consortium agreement	When data used jointly by a consortium organized to implement a specific joint project is used in order to promote the particular project (an example where there are presumed to be "duties regarding the management of the shared data with limited access" in that the user is using the data not only for its own but for the other members of the consortium as well)	When data provided to corporate members of a trade group is used by the members for their own sakes only (An example where the members use the data for their own sakes only, so that there are not presumed to be "duties regarding the management of the shared data with limited access")
Licensing agreement	When an equipment user (where the data holder is the licenser) has licensed an equipment manufacturer (where the data acquirer is the licensee) to use the operational data on its own equipment, the equipment manufacturer is allowed to use the operational data to upgrade its own machinery but is obligated to use it to maintain the relevant machinery owned by the machinery user [An example where there are presumed to be "duties for the management of the shared data with limited access" in that the data acquirer (equipment manufacturer) is allowed to use the data for its own business but is obligated to use it for the data holder (equipment user) to conduct maintenance]	When an equipment user (where the data holder is the licensor) has licensed an equipment manufacturer (where the data acquirer is the licensee) to use the operational data on its own equipment and the equipment manufacturer uses the operational data to upgrade its own equipment alone (An example where there are not presumed to be "duties regarding the management of the shared data with limited access" because there are no circumstances showing that the licensee is to control the data not as a mere licensee but specifically for the licensor)

VI. Category of subsequent acquisition

Category of subsequent acquisition in bad faith at the time of acquisition
Article 2 The term “Unfair Competition” as used in this Act means any of the following:
(xi) the act of acquiring shared data with limited access by theft, by fraud, by duress, or by other wrongful means (hereinafter referred to as an "act of wrongful acquisition of shared data with limited access"); or the act of using or disclosing shared data with limited access acquired through an act of wrongful acquisition of shared data with limited access;
(xii) the act of acquiring shared data with limited access **with the knowledge that there has been an intervening act of wrongful acquisition of shared data with limited access**, or the act of using or disclosing shared data with limited access acquired in such a way;
(xiv) the act of using or disclosing shared data with limited access disclosed by an undertaking holding that data (hereinafter referred to as the "holder of shared data with limited access"), for the purpose of wrongful gain or causing damage to that holder of shared data with limited access (using the relevant data for that purpose is limited to an act conducted in breach of the duties regarding the management of that data);
(xv) the act of acquiring shared data with limited access **with the knowledge that the disclosure of that data is an act of improper disclosure of shared data with limited access** (meaning, in the case described in the preceding item, the act of disclosing shared data with limited access for the purpose as provided for in the same item; the same applies hereinafter) **or that there has been an intervening act of improper disclosure of shared data with limited access with regard to the relevant shared data with limited access**, or the act of using or disclosing shared data with limited access acquired in such a way;

Category of subsequent acquisition in good faith at the time of acquisition
Article 2 The term “Unfair Competition” as used in this Act means any of the following:
(xiii) the act of disclosing shared data with limited access after **having acquired it and learning that there had been an intervening act of wrongful acquisition of shared data with limited access**;
(xvi) the act of disclosing shared data with limited access after **having acquired that data and learning that the relevant acquisition falls under an act of improper disclosure of shared data with limited access or that there had been an**

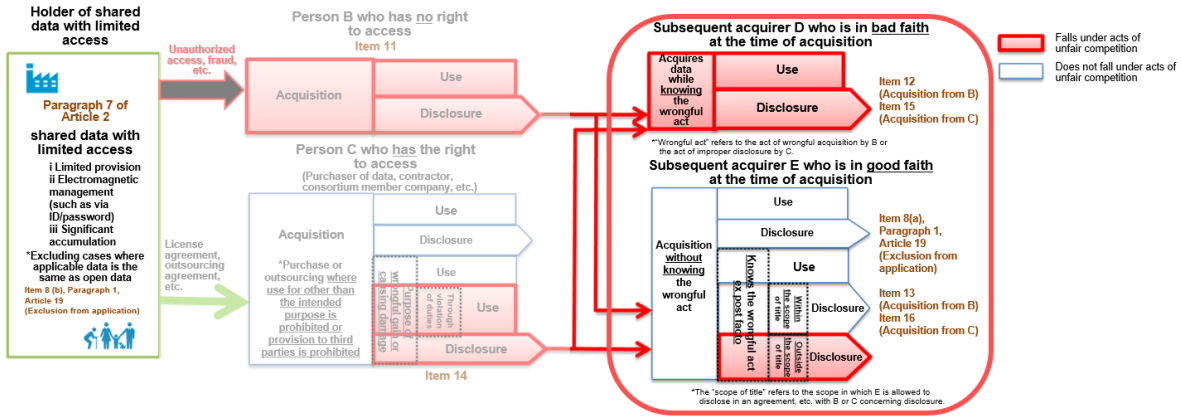
intervening act of improper disclosure of shared data with limited access;

Exclusion from application

Article 19 (1) The provisions of Articles 3 through 15, Article 21 (excluding the part under Article 21, paragraph (2), item (vii)), and Article 22 do not apply to the act prescribed in the relevant of the following items for the classification of unfair competition set forth in that item:

(viii) unfair competition set forth in Article 2, paragraph (1), items (xi) through (xvi) - any of the following acts:

*(a) the act by a person that has acquired shared data with limited access through a transaction (limited to a person that, at the time of acquiring the shared data with limited access, was without knowledge that the disclosure of that data was an act of improper disclosure of shared data with limited access or that there had been an intervening act of wrongful acquisition of shared data with limited access or an act of improper disclosure of shared data with limited access with regard to that data), of disclosing the shared data with limited access **within the scope of title acquired through the transaction**; or*



1. Category of subsequent acquisition in bad faith at the time of acquisition

(1) Overview

Shared data with limited access can, by nature, be easily duplicated and transferred. If distributed and re-distributed to third parties to whom such transfer is not expected, you will not be able to control the spread of the data. Rescue measures should therefore be established to prevent the spread of damage.

Particularly malicious is the act by a third party contractually unrelated to the data holder, of acquiring shared data with limited access and then using and disclosing it while aware that wrongful acquisition or unauthorized disclosure is involved (bad faith). Consequently, the act of acquiring shared data with limited access or using or disclosing the acquired shared data with limited access "with the knowledge that there has been an intervening act of wrongful acquisition of shared data with limited access (Act 2-1-12 of the Act) or "with the knowledge

that …(such action) is an act of improper disclosure of shared data with limited access … or that there has been an intervening act of improper disclosure of shared data with limited access (Act 2-1-15 of the Act) is characterized as "unfair competition."

Note that for "trade secrets," cases where "bad faith" is involved and cases where the actor did not know that there was wrongful acquisition or the like was involved, due to a serious mistake, are regarded as of "unfair competition" (gross negligence). For shared data with limited access, however, serious mistakes are not regarded as such. For shared data with limited access, therefore, the subsequent acquirer is not obligated to verify or investigate whether anything wrongful had previously occurred.

(2) The concept of "bad faith"

1) "Intervention"

(a) Article 2-1-12 of the Act (acquisition from someone without authorized access)

The act of "wrongful acquisition of shared data with limited access," which is an act of "bad faith," refers to wrongful acquisition defined in Article 2-1-11 of the Act.

In the phrase "there has been an intervening act of wrongful acquisition of shared data with limited access", "intervening" means that the wrongful acquisition had been performed at some time before you acquired the data. Consequently, unfair competition applies to the acquisition and the post-acquisition use and disclosure not only when you acquired the data directly from the wrongful acquirer but also when you acquired it indirectly if you are acting in bad faith at the time of your acquisition by knowing the fact that there was an intervening act of wrongful acquisition.

(b) Article 2-1-15 of the Act (acquisition from someone with authorized access)

"Improper disclosure of shared data with limited access", which is regarded as an instance of "bad faith," is the disclosure of shared data with limited access in order to obtain a wrongful gain and/or to cause damage to the holder of shared data with limited access (purpose of wrongful gain and/or causing damage) as set forth in Article 2-1-14 of the Act (it is not enough to identify instances of disclosure in violation of the relevant agreement; this point is different from the fact that for "trade secrets," "the improper disclosure of trade secrets," which is regarded as an instance of "bad faith," includes not only disclosure with an intention to obtain a wrongful gain and/or cause damage but also disclosure in violation of the relevant agreement, such as in violation of an obligation of confidentiality).

"Bad faith" is defined not only by the fact that there had been an intervening act of improper disclosure, but also the fact that it "is" an act of improper disclosure (Article 2-1-15 of the Act). This is because if you acquire shared data with limited access as the direct recipient of an act of disclosure as defined in Article 2-1-14 of the Act, the

action will constitute an act of improper disclosure.

2) "Bad faith"

Bad faith regarding a wrongful intervening act of acquisition of subsequently acquired data, an improper disclosure thereof for the purpose of wrongful gain or causing damage, or similar handling thereof refers to the awareness of the wrongful act. If it remains unclear whether such a wrongful act occurred, no bad faith is involved.

For charges of "bad faith" to be established, you must be aware, as described below, of both (a) the presence of a wrongful acquisition of shared data with limited access or of an act of improper disclosure of shared data with limited access, and (b) the fact that shared data with limited access wrongfully acquired or improperly disclosed is the same as data that has been or is to be subsequently acquired (the sameness of the data).

(a) An example of awareness of wrongful acquisition of shared data with limited access or improper disclosure of shared data with limited access

An example where in principle you are presumed to be aware of an intervening wrongful act

- If you asked a rightful acquirer of data whose provision to outside parties is prohibited to provide you with the data in return for material benefit while aware of the above fact
- If you have received from the data holder a written warning accompanied with clear grounds that there has been a wrongful act
- If you have learned that the data provider has admitted to having committed a wrongful act

An example where in principle you are not aware of an intervening wrongful act

- If you were provided at the time of data acquisition with grounds that the data provider had a legitimate right to provide the data
- If you received from the data holder a written warning asserting only that there has been a wrongful act, but if it is unclear whether this is true
- If you received from the data holder a written warning accompanied with reasonable grounds regarding the presence of wrongful acquisition, but if in a subsequent deliberation with the data provider the data provider presented some grounds presumably effective enough to overrule the above, so that you have concluded that there was no wrongful act

(b) An example of awareness of the fact that shared data with limited access

wrongfully acquired or the data improperly disclosed is the same as data that has been (or is about to be) subsequently acquired (the sameness of the data)

An example where in principle you are aware of the sameness of the data

- If a verification based on the traceability of digital watermarking presented by the data holder demonstrates that the data is the same
- If you received from the data holder a written warning accompanied with clear grounds that the data is the same
- If the subsequent acquirer has learned that the data provided by the data provider admits that there had been an intervening act of wrongful acquisition

An example where in principle there is no awareness of the sameness of the data

- If a verification based on the traceability of digital watermarking or the like presented to you by the data holder failed to prove the sameness of the data
- If the characteristics of the wrongfully acquired or otherwise handled data presented on a website are different from the characteristics such as the date and time the data was created of the subsequently acquired data
- If you have received from the data holder a written warning asserting only the sameness of the data, but if it is unclear whether it is true

In both (a) and (b) above, the reliability of the issuers of the written warning, various verification results, reports, and other documents seem to affect the determination as to the presence or absence of such awareness.

(3) The concept of "acquisition" (the relationship in timing between bad faith and acquisition)

"Acquisition" is as specified in III. 2., and refers to the act of obtaining control over data. This applies to the act by yourself or by a third party of acquiring data itself via a storage medium on which the data is recorded, of taking photos of a display showing the data, and additionally other actions taken by yourself or by a third party in order to acquire the data in a manner that does not involve movement of a storage medium on which the data is recorded or the like.

Specific examples

- Acquisition of data transferred over an Ethernet or wireless network

If you enter into an agreement with the data provider, the latter will send you the data and you (the subsequent acquirer) will receive it. In that manner, we assume that the following actions have been taken. In that case, in principle, “acquisition” applies to the action “3” below which therefore presumably have the potential to fall within the category of “subsequent acquisition in bad faith at the time of acquisition.”

1: You establish an agreement with the data provider.
2: You begin to operate in “bad faith.”
3: You receive transferred data.

- Acquiring data accessed through the data holder’s network

If you enter into an agreement with the data provider, they may provide you with an ID and a password for authentication with which to access the data server at any time. You, the subsequent acquirer, access the server yourself to obtain the data. In this manner of transaction, we assume that the following actions are taken. In that case, “acquisition” applies to the action “4” below which therefore presumably have the potential to fall within the category of “subsequent acquisition in bad faith at the time of acquisition.”

1: You enter into an agreement with the data provider.
2: You obtain an ID and a password.
(With the ID and password, you can access the server at any time.)
3: You begin to operate in “bad faith.”
4: With your ID and password, you access the provider’s server and download the data.

* If, however, you are in a position to have access to data on a cloud related to your own account, or otherwise in an environment where the data is virtually under your own control, you may be interpreted as having “acquired” the data even if you have not downloaded it onto your corporate server.
* Note that if a business operator who provides a service of acquiring data in a continuous manner and disclosing (providing) it to a third party continues to acquire data or disclose it without taking any measures after having acknowledged an intervening wrongful act, then the action of the operator will fall under unfair competition. The operator may therefore be obliged to stop providing such a service.

  Companies engaged in such business endeavors may take the following protective measures:

  1) If you have acknowledged an intervening wrongful act, then you entering a new agreement with a legitimate data holder can make it possible to keep acquiring and disclosing data.
  2) To protect the company from being held responsible for violating the existing agreement

concerning your provided service due to a forced suspension of service, the agreement documents for the provided service must contain and communicate the following in advance: if the company (the data provider) learns of a wrongful intervening act or other significant issue regarding the data to be provided with this service, the company reserves the right to stop supplying the said data.

2. Category of subsequent acquisition in good faith at the time of acquisition

(1) Overview

If unaware of an intervening or otherwise present wrongful act when acquiring shared data with limited access (in good faith), and afterwards become aware of the fact (effectively entering the status of bad faith), then the company (now aware of the fact) is obliged to take rescue measures to prevent the spread of damage to the data holder.

On the other hand, if the company was operating in good faith when acquiring the data, and then "entered into" bad faith, thereby being obliged to suddenly stop business activities due to an injunction or the like, business activities based on the data may be negatively affected, further inhibiting the distribution or use of the data.

In order to ensure a good balance in protection between the data holder and user, therefore, actions done by a subsequent acquirer who "entered into" bad faith after acquiring the data are limitedly characterized under "unfair competition" for acts of disclosure that may spread, thereby causing the holder to suffer considerable damage (Articles 2-1-13 and 2-1-16).

Note that for shared data with limited access, unlike "trade secrets," it is not regarded as falling under the category of "unfair competition" when you unaware of an intervening or otherwise present wrongful act due to gross negligence. For shared data with limited access, therefore, the subsequent acquirer is not obligated to verify or investigate whether wrongful conduct has occurred.

For the concepts of "bad faith" and "acquisition," refer to 1. (2) and 1. (3), respectively.

(2) Exclusion from application (Article 19-1-8a of the Act)

Even if the company discloses the data after "entering into" bad faith, the company (the subsequent acquirer), despite having acquired the data while unaware of an intervening wrongful act at the time of acquisition, will suffer unanticipated damage and business dealings will be at risk. In order to ensure the safety of operations after acquiring the data in good faith, therefore, having acquired shared data with limited access through a transaction, the company is exempted from the clause of unfair competition regarding an act of disclosure within the scope of title acquired under the agreement before "entering into bad faith" regarding an intervening or otherwise present wrongful act concerning shared data with limited access (Act 19-1-8a of the Act).

"Within the scope of title" refers to being within the range of conditions such as those concerning the period, objective, and manner of disclosure set forth in a transaction agreement (such as sales, purchase, and licensing) when acquiring the shared data with limited access. Note that even though the agreement expires on the surface, if the agreement is of a type where it is reasonable to expect that the contractual relationship would continue, then the continued agreement will be considered to be "within the scope of title."

Specific examples where you are in principle considered to be "within the scope of title"

- If, unless either party expresses its intention to terminate the agreement, the agreement is set to automatically renew with the same contractual provisions, and it is renewed with the provision stipulating the license to distribute the relevant data during the contract period, providing the data to a third party , after which either party "enters into bad faith"
- For agreements with unspecified durations where the data may be supplied to third parties as long as monthly fees are paid; if you supply the data that was acquired while still in good standing to a third party soon after leaving good standing (acting in bad faith) but maintain payment of the necessary fees