Contract Guidelines on Utilization of AI and Data

June 2018
Ministry of Economy, Trade and Industry
Contract Guidelines on Utilization of AI and Data:
Data Section

June 2018
Ministry of Economy, Trade and Industry
# Contract Guidelines on Utilization of AI and Data:
## Data Section

Table of Contents

<table>
<thead>
<tr>
<th>I</th>
<th>Introduction</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Purpose</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Importance and issues of data distribution and utilization</td>
<td>2</td>
</tr>
<tr>
<td>(1)</td>
<td>Promotion of data utilization</td>
<td>2</td>
</tr>
<tr>
<td>(2)</td>
<td>Concerns over damage caused by leaks and unauthorized use of data</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Increased complexity and sophistication of contracts and significance of these Guidelines</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Promotion of innovation</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>Significance of international cooperation</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>Government initiatives related to data contracts</td>
<td>4</td>
</tr>
<tr>
<td>II</td>
<td>Subjects, Structure and Application of these Guidelines</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>Expected readers</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>Contract types and overall structure of these Guidelines (Data Section)</td>
<td>5</td>
</tr>
<tr>
<td>(1)</td>
<td>Contract types</td>
<td>5</td>
</tr>
<tr>
<td>(2)</td>
<td>Overall structure of these Guidelines (Data Section)</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>Utilization of these Guidelines (Data Section) in negotiations</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>Relationship with AI Section</td>
<td>7</td>
</tr>
<tr>
<td>III</td>
<td>Basic Legal Knowledge Relevant Upon Examining Data Contracts</td>
<td>8</td>
</tr>
<tr>
<td>1</td>
<td>Legal nature and categories, etc. of data</td>
<td>8</td>
</tr>
<tr>
<td>(1)</td>
<td>Outline</td>
<td>8</td>
</tr>
<tr>
<td>(2)</td>
<td>Data ownership</td>
<td>9</td>
</tr>
<tr>
<td>(3)</td>
<td>Methods of categorizing data</td>
<td>10</td>
</tr>
<tr>
<td>(4)</td>
<td>Data use and competition policy</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>Various measures to prevent data leaks and unauthorized use</td>
<td>13</td>
</tr>
<tr>
<td>(1)</td>
<td>Protection by contract</td>
<td>13</td>
</tr>
<tr>
<td>(2)</td>
<td>Protection under the Unfair Competition Prevention Act</td>
<td>14</td>
</tr>
<tr>
<td>(3)</td>
<td>Protection by tort under Civil Code</td>
<td>16</td>
</tr>
<tr>
<td>(4)</td>
<td>Protection by Unauthorized Computer Access Prohibition Act</td>
<td>16</td>
</tr>
<tr>
<td>(5)</td>
<td>Technology for preventing unauthorized use, etc.</td>
<td>16</td>
</tr>
</tbody>
</table>
Appropriate allocation of consideration and profit ........................................... 17

Overview ........................................................................................................... 17

Forms of appropriate consideration and distribution of profit in data contracts ...... 17

IV “Data Provision Type” Contracts (Provision of Data from One Party to the Other Party) .......................................................... 19

1 Structure ............................................................................................................. 19

(1) Definition of data provision type contracts ................................................... 19

(2) Categories of data provision type contracts ................................................... 19

(3) Individuality of subject .................................................................................... 22

2 Main legal issues for data provision type contracts ......................................... 23

(1) Utilization rights to derived data, etc. utilizing provided data ...................... 23

(2) Liability against provided data which deviates from what was expected (quality of provided data) ................................................................. 25

(3) Damage arising out of utilization of provided data ........................................... 26

(4) Unintended utilization of provided data .......................................................... 26

(5) Issues for cross-border transactions ................................................................ 28

(6) Notes for data containing personal information, etc. .................................... 30

3 Causes and countermeasures regarding impediments to data distribution ........ 33

(1) Concerns and countermeasures regarding leaks of know-how caused by utilization of provided data ................................................................. 33

(2) Difficulty of calculating data value .................................................................. 34

4 Method of determining appropriate data provision type contracts .................. 34

V “Data Generation Type” Contracts (Handling of Data Generated With Participation of Multiple Parties) ................................................................. 38

1 Structure ............................................................................................................. 38

(1) Scope of subject of data generation type contracts ......................................... 38

(2) Issues regarding data generation type contracts ............................................. 40

2 Main legal issues relating to data generation type contracts ............................. 41

(1) Terms and conditions of utilization to be established between parties ............ 41

(2) Scope and granularity of applicable data ......................................................... 42

(3) Establishment of purpose of utilization ............................................................ 44

(4) Processing, etc. and utilization rights to derived data ..................................... 44

(5) Restriction of license, etc. to a third party ....................................................... 45

(6) Warranty/no warranty over contents and continuous generation of data .......... 47

(7) Distribution of profits ...................................................................................... 47
VI “Data Sharing Type (Platform Type)” Contracts (Data Sharing Using Platforms) (Handling of Data Generated With Participation of Multiple Parties) ................................................................. 55

1 Structure ........................................................................................................................................... 55
   (1) Introduction ................................................................................................................................... 55

2 Main issues to be considered for platform type ................................................................................. 61
   (1) Purpose and method of data application ....................................................................................... 62
   (2) Number of data providers and scope of participants ................................................................. 63
   (3) Adjustment of interests between data providers and data users ............................................... 64
   (4) Type and scope of applicable provided data ............................................................................... 64
   (5) Scope of data utilization .............................................................................................................. 66
   (6) Selection of platform operator ................................................................................................... 67
   (7) Necessity of terms of use ........................................................................................................... 67
   (8) Structure for promoting application of platforms ....................................................................... 67
   (9) Perspective of competition among platforms and internationalization .................................... 68

3 Main legal issues relating to platform type ......................................................................................... 69
   (1) Necessity and type of terms of use ............................................................................................. 69
   (2) Significance of specifying scope of data utilization in terms of use ......................................... 70
   (3) Type, etc. of data and services handled on platforms ............................................................ 71
   (4) Scope of participants ............................................................................................................... 77
   (5) Which entity should be platform operator .............................................................................. 78

4 Main items of terms of use ............................................................................................................... 79
   (1) Scope of license (scope of utilization) of provided data or utilized data or utilized services .... 79
(2) Responsibilities of data provider in respect of provided data (warranty/no warranty) 80
(3) Rights related to derived data and other derivative products .................................. 82
(4) Audits and complaint and dispute settlement.......................................................... 83
(5) Obligations and liabilities of platform operators (limitation of liability).................... 83
(6) Obligations and liabilities of data provider and data user (limitation of liability)..... 86
(7) Sanctions upon violation of terms of use ................................................................. 87
(8) Handling of provided data and derivative products upon withdrawal and termination 87

VII Examples of Major Contractual Provisions .............................................................. 89
1 Draft model contract for data provision type contracts ............................................. 89
2 Draft model contract for data generation type contracts ........................................... 107
I Introduction

These Guidelines (Data Section) explain matters that should be included in data contracts from the viewpoint of promoting reasonable negotiations and execution of contracts, reducing transaction costs and diffusing data contracts, etc. in light of the fact that so-called data contracts (contracts relating to the utilization, processing, transfer and other handling of data) tend to be incomplete contracts (contracts that fail to cover any events that may occur after the execution thereof). The basic ideas are as follows.

I Purpose

Data contracts have not been broadly executed in general and contractual practices have not been accumulated enough yet. Therefore, data contracts are likely to cause various problems when they are executed in the future. These Guidelines (Data Section) aim to, with respect to data contracts which have such characteristics as above and for which there is no standard form established, reduce transaction costs and diffuse data contracts in order to consequently promote the effective use of data by presenting major issues and questions for each type of contract and by providing examples of contractual terms that are easily accessible to the public and factors to be considered when preparing such terms.

The Ministry of Economy, Trade and Industry and other authorities have already published two guidelines related to data contracts. First, the “Contract Guidelines for Promotion of Data Transaction”1 published in October 2015 presented the conditions, points and other matters relating to the provision of data by right holders of the data, on the assumption that the right holders can be clearly identified from among the parties. Second, the “Contract Guidelines on Data Utilization Rights ver. 1.0”2 published in May 2017 presented how the consultations to decide the holders of utilization rights should proceed and the way of deciding the utilization rights by contracts.

Nevertheless, the two guidelines above were not prepared for the purpose of comprehensively presenting the types and terms of all data contracts in the first place, and, as it is apparent from the rapid progress of AI and IoT technologies in recent years, the environment surrounding data contracts has evolved dramatically on a daily basis against the background of technological innovation that enables collection, processing and analysis of enormous amounts of data. Therefore, the practice of data contracts and guidelines for disciplining such practice are also required to respond to those drastic changes in the environment. The typical examples of the issues are: issues related to so-called data ownership, issues of how we should consider the handling of derived data3 in the case when a contracting party creates (processes or integrates) new data and issues of how we should cope with the situation where the cases in which data is shared and made use of by utilizing platforms that go beyond the existing boundaries of companies and affiliates (“data sharing type (platform type)” as described in VI below) are increasing as a new type of contract. In addition, users of the previous guidelines have not only raised questions about the present situation where data distribution is taken as a given but also made requests for more clear explanation on how they should apply to specific cases (use

---

2 http://www.meti.go.jp/press/2017/05/20170530003/20170530003-1.pdf
3 In these Guidelines (Data Section), the term “derived data” refers to data that is newly generated through processing, analysis, editing, integration, etc. of any data.
I Introduction

cases, etc.) and on points of concern in the handling of personal information and cross-border transactions (transactions conducted across national borders).

Therefore, taking such circumstances into consideration, these Guidelines (Data Section), covering the contracts which stipulate the distribution and utilization of data and the value of which is often uncertain at the stage of execution, examine the positions of each party to data contracts based on the discussions of professionals on concrete cases, list matters that should be generally included in contracts after organizing them by contract types, and provide the examples of contractual terms and factors to be considered when preparing such terms.

2 Importance and issues of data distribution and utilization

Recently, the amount of data related to transactions has explosively increased in connection with the promotion of IT adoption in transactions, etc. In some cases, data creates added value when combined with other data, and combination of multiple data across industries is especially expected to lead to open innovation. In order to enhance the added value of data and strengthen competitiveness, it is important to expand the subjects and types of data to be utilized and to utilize them in various combinations.

(1) Promotion of data utilization

Data is not of much value when it is merely being possessed. In many cases, data itself is not valuable, and value is created only after processing and analyzing data and developing methods for utilizing the data for business activities. Therefore, it would be desirable, when conducting negotiations for contracts, to have the idea of empowering the parties who have the method (ability) to utilize the data, encouraging such parties to utilize the data, and distributing profits gained from such utilization of data among the parties.

Certain types of data create sufficient value only when collected in a certain amount. For example, real-time driving data of vehicles can be used for congestion analysis or the like when the data of a large number of vehicles are collected and create value that cannot be created just by analyzing the data of each vehicle. Similarly, in the case of data collecting the operation status of machine tools, etc., it becomes possible to perform statistically meaningful analysis on the operation of tools only by accumulating data of a large number of tools. In such cases, it is generally desirable that the party who can collect and utilize such large volume of data be authorized to utilize the data.

In connection with such allocation of the utilization rights, it is also important that the resulting interests would be distributed among the parties in an appropriate manner. In order to collect and process and analyze data and develop utilization methods, etc., it is required to make investments in hardware, such as sensors and servers, as well as to make human investments in data analysts and the like. It is desirable to procure that the parties have incentives for such investments and to grant the parties making such investments with appropriate profits (returns).

(2) Concerns over damage caused by leaks and unauthorized use of data

On the other hand, there are certain risks in the distribution and utilization of data. For example, trade secrets and know-how may be leaked out of the company, or privacy rights may be infringed due to leaks or unauthorized utilization of data. In general terms, data can be
I Introduction

easily duplicated and, if there is no appropriate management system, may be leaked to the outside through unauthorized access. Therefore, when data contains a company’s trade secret, know-how or the like, the company providing the data may be anxious that the trade secret and know-how might be leaked out of the company through the provision of the data. Moreover, if any personal information is included in the data, not only may the industry competitiveness of the parties be diminished, but personal rights, such as privacy rights, may also be infringed.

In considering the data distribution and utilization in individual cases, it is essential to pay careful attention to the concerns about such risks. In doing so, as it might be possible to minimize the risks by taking appropriate contractual and technical measures, it is advisable for the parties to understand such various measures in order to be able to correctly evaluate the risks and benefits and execute reasonable data contracts. The methods for preventing any leaks and unauthorized utilization of trade secrets and know-how, etc. are described in III below.

3 Increased complexity and sophistication of contracts and significance of these Guidelines

With respect to data contracts, which are a new type of contract and for which the matters to be decided are becoming increasingly complex and sophisticated, if the parties to the contracts can build reasonable business relationships for the data distribution and utilization at low cost, it is expected that not only the competitiveness of the parties but also, as a result, national competitiveness would increase in combination with the application of laws including the Antimonopoly Act and the Unfair Competition Prevention Act.

On the other hand, in light of the principle of freedom of contract, matters such as selection of counterparty, determination of contents, and method of contracting are left to the intention of the parties concerned. Therefore, these Guidelines (Data Section) only indicate the matters to be set forth in contracts and do not, as a matter of course, restrict any freedom of contract.

Specifically, for the purpose of generally diffusing data contracts among various transactions, these Guidelines introduce matters to be included in contracts executed between business operators for the distribution, utilization, sharing, etc. of data.

In order to increase the sophistication of contracts, it is necessary to go back to the principle that the utilization rights can be freely stipulated by contract. Since data is intangible by nature and is not subject of ownership and the utilization rights can be freely determined between the parties by contracts, it is desirable that the parties flexibly determine the conditions of utilization upon consultation and set forth specific details of the utilization rights and other matters, in reference to these Guidelines (Data Section) and taking into consideration the degree of contribution to the creation and utilization of data and other factors, to increase the sophistication of the contracts according to the actual situation of the transaction.

4 Promotion of innovation

These Guidelines (Data Section) aim to support parties who wish to distribute and utilize data and to enable the utilization of new, undiscovered value by not only promoting traditional innovations in which data is utilized through the efforts of individual companies without opening the data but also by further expanding the possibilities of open innovation.
I Introduction

It is also one of the purposes of these Guidelines (Data Section) to encourage the utilization of data and promote open innovation by providing the concept of data contracts and contract terms, etc. with consideration given to various positions.

5 Significance of international cooperation

As cross-border transactions are becoming more common in recent years, it is desirable to examine contracts related to data distribution and utilization that are available at a global level. In addition, cross-border transactions may cause an issue of cross-border data flows.

In a recent move, the Linux Foundation published the Community Data License Agreement (CDLA) on October 23, 2017. The CDLA, which provides for the conditions of licenses for open data, can be considered to be a data version of an open-source software license such as the GNU General Public License. While it is necessary to examine the handling of data based on the standpoints of both promoting the utilization of data and preventing leaks and unauthorized utilization of data as described above, it is considered that the CDLA supports the promotion of utilization of open data. These Guidelines (Data Section) mainly assume commercial transactions and do not presuppose that the data is open data, but it is necessary to take such international trends into consideration when examining appropriate contractual practices.

These Guidelines (Data Section) have been compiled in light of those perspectives as well.

6 Government initiatives related to data contracts

Government initiatives related to data contracts include the following.

(Omitted in the translation)

---

4 https://cdla.io/
II Subjects, Structure and Application of these Guidelines

This section defines expected readers of these Guidelines and describes the three main types of contracts related to data distribution and utilization, which are data provision type, data generation type and data sharing type (platform type) and explains the process of negotiation and negotiating power.

1 Expected readers

The readers of these Guidelines (Data Section) are to be a wide range of people (including contracting business operators, associated business and management units, and parties developing systems for data distribution and utilization).

This is because, considering the potential impacts that data contracts might have on management as a whole and also on the development of systems which enable data distribution and utilization, it is desirable to assume a wide range of readers that include not only the persons involved in the execution of the contracts but also all persons related to the contracts so that they can understand the issue awareness presented in these Guidelines (Data Section).

2 Contract types and overall structure of these Guidelines (Data Section)

(1) Contract types

In these Guidelines (Data Section), data contracts are organized in terms of (i) whether or not the factual state that one party retains existing data is clear, (ii) whether or not data that had not existed before is newly generated with the participation of multiple parties, and (iii) whether or not data is shared using platforms, and the contracts are accordingly categorized into three contract types—(i) data provision type, (ii) data generation type, and (iii) data sharing type (platform type).

The first contract type, data provision type (provision of data from one party to the other party), applies to any contract which, on the premise that there is no dispute between parties with respect to the factual state that only one party (data provider) retains data which is the subject of the transaction, is executed when a data provider provides data to the other party to determine the utilization rights of the other party and any other conditions of the data provision with respect to such data.

The second contract type, data generation type (handling of data generated with the participation of multiple parties) applies to any contract which, on the premise that data that had not existed before is newly generated with the participation of multiple parties, is executed between the parties involved in the creation of the data to determine the utilization rights.

The third contract type, data sharing type (data sharing using a platform), applies to any contract which is executed when multiple business operators provide data to a platform, which aggregates, stores, processes or analyzes the data, to share such data through the platform.

5 The term “retain” is used for convenience as a term indicating the factual state in which data is lawfully accessible to the party.

6 See 4-1-(1) for the meaning of the utilization rights.
II Subjects, Structure and Application of these Guidelines

(2) Overall structure of these Guidelines (Data Section)

The overall structure of these Guidelines (Data Section) is as follows.

First, Part III explains the legal nature of data, various measures to prevent data leaks and unauthorized use and distribution of appropriate considerations and interests from a general point of view, as basic legal knowledge that forms the basis for examining data contracts.

Next, Parts IV to VI sequentially explain matters such as the structure, main legal issues and appropriate method of contractual arrangement for each contract type mentioned above, namely, **data provision type**, **data generation type** and **data sharing type (platform type)**. In addition, Part VII presents examples of principal contractual terms for the **data provision type** and **data generation type**.7

3 Utilization of these Guidelines (Data Section) in negotiations

This section focuses on the procedure aspect of data contracts and explains about the utilization of these Guidelines (Data Section) in the process of consultation between the parties prior to the execution of the contracts.

Since there are no legal provisions governing the negotiation of data contracts, each contract party may conduct negotiation in a free manner.

However, there are certain matters to be noted.

First, there is the case where a party is in a transaction dependency relationship, etc. (dominant bargaining position)8 with the counterparty and is forced to accept any request from the counterparty. In such case, if a party offers the execution of a contract and ends up being unjustly forced to incur disadvantages, such as when the counterparty refuses to have any consultations on the contractual arrangements, including utilization rights, and demands that the party bear an excessive burden as a condition of the arrangements, an issue under competition law may arise separately.

In addition, when a large company with personnel that are familiar with contractual practices, etc. makes such arrangements with a small to medium-sized enterprise, including a venture company, it is desirable that the parties strive to negotiate on equal terms as much as possible based on their full understanding. In particular, when a party stands in a superior bargaining position over the counterparty, it should be noted that a problem under competition law may

---

7 With respect to the **data sharing type (platform type)**, no examples of contractual terms are presented in Part IV-4 as the details of the contractual terms to be determined may vary greatly depending on the individual circumstances such as the purpose of platforms and scope of parties concerned, but the primary considerations are shown in Part IV-4.

8 According to the “Guidelines Concerning Abuse of a Superior Bargaining Position under the Antimonopoly Act” of the Japan Fair Trade Commission, when a business partner has a superior bargaining position over the party, it produces a situation in which, if the business partner makes a request, etc., even if it is substantially disadvantageous to the party, the party has no choice but to meet that request, because any difficulty the party has in continuing the transaction with the business partner would substantially impede the party's business management, and in determining the presence or absence of a superior bargaining position, the degree of the party's dependence on transactions with the business partner, the business partner's position in the market, the possibility of the party changing business partners, and other concrete facts indicating the need for the party to carry out transactions with the business partner are comprehensively considered.
II Subjects, Structure and Application of these Guidelines

arise in a similar way if the party forces unjust arrangements against the background of the power balance in the transaction and the other party has no choice but to unjustly accept disadvantages.

Next, unlike the issue of attribution of intellectual property rights, the practice of data contracts have not been necessarily established, and there are many areas yet to explore. The parties are required to begin with comprehending the data related to the transaction as much as possible, and if the parties execute a contract without comprehending the data, it is possible that only one of them would enjoy benefits by the data distribution and utilization.

As described above, with respect to data contracts, it is possible that parties do not have sufficient knowledge about the existence, type, value and other matters concerning the data related to the transaction and, against the background of such lack of knowledge, contracts might be unilaterally executed under unfavorable conditions. These Guidelines (Data Section) are also expected to be used to supplement such knowledge disparities associated with data contracts.

4 Relationship with AI Section

Since the use of data may include development and use of software using AI technology, these Guidelines (Data Section) may also be referred to in conjunction with certain parts of the AI Section. In concrete terms, the discussions on the general handling of derivative data, etc. in these Guidelines (Data Section) would be of reference as a proposition for the course of acquiring and processing data in the early stage of development of software using AI technology and for the handling of trained parameters included in training data set and trained models used for software training using AI technology.

On the other hand, please see Guidelines (AI Section) for other discussions with respect to contracts for development of trained models or contracts for utilization of AI technology.
As basic legal knowledge relevant when examining these Guidelines (Data Section), the following is an explanation regarding the legal characteristics of data, various methods for preventing data leaks or unauthorized use, and appropriate distribution of consideration and profit.

1 Legal nature and categories, etc. of data

(1) Outline

Data is intangible, and because it is not the subject of rights under the Civil Code such as ownership or possession, usufruct, or security interest, it is not possible to prescribe the existence or absence of rights pertaining to data based on concepts of ownership or possession (see Article 206 and Article 85 of the Civil Code). And since, as described below in Part III-2-(2), the cases where data is subject to legal protection (whether as intellectual property, or as a trade secret under the Unfair Trade Practices Act) are limited, the protection of data is generally sought to be achieved through contracts between the interested parties.

Although copyrights, patent rights, and trade secrets exist as intellectual property rights, etc. relating to data protection, due to the following reasons it is not necessarily the case that these adequately function to protect data.

The works that are subject to protection by copyright are prescribed as productions that express thoughts or sentiments in a creative way (Article 2(1)(i) of the Copyright Act), and it is considered that in many cases it would be difficult for it to be found that there is a creative element in collections of data such as the data that is mechanically generated by devices such as sensors and cameras or the usage logs of smartphones, etc. Further, although it is prescribed that databases which, by reason of the selection or systematic construction of information contained therein, constitute intellectual creations are to be protected as independent works of the database (Article 12-2(1) of the Copyright Act), it is considered that there would not necessarily be many cases in which it could be found that data is a copyrightable work of the database by virtue of having processed the data (such as cleansing or analysis).

Also, the inventions that are subject to protection by patent are highly advanced creations of technical ideas utilizing the laws of nature, and it is considered that the cases in which data would be subject to protection by patent are limited.9

On the other hand, data may be subject to legal protection as a trade secret under the Unfair Trade Practices Act if it embodies know-how of an entity involved in the creation of data or in the distribution or utilization of data (such as know-how related to production methods in the manufacturing industry, know-how of sensor manufacturers regarding data cleansing, or know-how about utilizing data from service development providers in services) and it satisfies the following three elements: (i) is managed as a secret, (ii) has utility, and (iii) is not in the public domain. Yet it is not the case that data will necessarily be protected as a trade secret if the data is planned to be distributed to a certain extent through a transaction (for the protection of data planned to be distributed to a certain extent, see Part III-2-(2) below (amendments to the Unfair Competition Prevention Act relating to limited provided data”)).

---

9 For example, data is patentable if it comprises a “program, etc.” as prescribed in Article 2(4) of the Patent Act and satisfies the other criteria for granting of patents.
## III  Basic Legal Knowledge Relevant Upon Examining Data Contracts

The following table organizes the outlines of intellectual property rights, etc. relating to protection of data.

<table>
<thead>
<tr>
<th>Type of right</th>
<th>Nature of right</th>
<th>Whether able to be used for data protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copyright</td>
<td>The work must be a production in which thoughts or sentiments are creatively expressed and which falls within the literary, academic, artistic or musical domain (Article 2(1)(i) of the Copyright Act).</td>
<td>The cases in which mechanically generated data can be found to have a creative element are limited.</td>
</tr>
<tr>
<td>Patent</td>
<td>A patent right for a highly advanced creation of technical ideas using the laws of nature that is industrially applicable will become effective upon registration of its establishment. Patent examination is not available for inventions that are not found to have novelty or an inventive step (Article 2(1), Article 29(1), and Article 66(1) of the Patent Act).</td>
<td>Regardless of the method of processing or analyzing data, the cases in which the data itself can be found to highly advanced creations of technical ideas utilizing the laws of nature are limited.</td>
</tr>
<tr>
<td>Trade secret</td>
<td>Information is a trade secret if it meets the criteria of (i) being managed as a secret, (ii) having utility, and (iii) is not in the public domain, and in the case of a statutorily proscribed act such as acquiring a trade secret by unfair means (unfair competition), it is possible to seek an injunction, damages, or criminal penalty (Article 2(6), Article 2(1)(iv) through (x), Article 3, Article 4, Article 21, and Article 22).</td>
<td>Data can enjoy legal protection if the elements in (a) through (c) are satisfied.</td>
</tr>
</tbody>
</table>

### (2) Data ownership

In discussions concerning data contracts the term “data ownership” is sometimes used. There is currently no legal definition for this term and it is not the case that it is necessarily used with an implied meaning that “data is able to be conceived as being subject to ownership.” On the contrary, aside from the cases where data is subject to direct protection by intellectual property rights, etc., it is considered that the term “data ownership” is generally used to refer to the de facto position of being able to access and control data, or a contractual status in cases where an undertaking has been entered into by contract regarding the authority to use data.
III Basic Legal Knowledge Relevant Upon Examining Data Contracts

As described in (1) above, since data is not subject to rights of ownership, possession, usufruct, or security interests, it is not possible under the current laws of Japan to conceive of data as being subject to ownership or other property rights (except for the case where copyright or other such intellectual property rights arise). Although in contract practice there are cases where it is said that “data ownership” is attributed to one of the parties to the contract, it is difficult to consider that such contract party has a property right such as ownership over the data, and it is considered that this expression refers to the fact that such party is in a position of having the contractual status of being able to assert against the other party that it has the authority to use the data.

Understanding data ownership in the manner described above, we can attempt to specifically apply such approach to, for example, the situation of entering into a Data Creation type contract as described in Part V below. If in such situation the contribution of one party to the creation of the data is significantly large and the data is also closely related to the business of such party, then it could be said that there are cases where it could be found to be reasonable to prescribe in the contract that such party is in a position of having the contractual status of being able to assert against the other party that it has the authority to use the data. However, since the method of evaluating the degree to which the party has contributed to the creation of the data or the method of evaluating the relevance of the data to the business of the party may differ significantly depending on factors such as the industry area or the type of data, it is difficult at present to single out a uniform standard for which party should be said to be in the position of having a contractual status relating to the data (i.e., of having data ownership). As discussed in Part V below, factors such as the degree of a party’s contribution to data creation and whether the party has equipment ownership should be assessed as elements for determining who has the right to use the data, and it would be desirable to attempt to coordinate each individual right to use data by evaluating each determinative element from the perspective of promoting data usage and the necessity for maintaining the secrecy of data.

(3) Methods of categorizing data

When entering into a data contract, it is necessary to pay attention to the category of data being handled. The following is an explanation of some of the categories that are considered particularly important based on present cases: (a) structured data and unstructured data, and (b) person related data (which includes personal information) and non-person related data.

(a) Structured data and unstructured data

Both structured data and unstructured data are categories within big data. Big data is generally defined as “location information and behavior history from smartphones etc., information relating to viewing and consumption behavior of media such as the Internet and television, and the massive volume of data able to be obtained from miniaturized sensors and the like, due to the increased progress of digitization, greater sophistication of networks, and the advancement of IoT through miniaturization and increased affordability of IoT-related devices such as smartphones and sensors,” and structured data means big data that is structured to conform

---

to relational databases, etc.—for example, customer data or sales data. Unstructured data, on the other hand, includes an even broader scope of data. For example, in addition to the types of data that have traditionally been generated and circulated (such as voice data from telephones and radio broadcasts, etc., video data from television broadcasts, etc., and print data from newspapers and magazines, etc.), unstructured data includes types of data whose generation and circulation has been rapidly growing in recent times, such as text data contained in social media such as blogs and social networking services, video data circulated through video distribution services on the Internet, print data distributed as e-books, data sent from GPS devices, and data detected and sent from various sensors such as IC cards and RFIDs.

(i) Person related data / non-person related data

Although the phrase “person related data” is not defined under existing law, it is described as including “information about individuals such as attribute information, movement/behavior/purchase history, and personal information collected from wearable devices,” and including “human flow information and product information, etc. that has been processed so as to make individuals unidentifiable.” For this reason, person related data may include “not only personal information but also a broad range of information from which relationality with individuals is able to found, including information where the boundary with personal information is vague.”

In this way, person related data may also include personal information, and in such cases it is necessary to handle it appropriately in accordance with laws and regulations.

There is also a possibility for widespread adoption of the “anonymously processed information” system that was introduced in the Amended Personal Information Protection Act (which entered into force in May 2017) from the perspective of promoting the utilization of data. Anonymously processed information is defined in Article 2(9) of the Personal Information Protection Act, and means information produced from processing personal information so as neither to be able to identify a specific individual nor to be able to restore the personal information. Since anonymously processed information is information that pertains to individuals it does constitute “person related data,” but it is not “personal information” as defined under the Personal Information Protection Act, and thus it enables the promotion of free circulation and application of the information under regulations that are less stringent than those regarding the handling of personal information.

(4) Data use and competition policy

---

11 A type of database structure in which the database is designed and developed based on relational models. It is possible to use SQL and other database languages to integrate, extract, and otherwise handle the data.

12 Ministry of Internal Affairs and Communication, ibid note 29, pp. 29 and 53-54.

13 See Part IV-2-(6)-(iii) below regarding the details of anonymously processed information. Also, in preparing anonymously processed information, please see the Personal Information Protection Committee “Guideline regarding the Act on Protection of Personal Information (Anonymously Processed Information Section),” https://www.ppc.go.jp/files/pdf/guidelines04.pdf (November 2016 (partially revised in March 2017)).
III  Basic Legal Knowledge Relevant Upon Examining Data Contracts

It is currently considered that the collection and use of data itself is an activity that promotes competition, and is thus a desirable activity from the perspective of competition policy and that it is not treated as problematic in principle under the Antimonopoly Act either. Because the collection, accumulation, and use of data has the effect of invigorating competition through originality and ingenuity between business operators and creating innovation, it is considered that competition should be further promoted in respect of the processes of collecting, accumulating, and using data, and that it is desirable to remove obstacles to competition.

Yet it is not the case that there are no concerns at all. Generally speaking, it is considered that there are cases where it would become necessary to maintain and restore competition through regulation under the Antimonopoly Act, such as: the case where data comes to be accumulated at one specific business operator due to improper activity like seeking to remove competition or due to corporate integrations such as mergers, while at the same time becoming difficult to obtain by other business operators, which results in restrictions on competition in the market for the goods and services that hold an important place in terms of efficiencies, etc. for such data (hereinafter simply “Goods”); or the cases where data is utilized using means that are improper from the perspective of competition, as a result of which (for example) competition comes to be restricted in markets related to data, such as the market for Goods.

In regard to the collection of data, issues may arise under the Antimonopoly Act in cases where there is a negative effect on competition, such as where data is collected by improper means,14 or where the data collector promotes coordinated activity between competitors. Also, in regard to joint collection of data, jointly collected data makes it possible for participants in a competitive relationship to mutually ascertain the content, price, and quantity of Goods that will be sold in the future, and if this results in promotion of coordinated activity between competitors, it may become an issue under Article 3 of the Antimonopoly Act (unjust restrictions on trade).15 Further, in the Goods market, where data is used as important input goods, it is considered that it may become an issue under the Antimonopoly Act if a large portion of business operators in a competitive relationship engage in joint collection of data despite the fact that it would be possible for each participant to engage in data collection on its own, and the data collection of each participant is restricted and thereby competition in the market for such Goods is effectively restricted.

In regard to the accumulation and utilization of data, it may become problematic under the Antimonopoly Act—as constituting trading on restrictive terms or trading on exclusive terms—in the case where there is found to be obstructiveness to fair competition in the activities of a provider: for example, where it sells data together with other services for the analysis, etc. of such data (“tie-in sales”) or imposes an obligation on the counterparty to trade data with the provider only, or where it makes it possible to use data unjustly by restricting the collection or use of data by persons other than such provider (including by the owner of the devices to which industrial data pertains) on condition that the underlying technology such as AI technology will be provided (whether for a charge or free of charge).

It is also necessary to bear in mind that when a business operator is located within Japan or, despite living outside Japan, has an influence on the Japanese market, it may be subject to the application of the Antimonopoly Act in cases such as where it is engaged in activity that relates to collection or use of large quantities of data.

14 See Part V-2-(14) below regarding in the case of data generation.
15 For a discussion on data sharing type contracts, see Part VI-3-(4) below.
2 Various measures to prevent data leaks and unauthorized use

There are many stakeholders who are concerned that if provided data contains trade secrets or know-how, etc. of the provider, the providing of such data and consequent loss of control over it may result in leaks of such trade secrets and know-how to outside parties or unauthorized use thereof. Due to such concerns, there are also business operators who have second thoughts about providing data. For this reason, in (1) through (5) below we list various measures for preventing data leaks and unauthorized access: protection by contract, protection under the Unfair Competition Prevention Act, protection in tort under the Civil Code, protection under the Unauthorized Access Prevention Act, and technology to prevent unauthorized access, etc. Gaining an understanding of these various means of protection may enable the circulation and use of data while protecting against data leaks and unauthorized access by taking necessary measures as appropriate.

In making such explanations, we will first explain about protection by contract because the general principle, as stated above, is that protection of data is achieved through contracts between the interested parties, and then we will explain about protection under laws and the like.

(1) Protection by contract

First, in order to prevent outflow of trade secrets and know-how contained in provided data, it is important to impose confidentiality obligations on the data recipient. As a method of imposing stringent confidentiality obligations in order to protect trade secrets and know-how contained in provided data, one example is to limit the scope of officers and employees of the data recipient who will be able to access the provided data, and to make the data recipient contractually obliged to cause such officers and employees to submit written pledges relating to confidentiality.

Or, for example, another effective method is to include specific provisions in the contract regarding the storage and management methods for provided data, such as imposing an obligation to store the data on a high security server or to store it separately from other data. Further, there is also the method of including a provision to the effect that the data provider may request the data recipient to provide reports or allow onsite inspections, and that, if as a result of such report or onsite inspection there are found to be any issues with the status of management of the provided data by the data recipient, the data provider may take action such as demanding that the data recipient remedies such issues.

Also, in view of the fact that it is difficult to calculate the amount of damage incurred by data providers as a consequence of outflows of trade secrets or know-how, another method is to prescribe liquidated damages for the case where trade secrets or know-how are leaked from the data recipient. However, because prescribing liquidated damages may sometimes have the reverse effect of weakening the binding force of the contract if the amount of damages is too small (i.e., if the advantages to the data recipient in leaking the trade secrets or know-how are greater than the cost of breaching the contract and paying the liquidated damages, the liquidated damages clause will have diminished meaning as a means of preventing leaks of trade secrets and know-how), it is considered necessary to set an appropriate amount that takes such point into consideration.
III Basic Legal Knowledge Relevant Upon Examining Data Contracts

(2) Protection under the Unfair Competition Prevention Act

In order to enjoy legal protection as a “trade secret” under Article 2(6) of the Unfair Competition Prevention Act, the information must satisfy the three elements of (i) being managed as a secret, (ii) having utility, and (iii) not being in the public domain, and if provided data satisfies these three elements it will be able to enjoy protection under the Unfair Competition Prevention Act as a “trade secret.”

However, because there has been continued innovation in information technology such as IoT and AI, and the source of companies’ competitive advantage is starting to become data and its utilization, it is necessary to have in place a business environment that enables the safe and reliable utilization of data, so we examined the legal system from that perspective.

Recently, based on such background, the Act to Partially Amend the Unfair Prevention Act, Etc. was enacted in May 2018, which introduced remedial measures in civil law such as injunctions against the unauthorized acquisition or use, etc. of data that is provided in a protected form such as by ID or password, on the basis that such activity constitutes “unfair competition.” We refer to the amended Unfair Competition Act hereinafter as the “Amended Unfair Competition Act.”

Diagram 1: Outline of Amended Unfair Competition Act

The data that is subject to protection under the Amended Unfair Competition Act is “limited provided data,” which means “technical or business information accumulated or managed in significant volume by electromagnetic means as information provided to certain persons as a business (other than information managed as a secret)” (Article 2(7) of the Amended Unfair Competition Act).

“Limited provided data” was so defined after the Subcommittee on Unfair Competition
Elements of data that is the subject of protection

The Subcommittee stated that data that meets the following elements should be subject to protection.

(i) Managed with technology
The data must be managed by appropriate electromagnetic access control means (such as ID and password, dedicated network, data encryption, or scrambling) for provision to only a certain limited scope of persons and by which it is possible to clearly recognize a management intention to the effect that it is not permitted for third parties other than those persons contemplated in the contract with the data provider to use or be provided with the data.

(ii) Limited provision to outside parties
Unlike “trade secrets,” which are managed as a secret and are used inhouse by the owner or, as an exception, disclosed to limited persons who have executed a confidentiality agreement, the data must be of a kind that is intended to be optionally provided to certain outside parties in response to their requests.

(iii) Utility
The data must be recognized as having commercial value, by stripping the data objects of any illegal or immoral content and combining them together.

Unfair competition activities regarding data

The Subcommittee identified the following activities as “unfair competition activities” and stated that remedial measures should be introduced for these.

(i) “Unauthorized acquisition” type
- Where an unauthorized outside party acquires data by a management breach or, having so acquired such data, uses the data or provides it to a third party (Article 2(1)(xi) of the Unfair Competition Prevention Act)

  Note: “Management breach” means an act that is harmful to the data provider’s management of the data (such as unauthorized access or trespassing on a building), or an act equivalent to fraud, etc. in causing the data provider to provide the data after removing technical management measures (meaning acts of fraud, violence, or threat).

(ii) “Extreme bad faith” type
- Where data acquired from a data provider subject to the condition that provision to third parties is prohibited is used in a form of activity that is regarded as equivalent to embezzlement or defalcation (a form of activity that betrays an advanced relationship of trust between parties to a service agreement, etc.) with the purpose of obtaining unjust
Basic Legal Knowledge Relevant Upon Examining Data Contracts

profit or causing damage to the data provider (a “profit or harm motive”), or where such data is provided to a third party for a profit or harm motive (Article 2(1)(xiv) of the Amended Unfair Competition Prevention Act)

(iii) “Subsequent acquisition” type

- Where a person acquiring data knows that an improper act took place in relation to such data and proceeds to acquire the data to which such improper act pertains, or uses the data so acquired or provides it to a third party (Article 2(1)(xii) and (xv) of the Amended Unfair Competition Prevention Act)

- Where a person acquiring data did not know, at the time of such acquisition, that an improper act took place in relation to such data, and, after subsequently becoming aware of such improper act (i.e. thereby being in bad faith), provides such data to a third party (Article 2(1)(xiii) and (xvi))

Note: Excludes the case where the data is provided within an authorized scope prescribed in a transaction that predates the subsequent acquirer’s being in bad faith.

The Subcommittee labelled these activities as “unfair competition activities” and indicated that they would aim to make civil remedies available for these activities, such as injunctions (Article 3 of the Unfair Competition Prevention Act), damages (Article 4 of the Unfair Competition Prevention Act), and presumed amount of damages (Article 5 of the Unfair Competition Prevention Act).

(3) Protection by tort under Civil Code

Making a dead copy of valuable data in which a certain degree of money and labor has been invested can be described as the use of significantly unfair means to infringe business rights that deserve legal protection, and may constitute a tort under Article 709 of the Civil Code.

However, the judgment of the First Petty Bench of the Supreme Court of December 8, 2011 (reported in Hanrei Times, Vol. 2142, page 79) (the North Korean movie case) held that the use of works that do not constitute works prescribed in the items of Article 6 of the Copyright Act does not constitute tort unless there are special circumstances such as infringement of a legally protected interest other than the interest pertaining to the use of a work that is subject to regulation under the Copyright Act, and if the logic of this precedent is applied it becomes necessary to be aware that tort may not necessarily be constituted even in the case of making a dead copy of a database that is not the copyrightable work of a database.

(4) Protection by Unauthorized Computer Access Prohibition Act

If a third party acquires data by unauthorized login or an attack on a security hole, such act of unauthorized access will be subject to criminal punishment (the items of Article 2(4), and Article 3 and Article 11 of the Unauthorized Access Prohibition Act).

(5) Technology for preventing unauthorized use, etc.
III Basic Legal Knowledge Relevant Upon Examining Data Contracts

Methods to prevent unauthorized use or unauthorized leaks of provided data include encrypting the provided data, placing access restrictions on it, methods of making the source or other attributes of the data clear using digital watermarking technology, and blockchain technology. Also, a business model for preventing provided data leaking from the hands of data recipients is the method of installing a server at the data provider’s factory that contains the data recipient’s analysis system, performing the analysis of operating data, etc. within such server, and then providing the results of such analysis to the data provider. There is thus this kind of method of completing the provision and analysis of the data on the data provider’s premises (essentially without the data leaving the factory of the data provider).

3 Appropriate allocation of consideration and profit

(1) Overview

The determination of appropriate consideration in data contracts (appropriate allocation of consideration and profit) should be dealt with on a case-by-case basis, and it is not appropriate to address all such cases univocally given that there is a need to examine the specific individual circumstances.

As the questions of whether or not to locate value in data circulation and utilization and what degree of value should be found there are questions that fall within the scope of the principle of freedom of contract, these Guidelines (Data Section) do no more than indicate, as a source of reference for business practice, examples of typical approaches to the allocation of consideration and profit between parties in an equal relationship.

Generally speaking, the determinative factors that have an effect on the allocation of consideration and profit in data contracts include the type of data, the scope of use of the data (including geographical restrictions),\(^\text{16}\) the value generated by the data, usage restrictions on derivative data, generated rights such as intellectual property rights, the allocation of liability in the event that damage is caused, determination of license fees and royalties, and allocation of expenses for data generation and management.

If the value of data is unable to be calculated, it can naturally be considered that negotiations or final agreement on the data contract would also become difficult. We therefore provide examples below of “trial verification of value using data” and “initial royalties plus running royalties” as methods for verifying the appropriate allocation of consideration and profit in data contracts.

(2) Forms of appropriate consideration and distribution of profit in data contracts

(i) Trial verification of value using data

When engaged in business that uses data it is not clear how much value will be generated, so one method is to perform a trial run, on a small scale, of a business that uses data, and then use the results of such trial to verify the value of the data. Taking the case of a convenience store, for example—big data is used to identify potential changes to the product display method, which are implemented on a trial basis in certain number of stores in certain regions, then the increase in sales attributable to such method is verified and, based thereon, the company

\(^{16}\) See Part IV-2-(5) below regarding data localization and cross-border privacy rules.
receives provision of the data for an amount of consideration that is commensurate to such increase in sales, finally introducing the new display methods based on such data to all of its stores.

This kind of method may be a useful mechanism for the appropriate allocation of risks and results. Specifically, by using this method it may become possible to ascertain the results of using the data (such as increases in sales) and to calculate an amount of consideration for provided data that is commensurate to such results.

(ii) Initial royalties plus running royalties
This method is often used in license agreements for intellectual property rights, etc., and involves paying an initial royalty (a certain amount of money) when the contract is executed, then subsequently pay as a running royalty (an amount of money corresponding to the profits, etc. paid during the contract term) a certain proportion of any profits generated as a result of the use of the data. This method, too, can be described as one means of appropriately allocating risks and results.

Note, however, that data is something that is generated on a daily basis, and that data sometimes derives its value from the very fact that it is continually updated. In the case of such data, one method may be to enter into an agreement to pay running royalties on condition of continuous provision of the data.
VI  “Data Provision Type” Contracts

IV  “Data Provision Type” Contracts (Provision of Data from One Party to the Other Party)

1  Structure

(1)  Definition of data provision type contracts

In these Guidelines (Data Section), “data provision type” contract means a contract which is based on the premise that there is no dispute between the parties with respect to the factual state that only one party (data provider) retains the data subject to the transaction and that the data provider provides such data to the other party and which provides for the other party’s utilization rights and other conditions of the data provision.

For example, in the case where a manufacturer of a certain product has conducted various tests by itself in the course of developing products that satisfy dimensional accuracy and intensity requirements from a customer and the use of data acquired from such tests can drastically reduce the man-hours of the product development, a “data provision type” contract would be applicable for the transaction in which the manufacturer sells, or grants license of, such data to a third party.

The term “utilization rights” in this context means the authority to freely exercise the following rights: the right to utilize; right of possession and management; right to demand reproduction; right to claim payment of remuneration for sale or grant of rights; right to claim deletion, disclosure, correction, etc. of data and termination of its utilization; and any other rights arising under the contract with respect to the data.

The following terms used in this Part IV of these Guidelines (Data Section) have the following meanings.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data provider</td>
<td>The party who provides data under a data provision type contract.</td>
</tr>
<tr>
<td>Data recipient</td>
<td>The party who receives data under a data provision type contract.</td>
</tr>
<tr>
<td>Provided data</td>
<td>The data provided from the data provider to the data recipient under a data provision type contract.</td>
</tr>
<tr>
<td>Derived data</td>
<td>Data newly created through processing, analysis, editing, integration, etc. of the provided data.</td>
</tr>
</tbody>
</table>

(2)  Categories of data provision type contracts

Data provision type contracts can be organized into three categories, which are (i) assignment of data, (ii) license of data and (iii) joint utilization (cross license) of data, as described below.

(i)  Assignment

a  Assignment of data

As described in III above, as data is intangible and is not the subject of ownership under the Civil Code, a transfer of ownership of data is not included in the concept of an assignment of data. Therefore, an assignment of data is generally considered to mean that all authorities relating to the data, including the status to control the utilization of the data, are transferred to the assignee and the assignor ceases to have any authority relating to the data.
VI “Data Provision Type” Contracts

In the case where database copyright and other intellectual property rights have been established with respect to the data to be assigned, it is necessary to assign not only the status to control the utilization of individual data registered in the database but also the intellectual property rights relating to the data in order to prevent any intellectual property rights relating to the data from remaining with the data provider.

b Form of assignment of data
The followings are examples of the forms of assignment of data:

・ The method in which a record medium containing the data is delivered to the assignee and the assignor deletes such data;
・ The method in which the data is reproduced in a record medium of the assignee and the assignor deletes such data; and
・ The method in which access rights to the data in a server of a third party are granted to the assignee and the assignor ceases to have access rights to the data (or the method in which the assignor transfers the status under a contract with a third party relating to the management of the data to the assignee).

(ii) License
a License of data
With respect to the license of data, the data provider grants the utilization rights to the data retained by the data provider to the licensee within a certain scope, and the licensor does not cease to have all utilization rights to the provided data.

There is no concept of ownership under the Civil Code with respect to data, and the line between an assignment of data and a license of data is ambiguous. For example, it is unclear whether the data recipient is able to utilize the provided data in a manner not provided for in the contract. Therefore, if the category of license of data is adopted for a contract, it is desirable that the contract not only specifies that it is a “license” of the provided data but also warningly sets forth that “no authorities relating to the provided data, except for those expressly provided for in the contract, are transferred to the data recipient.”

In addition, with respect to the license of data, it is also advisable to specify in the contract whether the data provider reserves the right to grant a license of the provided data to a third party in addition to the licensee (non-exclusive) or makes the licensee exclusively utilize the data (exclusive).

b Form of license of data
The following is an example of the form of license of data:

・ The method in which the utilization rights (including access rights) to data in a server of the licensor is granted to the licensee but the licensor does not cease to have the utilization rights (including access rights) to such data and also obligates the licensee to delete, and suspend the access rights to, such data upon termination of the contract.
VI  “Data Provision Type” Contracts

(iii)  Joint utilization (cross license)

a  Joint utilization (cross license) of data

Joint utilization (cross license) of data means, in the case where there are two parties to the contract (Party A and Party B, for example), that Party A grants all or part of the utilization rights to the data retained by Party A to Party B by contract while, on the other hand, the Party B grants all or part of the utilization rights to the data retained by Party B to Party A by the same contract. The joint utilization (cross license) of data also applies in the case where there are three or more parties to the contract.

In the category of joint utilization (cross license) of data, both Party A and Party B permit the other party to utilize their respective data, and it becomes increasingly likely that the respective data might be contaminated by the other party. Therefore, it is desirable to further sophisticate the details of the obligation of confidentiality in the contract by such means as establishment of provisions relating to segregation management of data or restriction of employees who can access the data.

b  Form of joint utilization (cross license) of data

The following is an example of the form of joint utilization (cross license) of data.

- The method in which the utilization rights (including access rights) to data in each server of Party A and Party B is granted to the other party respectively but each party does not cease to have the utilization rights (including access rights) to its own data and also obligates the other party to delete, and suspend the access rights to, such data upon termination of the contract.

---

17 The difference from the “data generation type” described in V below is whether the factual state that either one party retains the existing data is clear or not.
VI “Data Provision Type” Contracts

Diagram 2: Categories of “data provision type” contract

(3) Individuality of subject

The data provision type transactions may be conducted either on a one-to-one or one-to-many basis. It can be organized as follows based on the categories of data provision type contracts.

<table>
<thead>
<tr>
<th>Category of data provision type contracts</th>
<th>1:1</th>
<th>1:n</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>License</td>
<td>Yes</td>
<td>Yes (No, in the case of exclusive license)</td>
</tr>
<tr>
<td>Joint utilization (cross license)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
2 Main legal issues for data provision type contracts

(1) Utilization rights to derived data, etc. utilizing provided data

(i) Derived data, etc. generated from provided data

The utilization of the provided data (original data) from the data provider may generate various derivative products through processing, analysis, editing, integration, etc. of such data or any other means by the data recipient. The following are conceivable examples of derivative products:

- Derived data acquired through the processing, analysis, editing, integration, etc. the provided data;
- Intellectual property rights created through the processing, analysis, editing, integration, etc. the provided data; and
- Trained parameters generated based on the provided data (please refer to AI Section, rather than this Section, for the handling of trained parameters).

In the case of assignment of data, as all rights relating to the provided data are transferred to the data recipient, the data recipient can also utilize the derived data or other derivative products generated from the provided data.

In the cases of license of data and joint utilization (cross license) of data, on the other hand, it cannot be unambiguously determined which party has the utilization rights to the derived data or other derivative products, so they are examined respectively in (ii) and (iii) below.

(ii) Utilization rights to derived data, etc.

a Derived data

The provided data from the data provider may be raw data which has not been organized in any manner, and it is possible that the processing, analysis, editing, integration, etc. of such data might generate data with new knowledge and value. It cannot be unambiguously determined whether the authority to use such derived data belongs to the data provider or the data recipient.

In general terms, if there is no clear agreement as to the utilization rights to the derived data, it is considered that the issue of whether the utilization rights to the derived data belongs to the data recipient or the data provider would be reasonably interpreted based on the nature of the provided data (original data), expenditure and efforts made to acquire or collect the provided data (original data), nature of trade secrets, degree and expense of the processing, analysis, editing, integration, etc. of the provided data (original data), whether all or part of the provided data (original data) is contained in the derived data as recoverable data, and other factors.

However, there are various types of derived data and it is necessary that the parties share a common understanding, and if it is left unclear as to which party has the utilization rights to derived data in the contract, it might be a source of dispute in the future. Therefore, it is desirable to define the derived data and make it clear as to the utilization rights to derived data in the contract.

In some cases, so-called statistics information might be generated as derived data. “Statistics information” means data acquired by aggregating the items of common factors extracted from information of multiple parties for each category. The utilization rights to statistics
VI  “Data Provision Type” Contracts

information also cannot be unambiguously clarified in many cases, and it is advisable to specify which party has the utilization rights to such data in the contract.

b  Intellectual property rights

It is also possible that the data recipient generates copyrights, patent rights or other intellectual property rights based on the provided data in the course of processing, analysis, editing, integration, etc. of the same. If the parties wish to change the holder of the intellectual property rights so generated, it is desirable to expressly set forth the holder of the intellectual property rights generated from the provided data in the contract to avoid any future dispute.

c  Utilization of derived data, etc.18

In the case where it is reasonably interpretable that the utilization rights to the derived data belongs to the data recipient or where intellectual property rights created through the processing, analysis, editing, integration, etc. of the provided data belong to the data recipient, it is considered that whether or not to approve the data provider to utilize such derived data, etc. is likely to become an issue. Therefore, it is advisable to set forth in the contract whether to permit the data provider to utilize the derived data, etc. and, if so, the scope of the authority of the data provider and consideration for such utilization.

It should be noted that, if the data provider obligates the data recipient to assign, or grant exclusive license of, intellectual property rights attributable to the data recipient created through analysis, etc. of the derived data or provided data for which the data recipient owns the utilization rights, it might constitute unfair trade practices under the Antimonopoly Act.

(iii)  Distribution of profits obtained from derived data, etc.

The data provider may argue that, from its own perspective, any derived data or intellectual property rights were generated because of the existence of the provided data. Therefore, it is possible that the data provider insists that it also owns the utilization rights to the derived data or that the intellectual property rights so created belong to the data provider or demands the data recipient to grant license of or transfer the utilization rights to such data or intellectual property rights.

In such case, the joint ownership of the utilization rights to the derived data and intellectual property rights created might be a possible solution.

However, if a patent right is jointly owned, the consent of other joint owners is required to assign or grant license of such patent right (Articles 73(1) and 73(3) of the Patent Act), and if a copyright is jointly owned, the content of all other joint owners is required to assign such copyright (Article 65(1) of the Copyright Act) and, moreover, to exercise the copyright by itself. As described above, it should be noted that, in the case of joint ownership of intellectual property rights, the future exercise of the intellectual property rights would be restricted, and it is necessary to make an express agreement separately by contract for any other arrangements.

18 Derived data, etc. means derived data and intellectual property rights created through processing, analysis, editing, integration, etc. of the provided data.
VI “Data Provision Type” Contracts

On the other hand, instead of adopting the joint ownership, it is also possible to make the utilization rights to the derived data or intellectual property rights remain with the data recipient and distribute a part of profits generated from the utilization of such rights to the data provider. In concrete terms, for example, the data recipient may pay a certain percentage of sales obtained from the business using the derived data to the data provider.

(2) Liability against provided data which deviates from what was expected (quality of provided data)

With respect to the data provision type contracts, it is possible that the provided data has quality problems, such as when the provided data is inaccurate, incomplete or invalid (no fitness for the purpose of the contract) or the provided data is infected and not safe or otherwise infringes any intellectual property rights of a third party, and that the data recipient fails to achieve the purpose of the contract as a result and accordingly pursue legal liability against the data provider for the quality of the provided data.

The “accuracy of data” in this context means that the data does not contain any data which differs from the fact, such as time axis variation, wrong unit conversion or falsification or fabrication of data just to pass examination, and the “completeness of data” means that all data is gathered together and there is no defect or inconsistency. In addition, the “validity of data” means that the contents of the data are sufficient to achieve the results as planned.

In the case that a data provision type contract is an onerous contract and a quality problem occurs in respect of the data, the liability for defect warranty (liability for non-conformity with contract) under the Civil Code is considered to apply. However, as there are various types of quality problems with respect to the provided data, it is desirable to clarify in the contract as to what extent the data provider should be liable for the accuracy, completeness, validity, safety, non-infringement of intellectual property rights of a third party and other factors of the provided data (for example, the representation and warranty clause may be used).

If it is specified in the contract that the data provider would not warranted any such quality of the provided data, such provision is considered to be effective in principle. However, in the case that the provided data has a quality problem caused by willful misconduct or gross negligence of the data provider, then it is considered that the data provider might be liable for such quality of the provided data (analogue application of Article 572 of the Civil Code). 19

In addition, it is also possible to make the data provider bear the obligation to make efforts for procuring the accuracy, completeness, validity, safety, etc. of the provided data by specifying, for example, that “the data provider shall, to the extent possible, make efforts to procure that the provided data is accurate and complete and is valid and safe in relation to the purpose of the contract.” However, it should be noted that, even if it is merely an obligation to make efforts for the accuracy, completeness, validity and safety of data, the data provider might be made liable for the failure to perform obligations as a breach of the obligation to make efforts if there

19 The question of who would/would not be liable for the quality of the provided data, and in what way they would be liable, may vary depending on the category of the field and nature and type of the provided data. Therefore, the existence, scope and details of the liability should be flexibly determined by contract taking into consideration various circumstances with respect to the contract, and these Guidelines (Data Section) merely present one of those proposals.
VI “Data Provision Type” Contracts

is a fact that the data provider has not made any effort for the accuracy, completeness, validity and safety of data.

(3) Damage arising out of utilization of provided data

It is possible that a legal dispute may occur between the data recipient and a third party in relation to the utilization of the provided data, such as when the data recipient utilizing the provided data becomes subject to a claim for damages from a third party for infringement of intellectual property rights relating to such data.

In such case, there are two different ideas as to who should bear the expenses and damages required to settle the legal dispute with the third party, and both of them are considered to be reasonable: (i) the data provider should bear those expenses and damages as long as they are caused by the provided data, and (ii) the data recipient should bear the expenses and damages caused by the provided data based on the premise that the data provider has not warranted for the quality of the provided data.

Therefore, it is advisable to set forth in the contract as to which party should be liable for expenses and damages incurred as a result of a legal dispute with a third party occurring in relation to the utilization of provided data. However, it is considered that the data provider is not required to bear expenses and damages caused by the provided data in the case that the data recipient utilizes the provided data beyond the extent stipulated by the contract (in other words, in the case where the data recipient utilizes the provided data in a manner contrary to the contract). Thus, in the case that the data provider bears such obligation, it is considered better to limit the liability by setting forth a provision in the contract such as “(the data provider shall be liable) only in the case that the data is utilized in the manner stipulated in the contract.”

In addition, in the case that the data provider is made liable, it is also possible, in order to limit the liability of the data provider, to set the maximum amount of the liability to be the amount of consideration received by the data provider from the data recipient.

(4) Unintended utilization of provided data

In the case that a provision on prohibition of unintended utilization is set forth in data provision type contracts, it is considered that the utilization of data is often restricted to a certain extent.

For example, in the case where machine tool manufacturer A and machine tool manufacturer B enter into a contract under which Manufacturer A places sensor in the machine tools and sells them to Manufacturer B and Manufacturer B provides Manufacturer A with data acquired from the sensor placed in the machine tools for “the purpose of maintaining the machine tools (maintenance purpose),” if Manufacturer A (i) utilizes such data to upgrade the version of other machine tools manufactured by Manufacturer A or (ii) processes the information acquired from such data to remove any confidential information of Manufacturer B and provide the processed information to a third party, it might fall under a utilization of provided data for a purpose other than “the purpose of maintaining the machine tools (maintenance purpose)” in both cases and therefore might be a breach of the provision on prohibition of unintended utilization.
VI “Data Provision Type” Contracts

Diagram 3: Data provision type contracts and provision on prohibition of unintended utilization

In the case where the provided data is expected to be utilized upon being processed, analyzed, edited, integrated, etc. in the future, it is considered necessary for the data recipient to consider including the provision which assume the cases of (i) and (ii) above in the contract.

In the case of (i), Manufacturer A would be able to utilize the data acquired from the sensor without breaching the provision on prohibition of unintended utilization if the purpose of data utilization is not limited to “the purpose of maintaining the machine tools (maintenance purpose) but extended to, for example, “the purpose of maintaining the machine tools (maintenance purpose) and improving the performance of the machine tools, such as developing a new model or otherwise upgrading the versions.”

In the case of (ii), as the information acquired from the sensor might contain trade secrets, know-hows, etc. of Manufacturer B, it is possible that Manufacturer A might not be able to obtain consent from Manufacturer B for the provision of the data to a third party (and as a result, the provision of the data to a third party might fall under an unintended utilization). In particular, in light of the current situation where data distribution has not been active yet, there is a good chance that, even if all confidential information is removed from the data provided from Manufacturer B, Manufacturer B might still deny to give consent for the provision of the data to a third party from a vague sense of anxiety that any of its know-how, etc. might be leaked in connection with the provision of the data to the third party.

Accordingly, in the case of (ii), it is necessary to have measures to obtain the consent from the data provider for the data provision to a third party. Examples of such measures are: (a)
VI “Data Provision Type” Contracts

establishing a provision regarding a procedure in which, when the data recipient processes the provided data and provides such data to a third party, the data provider checks the details of the data to be provided to a third party in advance and confirms that all confidential information of the data provider is removed; (b) obtaining the consent to the data provision to a third party by specifying that the profits obtained by the data recipients from processing the provided data and providing them to a third party are returned to the data provider at a certain rate; and (c) providing the data provider who gives consent to the provision of the derived data to a third party with the benefits of receiving data acquired from other data providers.

(5) Issues for cross-border transactions

(i) Data localization and restrictions on cross-border transfer

Data localization is a rule based on the idea that, with respect to an online service, etc. for example, the physical server performing such service must operate in the country where such service is provided; specifically, all data necessary to provide the service must exist within the same country. Despite different viewpoints, data localization and the cross-border transfer regulations which focus on the protection of personal information, as typified by the Personal Information Protection Act in Japan and the Data Protection Directive 95/46/EC and the General Data Protection Regulation (GDPR) in the EU, share the same idea of restricting the cross-border transfer of data (Mitsubishi UFJ Research and Consulting Co., Ltd. “Report on 2017 International Research Business for Establishment of Integrated Domestic and Foreign Economic Growth Strategy (Research of Regulations Relating to Digital Trades)” (February 2018)).

(ii) Foreign Exchange and Foreign Trade Act (Act No. 228 of 1949)

In Japan, the export controls under the Foreign Exchange and Foreign Trade Act have been implemented for the purpose of preventing any arms, nuclear weapons, etc. general-purpose items that can be diverted to military use and technologies relating to the above from falling into the hands of any country or terrorist subject to security concerns.

With respect to the technologies, in concrete terms, the technologies used for the development, etc. of weapons and sensible technologies used for commercial products are listed in the appended table of the Foreign Exchange Order (the “listed technologies”). It is required to obtain a license from the Minister of Economy Trade and Industry when the listed technologies are provided in any foreign country or provided by a resident to a non-resident (foreigner, etc.) (referred to as “regulations on listed technologies”).

Even if it does not fall under the listed technologies, it is required to obtain a license from the Minister of Economy Trade and Industry in the case that the technology to be provided might be used for the development, etc. of nuclear weapons, etc. or conventional weapons (referred to as “catch-all control”).

Therefore, when conducting a cross-border transfer of technical data, etc., which is one of the technological forms, it is required to comply with the Foreign Exchange and Foreign Trade Act upon confirming the details of the controls imposed thereby. In particular, as it is often difficult to take back technologies once they are provided, due care must be taken for the management of the technologies.
VI “Data Provision Type” Contracts

In addition, any transaction by which a resident provides technical data subject to the regulations on listed technologies or catch-all control to a non-resident in Japan is subject to the control even if it is conducted in Japan.

(iii) Governing law

With respect to transactions with foreign companies, it is desirable to make an agreement to set the laws of Japan as the governing law for such transactions so that one is able to hire Japanese attorneys and thereby eliminate communication barriers and make it easier to foresee the outcome of any disputes.

However, setting the governing law would not be sufficient as a choice of rules to apply in a dispute resolution, and, depending on the means of dispute resolution, the choice of the governing law as agreed between the parties might be made void or otherwise restricted. For example, if dispute resolution by court is chosen, the applicable law would be determined in accordance with the private international laws of the country in which the court is located in principle, and some countries do not allow the parties to choose the governing law. In such case, it is worth considering to choose out-of-court proceedings, etc. (for example, international arbitration) in order to adopt the law of its choice.

Especially in relation to data transactions, it should be noted that, even if the laws of Japan are selected as the governing law, it is considered that the parties might not be released from regulations of other countries relating to the data localization and cross-border transfers described above.

(iv) Jurisdiction (means of dispute resolution)

As conducting trials at a court in Japan would provide the benefits of reducing the procedural burden and making it easier to foresee outcomes, it is desirable to set a court in Japan as the court with exclusive jurisdiction.

However, even if a party files a lawsuit against a foreign company in a court in Japan and obtains a judgment from the court, it is often difficult to enforce the judgment due to the issue of mutual recognition. Therefore, arbitration is often chosen as the means of dispute resolution instead of court proceedings. In the case that arbitration is chosen as the means of dispute resolution, matters such as the number of arbitrators and the place and language of arbitration are also often determined. In the case of international commercial arbitration, since many countries have ratified the “Convention on the Recognition and Enforcement of Foreign Arbitral Awards” (so-called New York Convention; Convention No. 10 of July 14, 1961), there is a benefit of easily recognizing and enforcing the arbitral awards rendered in a foreign country. However, it should be noted that arbitration also has disadvantages such as (i) it is necessary to pay remuneration to arbitrators in the form of arbitration costs, and the amount could be high especially when there are three arbitrators, etc., and (ii) arbitration has only first trial and no appeals.

(v) Legal system relating to data protection in major countries

In the case where the counterparty to a data provision type contract is a foreign company and the provided data is transferred to a foreign country, it is possible, as to the issue of whether to
VI  “Data Provision Type” Contracts

set the laws of Japan or laws of such foreign country as the governing law, to choose whichever is more advantageous upon taking into consideration the details of the laws relating to data protection of such country.

However, it should be noted that even if the governing law is selected in the contract, the parties might not necessarily be released fully from the regulations regarding data protection of other countries.

(6) Notes for data containing personal information, etc.

(i) Whether or not provided data contains “personal data”

“Personal information” means (i) information relating to a living individual (ii)(a) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual) or (b) containing an individual identification code (Article 2(1) of the Act on the Protection of Personal Information).

In addition, personal information constituting a personal information database, etc. is referred to as “personal data,” and it is required to obtain in advance a principal’s consent upon providing personal data to a third party in principle (Article 23(1) of the Act on the Protection of Personal Information). Accordingly, in the case that the data to be provided by data provision type contracts contains “personal information” or falls under “personal data,” it should be handled in accordance with the regulations under the Act on the Protection of Personal Information.

In order for any information to fall under “personal data,” it is a precondition that it must first fall under “personal information,” and information “whereby a specific individual can be identified (including that which can be readily collated with other information and thereby identify a specific individual)” would fall under “personal information.” On the other hand, “statistics information,” which refers to data acquired by aggregating the items of common factors extracted from information of multiple parties and eliminating any relationship with individuals, is not required to be handled in accordance with the regulations under the Act on the Protection of Personal Information.

For example, vehicle information, driving information, location information and other information acquired through vehicle-mounted equipment such as driving recorders may fall under “personal data” if they are connected to the information of the drivers (driver ID, etc.) and are able to identify the specific individuals. However, on the other hand, the same may fall under “statistics information” if it is merely information that aggregates the above information for the purpose of identifying the places where traffic accidents tend to occur or where the traffic is likely to be heavy in a manner which has no relationship with any individual (or eliminates such relationship), and such information is considered unnecessary to be handled in accordance with regulations under the Act on the Protection of Personal Information.

(ii) In the case provided data contains “personal data”

In the case that the provided data contains “personal data,” it is required to obtain in advance a principal’s consent upon providing the provided data to a third party as described above in principle (Article 23(1) of the Act on the Protection of Personal Information).
VI “Data Provision Type” Contracts

However, if the transfer of personal data is conducted though (i) entrustment, (ii) business succession or (iii) joint utilization, the recipient shall not fall under “third party” (Articles 23(5)(i) through (iii) of the Act on the Protection of Personal Information).

In addition, (i) in the cases based on laws and regulations (Article 23(1)(i) of the Act on the Protection of Personal Information), (ii) in the cases in which there is a need to protect the life, body or property of a person (including a corporation), and when it is difficult to obtain a principal’s consent (Article 23(1)(ii) of the same), (iii) in the cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal’s consent (Article 23(1)(iii) of the same) or (iv) in the cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal’s consent would interfere with the performance of the said affairs (Article 23(1)(iv) of the same), it is not required to obtain in advance a principal’s consent upon providing the personal data to a third party.

It should be noted that the provision to a third party on an “opt-out” basis is permitted for general personal information (Article 23(2) of the Act on the Protection of Personal Information) but not for special care-required personal information.

(iii) Utilization of anonymously processed information

In the case that the provided data contains personal data, a conceivable means of processing such data for flexible utilization is anonymous processing. For example, it is possible to apply the framework of “anonymously processed information” under the Act on the Protection of Personal Information. “Anonymously processed information” means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each item in Article 2(9) of the Act on the Protection of Personal Information in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information.

The anonymously processed information system was established for free utilization of person related data on certain conditions alternative to the principal’s consent, and a party, when having produced anonymously processed information, shall disclose to the public the categories of information relating to an individual contained in the anonymously processed information without delay after producing such information (Article 36(3) of the Act on the Protection of Personal Information) and, when providing the anonymously processed information to a third party, shall (i) in advance disclose to the public the categories of information concerning an individual contained in anonymously processed information to be provided to a third party and its providing method, and (ii) state to the third party explicitly to the effect that the information being provided is anonymously processed information (Article 36(4) of the Act on the Protection of Personal Information).

With respect to the method of anonymous processing, Article 19 of the “Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3 of October 5, 2016)” provides the standards for the method of producing anonymously processed information pursuant to Article 36 of the Act on the Protection of Personal Information20, and the guidelines, etc. prepared by the Personal Information Protection

---

VI  “Data Provision Type” Contracts

Commission\textsuperscript{21} can also serve as a useful reference. When producing anonymous processed information, the information might not be deemed to have been “processed so as not to be able to identify a specific individual” if a party only deletes ID, name, etc. therefrom or if a party deletes ID, name, date of birth and other similar information but still a specific individual can be identified from any other information contained therein (for example, purchased products, time of purchase, place and gender). As described above, the method and degree of anonymous processing need to be determined on a case-by-case basis, so it should be noted that anonymous processing entails certain difficulties.

In addition, as described in IV-2-(4) above, even if anonymous processing of the provided data and provision of the same to a third party would not be a breach of the Act on the Protection of Personal Information, it might be a breach of provisions on prohibition of unintended utilization under data provision contracts. Therefore, careful examination of such provisions is required upon providing anonymously processed information to a third party.

In the case that information eventually becomes “statistics information” through processing, such information no longer has any connection with specific individual and therefore would not fall under “anonymously processed information” and, as a result, it is not required to be handled in accordance with the Act on the Protection of Personal Information as described above.

(iv) Notes for cross-border data

a Provision of personal data to a third party in a foreign country

In the case where a business operator provides personal data to a third party in a foreign country, the business operator must obtain a principal’s consent to the effect that “he or she approves the provision to a third party in a foreign country” in principle (Article 24 of the Act on the Protection of Personal Information). However, it is not necessary to obtain a principal’s consent to the effect that “he or she approves the provision to a third party in a foreign country” in the case that (i) the third party to which the personal data is provided is in a country designated in the Enforcement Rules for the Act on the Protection of Personal Information as a country that has a personal information protection system recognized to be at the level equivalent to that of Japan,\textsuperscript{22} (ii) the third party to which the personal data is provided has established a system that complies with the standards set forth in Article 11 of the Enforcement Rules for the Act on the Protection of Personal Information as the system necessary for continuously taking measures equivalent to those which shall be taken by a personal information handling business operator\textsuperscript{23}, or (iii) any of the exceptions set forth in Article 23(1) of the Act on the Protection of Personal Information applies.

\textsuperscript{21} Personal Information Protection Commission, Note 13 “Guidelines on the Act on the Protection of Personal Information (Anonymously Processed Information)”

\textsuperscript{22} There is no country which is currently designated in the Enforcement Rules for the Act on the Protection of Personal Information as a country that has personal information protection system recognized to be at the level equivalent to that of Japan. However, the proceedings regarding the designation of EU by the Personal Information Protection Commission under Article 24 of the Act on the Protection of Personal Information and the adequacy decision of Japan by the European Commission under Article 45 of GDPR have been carried out between the Personal Information Protection Commission and the European Commission.

\textsuperscript{23} The standards are to be falling under any of each following item:
VI “Data Provision Type” Contracts

The issue of whether or not the recipient falls under a “third party in a foreign country” would be determined based on the juridical personality. Therefore, while the provision of personal data by a Japanese company to its foreign subsidiary falls under the provision of personal data to a “third party in a foreign country,” the provision of personal data by a Japanese company within the same juridical personality such as to its foreign branch or office does not constitute the provision of personal data to a “third party in a foreign country.”

In addition, even in the case of a foreign corporation which was established under the laws and ordinances of a foreign country and has an address in a foreign country, such foreign corporation does not fall under “third party in a foreign country” if it falls under “personal information handling business operator.” Accordingly, in the case that a Japanese company provides personal data to, for example, a Tokyo branch of a foreign-affiliated company, the Tokyo branch of the foreign-affiliated company falls under “personal information handling business operator” and therefore does not fall under “third party in a foreign country.”

b Receipt of personal data from a party in a foreign country

In the case of receiving personal data from a party in a foreign country, the laws of such country would apply and the data need to be handled in accordance with the laws of such country. Therefore, in the case where a party sells a machine and acquires operation information of the machine which contains personal information from a sensor fitted on the machine, for example, if the party sells the machine to a foreign country and acquires the operation information of the machine which contains personal information directly from the sensor on the machine installed in such foreign country, it is necessary to examine the legal system regarding personal information of such foreign country where the machine is installed.

As described in IV-2-(5)-(i) above, as it is not uncommon that cross-border transfer of personal data is regulated by laws and ordinances in foreign countries and the scope of personal information varies among countries, it is extremely important to handle information in accordance with laws and ordinance of the applicable country.

3 Causes and countermeasures regarding impediments to data distribution

(1) Concerns and countermeasures regarding leaks of know-how caused by utilization of provided data

As mentioned in III-2 above, data providers have concerns that their trade secrets and know-how contained in the provided data might leak out of the company in connection with the provision of the data, and it can be said that such concerns would impede data distribution. As described in III-2 above, it would be possible to distribute data and protect the trade secrets and know-how contained in the provided data though legal protection by contract, the Unfair

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

(ii) a person who receives the provision of personal data has obtained a recognition based on an international framework concerning the handling of personal information
VI “Data Provision Type” Contracts

Competition Prevention Act, the Civil Code, the Act on Prohibition of Unauthorized Computer Access, etc. and technical means to secure the safety of the provided data.

(2) Difficulty of calculating data value

As described in III-3 above, the difficulty of calculating data value also impedes data distribution in certain ways. However, as described in III-3 above, there can be a way to adequately calculate the value of the data by applying the idea of experimental verification of the value to be created by using the data or any other means, so it is worth considering actively adopting such means.

4 Method of determining appropriate data provision type contracts

With respect to data provision type contracts, it is desirable to consider setting forth the following items in the contract. For specific examples of the provisions of data provision type contracts, please see the draft model contract for data provision type contracts in VII.

(1) Definitions of data and other terms

☐ Definition of provided data
☐ Definition of derived data
☐ Purpose of contract

(2) Details and method of provision of provided data

(i) Details of provided data

☐ Subjects of provided data (outline of the provided data)
☐ Items of provided data
☐ Amount of provided data
☐ Granularity of provided data
☐ Frequency of updating of provided data

(ii) Method of provision of provided data

☐ Forms of provision of provided data (paper/electronic file, and in the case of electrical file, the file format)
☐ Means of provision of provided data (e-mail transmission, downloading from a server, grant of access right to a server or return of data recorded in recording media)
☐ Frequency of provision of provided data
☐ Method to change the method of provision of provided data (forms, means and frequency of provision)
VI “Data Provision Type” Contracts

(3) License, etc. of provided data

- Categories of data provision type contracts (license, assignment or joint utilization)
- Prohibition of provision of provided data to a third party, etc.
- Prohibition of unintended utilization of provided data
- Prohibition of processing, analysis, editing, integration, etc. of provided data for purpose other than the Purpose
- Owner of intellectual property rights relating to provided data
- Proprietary/non-proprietary license in the case of license of provided data

(4) Consideration and conditions of payment

- Amount of consideration for provided data and the calculation method thereof
- Method of payment of consideration for provided data

(5) No warranty relating to provided data

- Warranty/no warranty regarding non-infringement of rights of third parties relating to provided data
- Warranty/no warranty regarding the accuracy and completeness of provided data
- Warranty/no warranty regarding the safety of provided data (whether or not provided data is infected with a virus)
- Warranty/no warranty regarding the effectiveness of provided data and its compatibility to the Purpose
- Warranty/no warranty regarding non-infringement of intellectual property rights of third parties relating to provided data

(6) Limitation of liability, etc.

- No grant of authority for the disclosure, amendment or addition of the details of provided data, etc. to data recipient
- Liability to resolve disputes with a third party arising in relation to provided data (in the case of utilization in a form not breaching the contract/in the case of utilization in a form breaching the contract)
- Maximum amount of damages incurred by data provider

(7) Status of utilization

- Report on whether or not the data recipient utilizes provided data in accordance with the contract
- Audit by data provider on whether or not data recipient utilizes provided data in accordance with the contract
VI “Data Provision Type” Contracts
- Payment of additional consideration, etc. in the case that provided data is discovered not to be utilized in accordance with the contract by the audit

(8) Management of the provided data
- Separate management of provided data from other information
- Duty of care of a good manager owed by data recipient relating to the data management
- Request for report or rectification relating to the management status of provided data

(9) Duty to mitigate damage
- Notification duty of data recipient when divulgence of provided data, etc. is found
- Duty of data recipient to examine and report preventive measures upon occurrence of data divulgence, etc.

(10) Confidentiality
- Definition of confidential information
- Details and exceptions of obligation of confidentiality
- Survival of obligation of confidentiality after termination of the contract and the survival period thereof

(11) Handling of derived data, etc.
- Existence of the utilization rights to derived data
- Owner of intellectual property rights arising from the utilization of provided data by data recipient
- Authority of data provider to utilize intellectual property rights arising from the utilization of provided data by data recipient
- Distribution of profits obtained by the utilization of intellectual property rights arising from the utilization of derived data by data recipient

(12) Effective period
- Effective period of the contract
- Automatic renewal of the contract

(13) Force majeure
- (In addition to standard force majeure events,) whether or not power failure, malfunction of communications facilities or suspension of provision or emergency maintenance of cloud services or other outsourcing services fall under a force majeure event
VI “Data Provision Type” Contracts

(14) Termination
(Standard provisions on termination of contract should be sufficient)

(15) Measures after termination of the contract
□ Destruction or deletion of provided data after termination of the contract
□ Submission of certification of destruction or deletion of provided data

(16) Elimination of antisocial forces
(Standard provisions on elimination of antisocial forces should be sufficient. For example, the model clause for Boryokudan elimination prepared by the Metropolitan Police Department.)

(17) Survival
□ Whether there is any excess or deficiency in the scope of provisions that should survive after termination of the contract

(18) Prohibition of assignment of rights and obligations
(Standard provisions on prohibition of assignment of rights and obligations should be sufficient)

(19) Entire agreement
(Standard provisions on entire agreement should be sufficient)

(20) Governing law
□ Which country or, state, etc.’s laws to choose as the governing law

(21) Dispute resolution
□ Whether to choose trial or arbitration as the agreed jurisdiction
□ Which place to choose as the forum for trial or arbitration
V “Data Generation Type” Contracts

V “Data Generation Type” Contracts (Handling of Data Generated With Participation of Multiple Parties)

I Structure

(1) Scope of subject of data generation type contracts

In these Guidelines (Data Section), “data generation type” contracts apply when new data that never existed before is generated with participation of multiple parties and the parties who participate in the data generation make an agreement as to the utilization rights to such data. The subject of this type of contract includes, for example, so-called raw data detected by sensors or the like and derived data acquired through processing, analysis, editing, and integration, etc. (in this Part V, “processing, etc.”) of such raw data.

The following are specific examples of assumed cases. In these Guidelines (Data Section), the contracts are assumed to take the form of negotiated transactions between the parties, but it is also possible that they take the form of terms of use or contractual clauses in cases such as Case 1 below or when executing a contract with general consumers.

Case 1

Machine tool manufacturer A plans to put a sensor in the machine tools delivered to the factories of its customers (B1, B2…) to analyze operation data of the machine tools obtained from the sensor. The operation data will be utilized when providing advice, maintenance or other after-services relating to the use of the machine tools to the customers using the machine tools from which the data was acquired. In addition, Manufacturer A considers analyzing the data acquired at each factory of customers and providing the method of use for productivity improvement to each customer as a best practice. Further, Manufacturer A considers utilizing such results of data analysis to apply for its own machine tool products and also plans to sell statistic information of the operation data to a third party in the future.

Diagram 4: Case 1

Parties involved in the data generation: Machine tool manufacturer A
Machine tool users B1, B2…

Data in question: Operation data of the machine tools
Analysis data of the operation data above

Case 2
In the wake of overworked bus drivers becoming a social problem, a bus company A, which operates a long-distance bus service, decided to make its employees put on a wearable device during work hours and acquire their vital data (body temperature, heart rate, perspiration, etc.) during work to conduct health management of the employees based on such data as a measure for improving the work environment. Specifically, Company A plans to co-develop a wearable device with Company B, which engages in health care services, and establish a system to monitor vital data of the employees (C1, C2…) acquired from the device on a real-time basis and raise an alert for those employees with physical deconditioning or accumulated fatigue. In addition, the vital data of each employee acquired from this system will be accumulated in the system managed by Company B, which will analyze those data to draw up and give advice to the company-wide healthcare management policy. Moreover, Company B is considering whether it may be possible for the vital data acquired through such service to be processed and utilized for other health management services in which Company B engages.

Diagram 5: Case 2

Parties involved in the data generation: Bus company A  
Healthcare service provider B  
Company A’s employees (bus drivers) C1, C2…

Data in question: Vital data of the employees  
Analysis data of the data above

Case 3

A leading logistics business operator A owns a number of delivery bases and warehouses all over the country and has a number of delivery vehicles traveling on the roads across the country all the time. Business Operator A intends to request Company B, which engages in weather forecasting and distribution of weather data and news, etc., to install environment sensors developed by Company B in each base facility and delivery vehicle in order to
V  “Data Generation Type” Contracts

generate weather forecasts based on the weather data acquired from such environment sensors. While Business Operator A plans to improve its delivery efficiency by using such information, it also plans to sell such information to third parties as a new profitable business because the weather forecasts to be acquired from this business are expected to be more accurate than traditional forecasts. In addition, Business Operator A also intends to request its subcontracting companies (C1, C2…) to install the sensor in each of their delivery vehicles.

Diagram 6: Case 3

Parties involved in the data generation: Logistics business operator A
Weather forecast service provider B
Business Operator A’s subcontractors C1, C2…

Data in question:
Weather data (temperature, humidity, atmospheric pressure, wind speed, etc.) acquired from the environment sensor
Weather forecast data acquired from analysis of the data above

(2) Issues regarding data generation type contracts

The main issues that would arise when executing data generation type contracts are as follows.

(i) Rules for arranging utilization rights are not clear despite the participation of multiple parties in data generation
V “Data Generation Type” Contracts

For example, in Case 1, it can be considered that the customers (B1, B2...) who actually operate the machine tools should have the utilization rights to the operation data. On the other hand, it is also possible to consider that Company A, which planned the installation of the sensors and organized the types and items of the data to be acquired, should have the utilization rights to the operation data. In addition, although the parties should consider the method of deciding the holder of utilization rights to derived data acquired by analyzing the raw data acquired from the sensors as a separate issue from the utilization rights to the raw data, there is no clear standard for deciding the utilization rights to the derived data either. Since the arrangement rules are not clear, the matter of how fairness among the parties is secured would become another issue.

(ii) Utilization method of generated data is often not necessarily clear

Despite the fact that the generation and accumulation of data has progressed due to the widespread adoption of IoT technologies and other reasons, it is often the case that parties fail to share a clear image as to the method of utilizing the data so generated. In addition, while some data creates greater value depending on the method of processing, etc., it is also often unclear at the time of executing the contract as to what kind of value will be created. Therefore, it is not easy to agree on the basis on which the profits and expenses are to be distributed.

(iii) Consideration of personal information and privacy rights

In the case that generated data contain any personal information, the regulations under the Act on the Protection of Personal Information, including the provision which requires a principal’s consent in principle in order to provide such data to a third party, will apply. In addition, even if the information does not fall under personal information, it might infringe a privacy right of any individual in some cases depending on the method of utilization, etc.

2 Main legal issues relating to data generation type contracts

(1) Terms and conditions of utilization to be established between parties

Parties will have to clarify the data generated in relation to the transaction (applicable data) and establish the terms and conditions of utilization of the applicable data, and the following are examples of the desirable terms and conditions that the parties should agree on.

<table>
<thead>
<tr>
<th>Items</th>
<th>Matters to be established</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope of applicable data</td>
<td>• Make efforts to clarify the scope of data generated in relation to the transaction (applicable data) by making a list of the applicable data or in any other manner</td>
</tr>
<tr>
<td></td>
<td>• Set forth the method of deciding the holder of utilization rights to any data not covered by the list above and other data for which the utilization rights have not been clearly agreed</td>
</tr>
<tr>
<td></td>
<td>• Roughen the granularity of data to the extent that business secrets and know-how can be removed or diluted as necessary to limit the scope and contents of the data to be acquired</td>
</tr>
</tbody>
</table>

41
V “Data Generation Type” Contracts

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose of utilization</strong></td>
<td>• Clarify the scope of utilization rights to the applicable data by establishing the purpose of utilization (for example, limit to utilization within a certain business domain or in relation to research and development contracts already determined between the parties)</td>
</tr>
<tr>
<td></td>
<td><strong>Availability of processing, etc. and utilization rights to derived data</strong></td>
</tr>
<tr>
<td></td>
<td>• Set forth the availability of processing, etc. of the applicable data and the method thereof</td>
</tr>
<tr>
<td></td>
<td>• Provide for utilization rights to derived data generated through processing, etc.</td>
</tr>
<tr>
<td><strong>Warranty/no warranty over content and continuous generation of data</strong></td>
<td>• Agree on the matters warranted and not warranted in relation to the accuracy of data and other matters (see IV-2-(2) above)</td>
</tr>
<tr>
<td></td>
<td>• In the case that data contains any personal information, warrant that the provisions of the Act on Protection of Personal Information are complied with and any necessary proceedings thereunder have been implemented (the purpose of utilization, details of consent to provision to a third party (or business entrustment or joint utilization), details of confirmation and record obligation, etc.)</td>
</tr>
<tr>
<td></td>
<td>• Agree on the matters warranted or not warranted in relation to the continuous generation of data and procurement of the amount of data</td>
</tr>
<tr>
<td><strong>Restriction of provision to a third party</strong></td>
<td>• Availability of provision of data to a third party</td>
</tr>
<tr>
<td></td>
<td>• In the case that provision of data to a third party is permitted, the terms and conditions imposed on the third party</td>
</tr>
<tr>
<td><strong>Distribution of profits and expenses</strong></td>
<td>• In the case that the provision of the applicable data to a third party, etc. generates profits, set forth the distribution of profits and expenses</td>
</tr>
<tr>
<td><strong>Management method and security</strong></td>
<td>• Set forth specific storage destination and management method of data and other matters based on the nature of data and risks</td>
</tr>
<tr>
<td><strong>Period of utilization</strong></td>
<td>• Determine the period in which data can be utilized</td>
</tr>
<tr>
<td><strong>Regions of utilization</strong></td>
<td>• Determine the countries and regions in which data can be utilized</td>
</tr>
<tr>
<td><strong>Handling of data upon termination of contract</strong></td>
<td>• Set forth whether data, including derived data, are required to be deleted or returned after termination of the period of utilization</td>
</tr>
<tr>
<td><strong>Governing law and jurisdiction</strong></td>
<td>• Agree on the law and jurisdiction applicable to the contract</td>
</tr>
</tbody>
</table>

(2) Scope and granularity of applicable data

(i) Clarification of scope of applicable data

Upon determining the data utilization rights, it is important for the parties to first clarify what kind of data would be generated and would become subject of the agreement in relation to the transactions. In particular, in the case where contracting parties include consumers or small and medium-sized companies, it becomes more important to share the common recognition as to what kind of data would be generated (collected) in the transactions and how the utilization...
V  "Data Generation Type" Contracts

rights to such data would be distributed. For example, in the case of the operation data of machine tools in Case 1, there is a possibility that any manufacturing know-how, production level or other matters of Customer B1 or other customer can be conjectured by analyzing the details of such data, and in such cases, it is often that Customer B1 and other customers do not recognize when and what kind of data had been measured and provided to machine tool manufacturer A.

As a specific method, it is useful to make a catalogue by listing the data to be generated before commencing any discussion regarding the utilization rights to the data. See examples of catalogue at the end of this Part V ((reference) Data Catalogue) for the specific form of catalogue. Since the purpose of preparing such catalogue is to avoid any misunderstanding or surprise attack among the parties and prevent any future dispute, it is desirable to list the applicable data as much as possible without any absence or overlaps in such catalogue.

In addition, there might be cases where it is practically difficult to list all data to be generated and clearly determine the utilization rights to each of such data or where part of the data is not covered by the list above. With respect to those data for which the utilization rights have not been clearly agreed, it is not necessarily desirable in some cases to permit the parties who can practically access the data to freely utilize the data. In preparation for such cases, it is also reasonable to grant the utilization rights to either party or establish a basket clause to the effect that the utilization rights would be determined upon consultation among the parties.

(ii) Granularity of data

In connection with the scope of applicable data, it is conceivable to roughen the granularity of or limit the scope and contents of the data to be generated in order to decrease possible leaks of trade secrets or know-how from the data. In addition, in the case where the applicable data relates to an individual, it is also conceivable not to collect part of the information intentionally in order to prevent the data from falling under personal information and from infringing the privacy rights of such individual.

For example, various data regarding vehicle travel include location and other information of the vehicle, and in the case where an individual driver can be identified from the various data so acquired (including the case where it is easily possible to cross-reference against other information and thereby identify the individual driver), such data would fall under personal information of the individual driver. In other words, even if the data itself is not linked to information that can identify a specific individual, such as the driver’s name, if it is possible to identify the individual driver based on the vehicle location information itself or other information that can be easily cross-referenced, then the travel data would fall under personal information of the individual driver. On the other hand, by deleting location information for a certain interval of time at the start and arrival of the travel respectively and acquiring location information only for the time when the vehicle travels highway roads to make it impossible to identify the individual driver or by otherwise processing the data to make it anonymously processed information under the Act on Protection of Personal Information, it would be possible to provide the data to a third party under a more moderate discipline than in the case of handling personal information.

However, processing, etc. of data may affect the usability of the data, so the parties are required to make a well-balanced examination based on the perspectives of both data utilization and data protection.
(3) Establishment of purpose of utilization

It is a condition that restricts any utilization of data beyond the scope of the purpose of utilization established. The establishment of the purpose of utilization concerns the whole business model of data generation, and it is desirable to make an evaluation from aspects of both promoting the utilization and necessity of keeping information confidential based on the basic viewpoints described in I through III above. From the perspective of necessity of keeping data confidential, it is advisable to make efforts to clarify the purpose of utilization assuming specific risks, such as prohibiting the utilization of data for any business which competes with the business of either party. On the other hand, from the perspective of promoting the data utilization, it is necessary to avoid interfering with such business by providing excessively detailed information.

For example, the “purpose of utilization” can be established as (i) the development of know-how and tools regarding the method of utilization of machine tools and the provision of services to B1 in Case 1, (ii) the implementation of healthcare management of employees and planning of improvement measures of working environment in Case 2, and (iii) the generation of weather forecasts based on the collected data in Case 3.

(4) Processing, etc. and utilization rights to derived data

(i) Restriction on method of processing, etc.

Generated data would often be subject to some kind of processing, etc. and used for business. With respect to the method of the processing, etc., advanced processing based on the knowledge of statistics, etc. might be applied, and it might be able to bring out great value from the existing data by using a newly developed method. As such, it is reasonable to promote the development of new analysis methods, so it is desirable not to restrict analysis method in the contract. However, for the purpose of preventing data from being utilized in a manner that is not expected by the parties, it is also possible to permit processing, etc. of data by a certain method. In particular, with respect to any personal information, since it is conceivable to make the information into anonymously processed information and provide it to a third party without obtaining the principal’s consent, the parties may establish the matters to be noted in the case of preparing anonymously processed information depending on the nature of the information.

(ii) Establishment of utilization rights to derived data

Any derived data acquired from such processing, etc. can be considered to be newly developed data itself. Accordingly, it is necessary to make an agreement among the parties as to the utilization rights to the derived data and the intellectual property rights regarding the derived data separately from the allocation of the utilization rights to the raw data, which existed before such derived data was created.

The specific details to be established for derived data are the same as those for raw data, and the matters that need to be determined for each derived data are: the method of processing, etc. and the utilization rights to the data derived thereby; the purpose of utilization and other scope of utilization; granularity of data; restriction of third party utilization; distribution of profits; costs and expenses to be borne by the parties; period and regions of utilization; and handling of data upon termination of contract.
V “Data Generation Type” Contracts

The utilization rights to derived data would be determined based on considerations such as (i) the contribution of each party to the generation of raw data subject to the analysis (costs borne by the parties, ownership of the tools, and which party took the initiative in planning the installation method of sensors, etc. and in monitoring for the continuous data generation), (ii) efforts made in the data processing, etc. and importance of necessary technical knowledge, and (iii) risks incurred by the parties due to utilization of derived data and other factors.

For example, in Case 1, the decisions may be made based on the following factors.

<table>
<thead>
<tr>
<th>Contribution of the parties</th>
<th>Machine tool manufacturer A</th>
<th>Data analysis and processing</th>
<th>Customers (user of the machine tools) B1</th>
</tr>
</thead>
<tbody>
<tr>
<td>· Plans the installation method of sensors</td>
<td>· Customer B1 owns and uses the machine tools, and the data would be generated only after Customer B1 uses the machine tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Implements the monitoring for continuous generation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data analysis and processing</th>
<th>· The selection of data analysis method and implementation of the analysis will be undertaken by Manufacturer A, which has expertise in those areas.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks</td>
<td>· Leaks of trade secrets and know-how regarding the manufacturing method</td>
</tr>
<tr>
<td>· Leaks of information regarding the manufacturing situation of the product</td>
<td></td>
</tr>
</tbody>
</table>

| Arrangements | The results of analysis can be used for the service provision to Customer B1 and research and development of new product of Manufacturer A but not for the purpose of providing best practices to any competitor of Customer B1. |

(5) Restriction of license, etc. to a third party

(i) Matters to be considered with respect to license, etc. to a third party

With respect to assignment or license to a third party or joint utilization (cross license, etc.) with a third party of applicable data and derived data, as it is often the case that, unlike utilization by the party itself, the other party expresses disapproval, it is desirable to make clear agreement in advance.

Among other things, permission of utilization, etc. to competitors is assumed to cause significant opposition. On the other hand, the other party might not overly express opposition
V “Data Generation Type” Contracts

to or interest in the permission of utilization, etc. to any person other than competitors, so there is good chance that the parties will be able to establish the available scope of permission of utilization, etc. to a third party without giving rise to any complaints from either party.

The basic idea is to weigh the advantages to be obtained and the disadvantages to be incurred by the parties by permitting a third party to utilize data. The specific matters to be considered are assumed to be as follows.

- Nature of the data (whether it is possible to conjecture any trade secret or know-how from the data, whether the data infringes privacy rights of any individual, etc.)
- Method taken to prevent leaks of trade secrets and know-how, etc. (delete any information that would identify the factory, handle the data as statistic information of all tools of the same type, etc.)
- Whether or not the third party to which the data is provided is a competitor
- What kind of restriction should be imposed on the utilization by the third party to which the data is provided (provided that it is necessary to make careful judgment on whether effectiveness can be ensured)
- Amount of consideration and distribution method of profits

(ii) Provision of analysis results of applicable data and derived data to a third party (“reapplication for other client/project”)

In relation to data generation contracts, there are some cases where the parties provide know-how acquired from the processing, etc. of applicable data and derived data to a third party through consultation services or other means.

For example, in Case 2, this applies to the case where Company B, which engages in healthcare services, considers processing the vital data acquired from the business described in Case 2 to utilize them for other healthcare management service. In addition, it is also conceivable that the machine tool manufacturer might create a database for analysis through processing, etc. of the applicable data acquired from multiple manufacturing companies, and prepare trained models for optimal utilization of machines and predictive analysis of malfunctions to utilize them as consultation services for new customers and third parties.

While any such reapplication of services for other client/project can enjoy benefits from original applicable data and derived data, it is difficult to make a quantitative evaluation of the degree of contribution of the applicable data and derived data to the economic profits obtained by the provider of the reapplied services as a whole. Therefore, it is considered difficult to apply distribution of profits to those services in many cases.

In such cases, if the service provider (in Case 2, Company B) develops a system for generation and processing, etc. of data (in Case 2, a system for acquiring and monitoring the vital data), the conceivable approach includes discounting the expenses required for the development of the system or providing the consultation services based on the applicable data and derived data (planning and giving advice of company-wide healthcare management measures) from the service provider (in Case 2, Company B) to the other party (in Case 2, Company A) with discount. In addition, it is also possible to take an approach that allows a company to utilize applicable data and derived data acquired from other business operators for its own business in return for permitting their applicable data and derived data to be utilized for any service.
provided to other business operators. For example, in Case 1, the data acquired from the machine tools of Customer B2 may be utilized for the service provided to Customer B1 on the condition that Customer B1 permits Company A to utilize the data acquired from its machine tools for the service provided to Customer B2 (provided that Company A has also executed the similar contract with Party B2). The parties are required to choose a suitable method for each case.

(6) Warranty/no warranty over contents and continuous generation of data
When applicable data and derived data come into use for other economic activities, any inaccuracy in data or failure of continuous generation of data might cause damage. Accordingly, it is advisable that the parties clarify the responsibilities for the details and continuous generation of data in advance.

For example, in the case where vehicle behavior information, etc. is collected through onboard communication devices of vehicles, it is possible that any figure data that is different from the actual vehicle behavior may be sent to a data center due to network problems or other causes and that the utilization of such inaccurate data causes damage. Therefore, it is desirable to set forth whether the accuracy of data, etc. is warranted or not in advance.

In Case 1, Customer B1 might not operate the machine tools depending on the production situation for each season and therefore the operation data might not be acquired on a continuous basis. In such case, since the data cannot be generated on a continuous basis due to the production situation, which is a reason that cannot be adjusted by Customer B1, it is often considered not reasonable to make Customer B1 responsible for the continuous generation of data and therefore Customer B1 would not be made responsible, etc.

On the other hand, in Case 2, as the vital data provided from Company A can be considered to fall under personal information, it is conceivable that the contract would include a provision requiring Company A to warrant to Company B that Company A has obtained the principal’s consent for the handling of the vital data to be provided.

In addition, in Case 3, it is considered reasonable that Business Operator A warrants to Company B that Business Operator A has been licensed by Subcontracting Company C1 and other companies to acquire and utilize data.

(7) Distribution of profits
In data generation type contracts, there are cases where it is planned to gain profits by not only utilizing the data by the parties themselves but also by providing such data to a third party, etc. Such profit model is considered to take various forms, including the following models.

- Receive license fee by granting license, etc. of the applicable data itself to a third party
- Create analysis models using the applicable data and provide ASP (Application Service Provider) services developed based on such analysis models to a third party

In addition, the conceivable calculation methods for the distribution of profits include fixed-charge method, usage-based rate method and sales distribution method. It is not possible to simply compare the relative merits of these methods, and it should be selected based on the individual situation.
V  “Data Generation Type” Contracts

For example, in Case 1, if Company A delivers the same type of machine tools to a considerable number of factories and the analysis data to be assigned or licensed to a third party have been acquired by statistically processing the operation data of such considerable number of factories, and therefore the degree of contribution of the operation data of Customer B1’s factory itself is small and the risk of the leaks of trade secrets and know-how of Customer B1’s factory is also low, it is conceivable that the method of reducing the sales price of the machine tools sold by Company A to Customer B1, instead of Company A paying to Customer B1 the consideration based on the amount of data sold, would be adopted.

In Case 3, the possible methods of distributing the sales obtained by selling the weather forecast information include (i) the method of distributing the amount between Business Operator A and Company B based on the sales; (ii) the method of paying fixed charge from Business Operator A to Company B; and (iii) the method which combines (i) and (ii) above. In the case of the method of only paying fixed charges from Business Operator A to Company B, Business Operator A would bear both risks and returns of the business, and in the case of distributing the sales, Business Operator A and Company B would share risks and returns.

In addition, it is also conceivable that, on the condition that one party (Party X) permits the utilization rights to applicable data and derived data to the other party (Party Y), Party Y provides any derived products (including consulting services) created based on such data to Party X. It is possible to adopt a method that gives rise to differences in the contents of service. For example, a company provides those factories which have accepted to provide their data for the company’s services with consulting services using machines which utilize the analysis data of the factories which have also accepted to provide their data.

(8) Costs and losses to be borne by parties

In distributing the data utilization rights, it is possible that the parties determine the expenses to be allotted taking into account the amount of costs borne by each party. Contrary to such example, it is also possible that the parties consider the costs to be borne when determining the distribution of profits.

As an issue of contract in general, in the case where unexpectedly high costs arise after commencing a business jointly conducted by multiple business operators, a dispute would often arise among the parties because they had not clearly determined the distribution of costs in advance. Accordingly, it is desirable, in terms of preventing any dispute from arising, to clarify in advance the details of agreements in the contract with respect to the items for which the cost increase is concerned upon discussion among the parties. As it is obviously not practicable to clarify all concerns in advance, it might be necessary in some cases to take measures such as predetermining the conduct of review of the details of the agreements or stipulating that any party may make an offer for the review to the other party at the time when the business has progressed to a certain extent.

(9) Management method and security

---

24 Similarly, Business Operator A also needs to consider distributing profits with Subcontracting Company C.
It might be necessary to store applicable data and derived data for a certain period of time considering their economic value. Therefore, it is required to determine a method for safe and effective management of data with an adequate cost. However, as the balance of the safety and effectiveness differs depending on the nature, risks, and other factors of the data, it is desirable to make an agreement among the parties as to the specific management method from security and other aspects.

In particular, it should be noted that there are regulations concerning data storage destinations for some types of data or in some countries. Such regulations are often discussed as restrictions on cross-border transfer of personal information and data localization regulations (see “Data localization and restrictions on cross-border transfer” in IV-2-(5)-(i) above for the details of each country). Although the restrictions on cross-border transfer had tended to receive attention before, the data localization regulations, among others, are well-known from the Cybersecurity Law in China and regulatory law in Russia, and the number of countries which have data localization regulations are increasing throughout the world. Therefore, the parties must be careful when implementing data generation in an international framework. While a lot of EU countries also have such regulations, EU aims for free data distribution within EU and is currently progressing toward abolishment of such data localization by each country.

In addition, in the case where the management of applicable data and derived data is delegated to a third party, it is necessary to select an adequate delegator and execute a contract with the delegator under which the implementation of an appropriate management method can be secured. Above all, in relation to the assignment of responsibilities, it is required to clarify in advance which party should be responsible for information leaks or any other issues arising at the delegator.

Moreover, in the case where data contains any personal information, especially EU-derived personal data, since the EU General Data Protection Regulation (GDPR) sets forth matters to be stipulated by contract (Article 28(3) of the GDPR), imposes certain restrictions on transfer outside EEA (European Economic Area) and establishes other strict regulations, the parties need to proceed cautiously, including requesting reviews by professionals.

(10) Period and regions of utilization

Upon distributing the utilization rights to applicable data and derived data, the period and region in which the data can be utilized should be stipulated. If the period in which the data can be utilized is not clarified in advance in the contract, it is possible that the data would be considered to remain available as long as the effective period of the contract continues, thereby making the available period unclear, which is not desirable from the perspective of clarifying rights and authorities. In addition, in the situation where applicable data and derived data may be utilized online or abroad, a dispute might arise in the future if the parties fail to specify in advance the regions where the data can be utilized, and therefore it is advisable to stipulate such available regions.

(11) Handling of data upon termination of contract

While it is possible either that data is required to be destroyed or deleted after the termination of contract, or the parties continue to hold utilization rights after the termination of contract, it is not necessarily unreasonable to prescribe different handling of data upon termination of contract depending on the type of data, such as requiring trade secrets, know-how, personal
V “Data Generation Type” Contracts

information, etc. to be destroyed or deleted but allowing the parties to continue to hold utilization rights to any other data after the termination. In such case where different handling of data upon termination of contract is established according to the type of data, it is necessary to clarify which data is to be handled in what manner.

In addition, if the destruction or deletion of data is to be required, the rules for destruction or deletion of data upon termination of contract should be stipulated. It is also desirable to provide for the preparation of evidence of the destruction or deletion (not only an evidence for destruction or deletion by the parties themselves but also a certificate, etc. of destruction or deletion by a professional or other third parties should be considered depending on the importance of the data) as necessary.

On the other hand, in the case where it is determined that each party would continue to hold the data utilization rights which such party had held until then after termination of the contract, if it is not clear whether the provisions regarding the management method of data would survive the termination of contract, it might become unclear whether the other party would continue to bear the same management obligations as those held during the term after the termination. Therefore, it is advisable to clarify whether such provisions would survive the termination of contract.

(12) Governing law and jurisdiction

Although it is considered that even worldwide there are not very many laws concerning the generation of data itself, the regulations that would apply when any personal information is involved in the process of data generation differ by country, so the parties should pay attention to the legal system of the applicable country.

See IV-2-(5)-(iii) and (iv) above regarding governing law and jurisdiction.

(13) Points to note when executing data generation type contracts with consumers

Article 10 of the Consumer Contract Act sets forth that, with respect to consumer contracts executed between consumer and business operator, any clause that restricts the rights or expands the duties of the consumer beyond the application of discretionary provisions in any laws and that unilaterally impairs the interests of the consumer, in violation of the principle of good faith, is void.

In addition, with respect to the provisions relating to damages in the case where a consumer incurs damage due to divulgence of data, etc., the following exemption clauses become void (Article 8(1) of the Consumer Contract Act):

· Clauses which completely exempt a business operator from liability to compensate a consumer for damages arising from default by the business operator;
· Clauses which partially exempt a business operator from liability for damages arising from default by the business operator (limited to default which arises due to an intentional act or gross negligence on the part of the business operator, the business operator’s representative, or employee);
· Clauses which completely exempt a business operator from liability for damages to a consumer which arise from a tort committed during the business operator’s performance of a consumer contract;
V “Data Generation Type” Contracts

- Clauses which partially exempt a business operator from liability for damages to a consumer arising from a tort (limited to cases in which the same arises due to an intentional act or gross negligence on the part of the business operator, the business operator's representative, or employee) committed during the business operator’s performance of a consumer contract.

Attention should be paid to such consumer protection framework when executing data generation type contract with consumer.

(14) Antimonopoly Act and Subcontractors Act

For example, there are cases where the production situation from upstream to downstream in the supply chain is monitored and shared in an effort to reduce idle resources in the whole supply chain and improve productivity. While such efforts are often considered to cause pro-competitive effects, in the case where the provision of data relating to the manufacturing process is demanded against a manufacturer, which is in the position of subcontractor, by a business operator, which is in the superior bargaining position, taking advantage of the position, and the scope of the data in question and allocation of utilization rights to such data are unreasonably detrimental to the manufacturer, it might fall under abuse of superior bargaining position under the Antimonopoly Act (Article 2(9)(v) of the Antimonopoly Act) or other similar provisions. In addition, if the Subcontract Act is applicable, it might fall under the prohibition of unjust demand for provision of economic interests (Article 4(2)(iii)).

As described above, the parties should pay careful attention as to whether there might be any problem from the competitive perspective when executing a data generation type contract.

3 Method of determining appropriate data generation type contracts

With respect to data generation type contracts, it is desirable to consider setting forth the following items in the contract. For specific examples of the provisions of data generation type contracts, please see the draft model contract for data provision type contracts in VII.

(1) Definitions of data and other terms
   - Definition of applicable data
   - Definition of forms of processing and definition of derived data

(2) Allocation of data utilization rights
   - Specific details of utilization rights
   - Method of determining utilization rights to applicable data not individually provided for in the contract

(3) Provisions regarding forms of processing of data and allocation of utilization rights to derived data
   - Provisions regarding forms of process of applicable data
   - Allocation of utilization rights to derived data
V “Data Generation Type” Contracts

(4) Warranty/no warranty relating to data
- Warranty/no warranty regarding non-infringement of rights of a third party relating to data for which the other party holds utilization rights under data generation type contract (the data accessible by the counterparty)
- Warranty/no warranty regarding accuracy and completeness of the data accessible by the counterparty
- Warranty/no warranty regarding safety of the data accessible by the counterparty (whether or not the data accessible by the counterparty is infected, etc.)
- Warranty/no warranty regarding effectiveness of the data accessible by the counterparty and its compatibility to the purpose
- Warranty/no warranty regarding non-infringement of intellectual property rights of a third party relating to the data accessible by the counterparty
- Warranty/no warranty regarding implementation of proceedings under the Act on Protection of Personal Information relating to generation, acquisition, provision, etc. of the applicable data

(5) Distribution of profits and costs
- Consideration for allocation of utilization rights
- Method of distribution of profits
- Method of distribution of costs

(6) Measures to be taken when utilization is restricted by rights of a third party
- Cooperation when it is found out that utilization by the other party might be restricted

(7) Management of data
- Separate management of the data accessible by the counterparty from other information
- Duty of care of a good manager relating to the data management of the data accessible by the counterparty
- Request for report or rectification relating to the management status of the data accessible by the counterparty

(8) Confidentiality
- Definition of confidential information
- Details and exceptions of obligation of confidentiality
- Survival of obligation of confidentiality after termination of the contract and the effective period thereof
V “Data Generation Type” Contracts

(9) Change to scope of applicable data
   □ Proceedings to change applicable data

(10) Effective period
   □ Effective period of the contract
   □ Automatic renewal of the contract

(11) Force majeure
   □ (In addition to standard force majeure events,) whether or not power failure, malfunction of communication facilities or suspension of provision or emergency maintenance of cloud services or other outsourcing services fall under a force majeure event

(12) Termination
   (Standard provisions regarding termination should be sufficient)

(13) Handling of data upon termination of contract
   □ Whether destruction or deletion of data is required after termination of contract
   □ In the case that destruction or deletion is required, whether the submission of a certificate of destruction or deletion is required

(14) Elimination of antisocial forces
   (Standard provisions regarding elimination of antisocial forces should be sufficient)

(15) Survival

(16) Prohibition of assignment of rights and obligations
   (Standard provisions regarding prohibition of assignment of rights and obligations should be sufficient)

(17) Entire agreement
   (Standard provisions regarding entire agreement should be sufficient)

(18) Governing law
   □ Which country or state, etc.’s laws to choose as the governing law.
V  “Data Generation Type” Contracts

(19) Dispute resolution

- Whether to choose trial or arbitration as the agreed jurisdiction
- Which place to choose as the forum for trial or arbitration

(Reference) Data Catalogue

- Sample in the case where the manufacturer installs sensor in the machine and acquire data

<table>
<thead>
<tr>
<th></th>
<th>Product or machine name/product or machine ID</th>
<th>Sensor ID</th>
<th>Place of operation</th>
<th>Data items</th>
<th>Data aggregation period</th>
<th>Form of data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[TBD]</td>
<td>[TBD]</td>
<td>[TBD] factory</td>
<td>[TBD]</td>
<td>[TBD] 2018 to [TBD] 2018</td>
<td>[TBD] form</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VI “Data Sharing Type” Contracts

VI “Data Sharing Type (Platform Type)” Contracts (Data Sharing Using Platforms) (Handling of Data Generated With Participation of Multiple Parties)

1 Structure
(1) Introduction

This Part VI describes the type of contract which aims to share data using platforms (“data sharing type” or “platform type”).

Against the backdrop of the recent situation where it has become possible to collect and analyze large quantities of data due to rapid development of IoT (Internet of Things), big data, AI (artificial intelligence), robotic sensors and other technologies, which is also called the fourth industrial revolution, there has been an increased recognition of the importance of the active collection and application of data that is distributed or lying dormant in various locations. While the entire economic, industrial and social system is undergoing these major changes, the necessity to create and develop platforms that go beyond the existing boundaries of companies and affiliates has been pointed out as a strategy for Japan to survive the fourth industrial revolution especially with respect to “real data”—such as health information, driving data, and operation data of factory facilities—which is one of Japan’s strengths.25

In such tide of the times, the number of cases where initiatives are being made for data sharing and application utilizing platforms is increasing in Japanese industry. For example, initiatives are being considered such as an initiative in which multiple ship builders, ship owners, operating companies, etc. aggregate individually held ship data and hydrographic phenomenon data into a platform for sharing, and an initiative in which multiple video camera installation business operators aggregate individually held video data into a platform to apply them for public purposes such as commercial use and urban planning and disaster prevention.

Although the details of such platform-type initiatives vary depending on the purpose of the initiative and the nature of the applicable data, this Part VI mainly assumes the following type of initiative:
- multiple business operators which belong to different company groups provide data to a platform,
- the platform aggregates, stores, processes or analyzes such data, and
- the multiple business operators share or apply such data through the platform.

The following terms used in this Part VI have the respective meanings set forth below.

| “Platform” | Although the meaning of the term platform may greatly vary depending on the case in which the term is used, in these Guidelines (Data Section), it is used as “a place or base which aggregates and stores large quantities of data provided by multiple business |

---


### VI “Data Sharing Type” Contracts

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Platform operator,” “platform business”</td>
<td>“Platform operator” means a business operator who operates a platform, and a business conducted by a platform operator through the platform is referred to as “platform business.”</td>
</tr>
<tr>
<td>“Data provider,” “provided data”</td>
<td>“Data provider” means a party who provides data to a platform in accordance with the terms of use established in advance by a platform operator or an individual contract with a platform operator, and such data provided by the data provider into the platform is referred to as “provided data.” Provided data may include raw data as well as processed data acquired from certain processing, etc. of raw data by the data provider. In addition, depending on the business field in which the platform is used, not only industrial data but also personal information or other person related data may be included.</td>
</tr>
<tr>
<td>“Data user,” “utilized data,” “utilized service”</td>
<td>“Data user” means a party who shares or applies data provided by a platform or utilizes services provided by a platform in accordance with the terms of use established in advance by a platform operator or an individual contract with a platform operator. The data shared or applied by the data user through the platform is referred to as “utilized data,” and utilized data may include provided data provided by data provider to the platform as well as data acquired from processing or analysis of such provided data by the platform. In addition, any service provided by the platform based on the results of the processing and analysis of the provided data (including solutions newly generated, etc.) is referred to as a “utilized service.”</td>
</tr>
<tr>
<td>“Participants”</td>
<td>Business operators who participate in the platform business (including data providers)</td>
</tr>
</tbody>
</table>

---

26 Although online market places, social network systems (SNS), etc. are also sometimes called “matching type” and “media type” platforms respectively, these Guidelines (Data Section) do not cover such platforms used in B to C or C to C transactions.
VI  “Data Sharing Type” Contracts

and data users) are collectively referred to as “participants.”

(2)  Structure and subject

(i)  Basic structure and subject

As described above, the basic structure of the platform type covered by this Part VI is assumed to have a platform, which aggregates, stores, processes or analyzes data, at the center, surrounded by a group of data providers, who provide data to the platform (X1, X2, X3…), and a group of data users, who share and apply data through the platform (Y1, Y2, Y3…). The image of this structure can be shown as Diagram 7 below.

![Diagram 7: Platform type (basic structure)](image)

While it is considered that the parties comprising the data providers group and the parties comprising the data users group often overlap in actual cases (in Diagram 7 above, each of X1 and Y1, X2 and Y2 and X3 and Y3 are the same entity), it is also possible that, besides the case where the parties in each group are completely identical, the parties in each group might not be completely identical and there might be parties who only provide data or who only utilize data. For example, when secondary data acquired by processing or analyzing primary data collected by the platform is made available to third party other than the data providers group, the parties who are not data providers become data users and therefore the members of each group would not be the same. This Part VI also regards such cases where there are parties who only provide data or who only utilize data as the platform type.

Platforms are expected to aggregate and store provided data and provide the provided data as primary data, which is the original provided data, or as secondary data, which is acquired from certain processing or analysis of the provided data, and, moreover, to develop or generate utilized services based on the results of the processing or analysis of the provided data to provide such services (see Part VI-2-(1) below).

Platform operators are not required to perform the above process from aggregating data to providing utilized services all by themselves, and any third party other than the platform operators may perform all or part of the process. Such third party can be a person who...
VI  “Data Sharing Type” Contracts

processes or analyzes data (A and B in Diagram 8) or a person who develops utilized services or other services (C in Diagram 8) as delegated by the platform or data users, or a person who processes or analyzes, or develops solutions or other utilized services based on, the utilized data provided from the platform and provides the results to data users (D and E in Diagram 8) (see Diagram 8).

In the aim of developing new utilized services or creating business opportunities through platforms, it is conceivable to build and expand the network (ecosystem) centered on platforms, such as by making business operators other than data providers or data users actively participate in the platform business as above and also collaborating with other platforms.27

Diagram 8: Platform type (in the case that a third party performs processing, analysis, etc.)

(ii) Difference from cloud service type

As something similar to the platform type, another conceivable initiative is one in which data provided by certain data providers or the results of processing or analysis of such data are utilized only by such data providers (or their group companies) and not shared with any participant other than such data providers as data users (see Diagram 9 below).

---

27 See Part VI-3-(4)-(ii) for the collaboration with other platforms.
VI “Data Sharing Type” Contracts

Such initiative might be similar in nature to the platform type covered by these Guidelines (Data Section) if the data or the results of processing or analysis of the data would be shared within the company group of the data provider (for example, in the case where Z1 in Diagram 9 above is not a single company but is a company group). However, as there is no sharing or application of information beyond the existing boundaries of the company group, it is rather more similar in nature to the traditional cloud services in which a cloud service operator provides application services to each customer business operator through the network.

As long as the cloud service operator adopts a system to perform adequate separate management of data of each customer business operator, it may be regarded as a bundle of one-to-one data provision type transactions between the cloud service operator and each customer business operator (Z1 to Z3). Therefore, as it seems that many items considered in Part IV (“Data Provision Type” Contracts) above are applicable, these Guidelines (Data Section) basically do not take the cloud service type as platform type.

(iii) Difference from data market place type

There is also a platform called data market place type (or market place type) which aims to match business operators who wish to earn consideration by providing their data to third parties and business operators who wish to utilize third party data. In this type, the parties who provide data and parties who utilize data are usually not the same, and it is different from the platform type in that it does not have data sharing as its main purpose, and it may be regarded as a bundle of one-to-one or one-to-n data provision type transactions between data providers and the platform and between the platform and data users respectively. Therefore, these Guidelines (Data Section) basically do not include the data market place type as a platform type.

(iv) Difference from joint utilization of data (cross license) type

As an initiative to share data among multiple business operators, there is a joint utilization of data (cross license) type which falls under the type of “data provision type” contracts described
VI  “Data Sharing Type” Contracts

in Part IV-1-(2)-(iii). However, the joint utilization of data type differs in structure from the platform type in that there is no party equivalent to the platform operator and that data is assumed to be directly exchanged among business operators in this type. Therefore, the difference between the two types of transactions is that while there is usually no direct contractual relationship between data providers and data users in the platform type, there is a direct contractual relationship between each business operator in the joint utilization of data type (see Part VI-1-(3) below).

While it is also conceivable to adopt the joint utilization of data type when data is shared between two parties or among multiple parties, it is considered that the platform type would often make it possible to design the scope of utilized data or utilized services, determination of participants, and other matters in a more flexible and diverse manner when data is shared among more than a certain number of business operators.

(3)  Legal relationship between parties

As shown in Diagram 7 above, the platform type centers on a platform with data providers and data users surrounding it. Therefore, with respect to contractual relationships, there is usually considered to be the contractual relationship between each data provider and the platform operator and that between each data user and the platform operator respectively, and no direct contractual relationship between each data provider and each data user nor between each of the data providers or each of the data users in the platform type.

Accordingly, in the case where a data user breaches the contract (often in the form of the terms of use) with a platform operator, for example, only the platform operator may directly pursue such breach of contract, and data providers and other participants have no means to pursue the liability other than practically demanding the platform operator to pursue the breach of contract, unless otherwise agreed by the parties. Therefore, platforms have major roles to play, and platform operators are required to have neutrality and creditworthiness (see Part VI-3-(5)-(i) below) and to monitor whether the participants comply with the contract (see Part VI-4-(4)).

(4)  Structure of data provision and utilization, etc.

(i)  Data provision and collection

There can be various methods for data providers to provide data to a platform, such as (i) the method in which the data held by the data provider is provided as raw data in the original form or as processed data acquired from certain processing or analysis of the raw data and (ii) the method in which data is collected in the platform on a real-time basis through a sensor installed in the manufacturing facilities, vehicles, etc. or any other data collecting equipment. When focusing on the provision or collection of data, the case of (i) is the same as or similar to the case of Part IV (“Data Provision Type” Contracts) above, and the case of (ii) is the same as or similar to the case of Part V (“Data Generation Type” Contract) above, and the matters examined in each part are basically considered to be applicable in each case. However, as the scope of utilization, etc. available after the data have been provided or collected is different in the platform type, there are matters to be noted from the perspectives specific to the platform type (see Part VI-2 (“Main issues to be considered for platform type”) and Part VI-3 (“Main legal issues relating to platform type contract”) below.

60
VI “Data Sharing Type” Contracts

In addition, the data to be collected by the platform are not limited to those provided from the data provider, and there can be cases where the platform obtains information from any third party vendor providing data or receives public data from public agencies.

(ii) Data storage, processing and analysis

When a platform is provided with data from each data provider, it is assumed to aggregate and store the provided data and then process or analyze or organize the provided data to facilitate the utilization thereof. For example, conceivable arrangements to be taken by the platform operator include: (i) unification of the format of the data; (ii) if any personal information or other person related data is incidentally included, deletion of such data or creation of anonymously processed information as prescribed under the Act on Protection of Personal Information; (iii) creation of statistic information; and (iv) generalization of the data so that the data provider cannot be identified.

Moreover, it is often necessary to conduct a certain amount of analysis in order to maximize the data value, and the practical realization of analytical technology using AI (artificial intelligence) has been especially progressing in recent years.  

(iii) Data sharing and application

There are also various conceivable methods for data users to share or apply utilized data provided by a platform. For example, there can be a method in which the utilized data is accessed or acquired directly from the database of the platform through an API, or a method in which the results of analysis of the data is made available to the data users through certain application programs. In addition, as a form of data application, it is possible that a platform operator provides the provided data accumulated in the platform or the data processed or analyzed in the platform to a third party.

Moreover, it is also conceivable to adopt a system to provide utilized services to data users together with, or instead of, utilized data, or to generate new business opportunities. The necessity of development of services by manufacturers has been recognized recently, and it can be argued that platforms may function not only as a base for data sharing or applications but also as a system to achieve the development of services by manufacturers.

2. Main issues to be considered for platform type

---

28 See Part III-1-(3)-(ii) above for person related data.

29 See Part V-3-(4) of these Guidelines (AI Section) for rights and authorities and terms and conditions of utilization relating to each data and derivative products generated in the course of utilizing AI technology.

30 API (Application Programming Interface) means an interface that enables a program to make its functions available from other programs.

31 See the descriptions in Part IV relating to the data provision type for the matters to be noted with respect to the contracts relating to the data provision between platform operator and third party.
VI “Data Sharing Type” Contracts

The main characteristics of the platform type that are different from those of “data provision type” and “data generation type” are as follows, and it is considered useful to have recognition of such characteristics when considering whether to adopt the platform type.

- There exists a platform, and data of multiple business operators are aggregated in the platform
- Data provided by data providers are assumed to be provided to or shared with third parties
- It is possible that one business operator participates in the platform as both data provider and data user
- The details, scope and other matters of the provided data and utilized data can be flexibly adjusted or controlled in the platform
- A number of various parties, including multiple data providers and data users and other participants, may participate in the platform

As the details of the platform type may vary greatly based on various factors such as the purpose of utilization of the platform, related business fields, scope of participants, details and scope of provided data and scope of utilization of utilized data, it is necessary to consider the platform system on a tailor-made basis according to the individual situation. The following descriptions are the main matters that are considered to be generally required to be considered when adopting the platform type.

(1) Purpose and method of data application

First, it is necessary to consider whether or not the purpose of data application is suitable for the platform type. In particular, among various methods of data application, when considering the data sharing among multiple business operators in different company groups, the platform type can be adopted.

The conceivable purposes of sharing data among multiple business operators utilizing a platform are, for example, to improve the operating rate of the factories of each business operator by sharing the results of analysis based on the operation data, etc. of various facilities and machines acquired from manufacturing facilities, etc. of the factories of multiple business operators, to improve efficiency of the entire inventory and transportation network by sharing data in the whole supply chain of manufacturers, logistics operators, retail operators, etc., and for other purposes of improving efficiency, etc. of the existing business process through data sharing and joint utilization of the results of data analysis.

In addition to the above, it is considered important, as a strategy for Japan to survive the fourth industrial revolution, to develop or generate new solutions or other services that had not existed before based on the results of data analysis and to promote innovation.

The necessity of data sharing and application by multiple business operators beyond the existing boundaries of companies and affiliates has been recognized in order to achieve the above purposes, and the platform type can be considered suitable for data applications which aim to improve efficiency of the existing business processes and promote innovation by sharing or applying data beyond the existing framework as described above.

As a number of participants would be involved in the platform type, it is useful to make the purpose of the platform business as clear as possible and specify them in the terms of use, etc. as necessary to establish common understanding among the participants as well as to promote
their active participation in the platform business. In particular, as described in VI-2-(8)-(i) below, in terms of encouraging data providers to provide their data, it is desirable to have a purpose that can explain, and does not conflict with, the significance and advantages for the data providers to provide their data.

(2) Number of data providers and scope of participants

(i) Number of data providers

While the purpose of adopting the platform type is to share or apply data among multiple business operators as described in Part VI-2-(1) above, adopting the platform type would make it necessary to select a platform operator and to establish rules for operating the platform, and costs would also be incurred for operating the platform, so if the number of parties involved in the data sharing or application is small, it is generally considered more appropriate to adopt the joint utilization of data type (cross license) described in Part IV-1-(2)-(iii), which does not use a platform. On the other hand, if the number of parties involved in data sharing or application is large (including the case where there are only several participants at the beginning but it is anticipated that a large number of business operators would share data in the future), the platform type can be adopted.

The decision of how to set the scope of data providers depends greatly on the purpose of data sharing or application utilizing platform. It may be advisable to set the scope of data providers as wide as possible in terms of collecting data as much as possible. However, in the case of the platform type covered by these Guidelines (Data Section), data providers often become data users and the necessity of adjustments to the interests among participants increases as the number of participants increases as described in Part VI-2-(3) below, so it is important to take such matters into consideration when examining the scope of data providers required to achieve the purpose.

(ii) Scope of participants (how open the platform should be)

In addition to the platforms which limit the platform participants to certain business operators by strictly setting the requirements for participation in the platform as data provider or data user (for example, the requirement to obtain approval from the platform or existing participants for new entry), there can be platforms which allow wide participation of third parties who wish to participate in the platform as long as they satisfy the conditions set forth in the terms of use (the latter platform is sometimes referred to as “open type platform”). Further, some open type platforms are open for both data providers and data users, and others are open only for either data providers or data users. For example, it is conceivable that a platform would be open only for data users when any versatile utilized data or utilized service can be generated based on the provided data. The fact that the data utilization can be flexibly designed by utilizing platforms as above can be considered as one of the characteristics of the platform type.

Although it might be more desirable to adopt open type platform in some cases from the perspective of promoting innovation through data sharing or application, there can be some cases where it is difficult or inappropriate to adopt an open type depending on the purpose of introducing the open type platform and the nature and details of the applicable data. It is also possible to limit the participants to certain business operators at the beginning and then gradually transfer to an open type platform.
(3) **Adjustment of interests between data providers and data users**

As a number of participants would be involved in the platform type, it is necessary to adjust the interests among the participants. It should be particularly noted that the interests may be greatly different between data providers and data users. In other words, since data is an important asset of each business operator for conducting business activities, data providers tend to be cautious about permitting any third party to access the data itself and, even if they permit the access, tend to wish to limit the scope of the access (the scope of the provided data, scope of the parties to which the data is provided, scope of the purpose of utilization, etc.). On the other hand, data users who utilize the utilized data or utilized services through the platform tend to wish to receive the provided data from the platform as much as possible and to access the utilized data without any limits.

In order to adjust such constructive difference in the interests between data providers and data users, it is required to appropriately set the types and scope of the applicable provided data (see Part VI-2-(4) below), the scope of utilization of data (see Part VI-2-(5) below) and other matters, and to design the scope of utilization relating to the provided data and the scope of utilization relating to the utilized data or utilized services to be interrelated (see Part IV-3-(2) below). In addition, the selection of a platform operator which comes in between data providers and data users would be also important (see Part VI-2-(6) below).

In adjusting the interests between data providers and data users, as data providers also often participate as data users in the platform type, it should be remembered that, if data providers permit other participants to share or apply their own data, their opportunities for sharing or applying data of other companies would increase and consequently it would be beneficial to all the participants.

(4) **Type and scope of applicable provided data**

(i) **Nature of data**

When considering the platform type, it is important to appropriately select the types and scope of the applicable provided data. As one of the perspectives, it is conceivable, for example, to separate data which might reduce the competitiveness of the company if disclosed to other business operators (especially to competitive business operators of the company) and data which would have no direct effect or have only a small effect on the competitiveness of the company even if disclosed to other business operators, and preferentially provide the latter as provided data (see Part VI-3-(3)-(i) below). This is useful from the perspectives of both reducing the psychological resistance of data providers who tend to be cautious about disclosing their own data to third party through platform as described in Part VI-2-(3) above and reducing...
the concerns for any issue to arise under the Antimonopoly Act when data is shared among competitive business operators (see Part VI-3-(4)-(i) below).

It is not necessarily possible to unambiguously decide which types of data fall under data that would have no direct effect or have only a small effect on the competitiveness of the company even if disclosed to other business operators, and it is considered that they are often decided based on the attribution of other business operators that utilize such data, the method of utilization of such data (whether it is utilized as raw data or upon processing or analysis, etc.) and the strategic decision-making of each business operator or the industry.

In addition, even the data that might reduce the competitiveness of the company if disclosed to other business operators (especially to competitive business operators of the company) may be shared or applied by utilizing platform. For example, even if the data might reduce the competitiveness of the company if disclosed to other competitive business operators in a certain industry, it is conceivable that the data might be able to be shared or applied among multiple business operators through the platform by limiting the data users of the data to business operator in completely different industries, or by not offering that data and instead only offering data that has been processed or analyzed for generalization to make it impossible to identify the data provider.33

(ii) Standpoint of “open”/“closed” data

As some data held by data providers possess value as a trade secret or know-how or great value for business by itself, it is important to examine from the open/close standpoint the question of which data, of all the internal data of the company, should be provided to the platform as provided data and which data should be intentionally retained within the company (see Part VI-3-(3)-(i) below).

Based on the purpose of the platform type to improve the efficiency, etc. of the existing business process through data sharing or application and consequently promote innovation such as generation of new solutions, it is not desirable that data providers excessively refrain from providing their data, and it is expected that an appropriate balance between data to be open and data to be closed would be procured upon taking into consideration the standpoints in Part VI-2-(4)-(i) above (Nature of data).

(iii) Exclusion of unnecessary data

In terms of increasing the platform value, it is generally desirable that data providers provide as much data of as many different types as possible. However, there are some data that might cause an increase in the management cost for operating the platform or restrictions on data utilization if unnecessarily collected. For example, in the case where any information relating to personal information or privacy rights is incidentally included in the provided data, it is necessary to carefully consider the handling of such information taking into consideration that such information must be handled in compliance with the regulations under the Act on

33 However, in the case where any data that might reduce the competitiveness of the company if disclosed to other business operators (especially competitive business operators of the company) are aggregated in the platform, it is deemed necessary to take adequate measures under the system and the terms of use to prevent the provided data from being disclosed to any competitive business operator of the data provider.
VI  “Data Sharing Type” Contracts

Protection of Personal Information and other related laws and ordinances (see Part VI-3-(3)-(vi) below).

From such perspectives, it is also important to consider if there are any data that should be specifically excluded from the provided data to be collected by the platform based on the nature and value of the data.

(5)  Scope of data utilization

The scope within which the platform operator, data users and other participants may utilize the provided data collected by the platform from data providers would not be automatically determined without agreement, but needs to be set forth in the contract between data providers and the platform operator (see Part III-1-(2) above for discussions on data ownership).  Such scope of data utilization would be considered from the standpoint of “who (the scope of data users)” may utilize “which data (the types and scope of utilized data)” “for what purpose (the purpose of data utilization)” and “by which method (the method of data utilization).”

See Part VI-3-(3)-(iii) for rights and authorities relating to derived data and other derivative products generated by the utilization of provided data by platform operator and utilization of utilized data and utilized services by data users.

(i)  Scope of data users

It is necessary to consider the scope of parties to which the data utilization would be permitted, in other words, the scope of data users.  While it is considered that data providers often become data users in general platforms, it is required to examine whether it is necessary to permit data utilization by any other parties.  In addition, it is also conceivable to set different scope of data users for each type of utilized data or utilized service.

(ii)  Types and scope of utilized data

If the platform type is adopted, the types and scopes of the provided data and utilized data can be set inconsistently, and it is possible to adjust the interests between data providers and data users by requesting the data providers to provide as much provided data as possible to the platform and setting the types and scope of data that may be utilized by each data user in a flexible and fine-tuned manner based on the nature and details of the provided data, attribution of the data users and other factors.

(iii)  Purpose and method of data utilization

It is considered that the issue of how specific the purpose and method of utilization of the provided data by the platform operator and the purpose and method of utilization of the utilized data or utilized services by the data users should be determined varies by the purpose of utilization of the platform, etc.  In light of the fact that data providers tend to be cautious about disclosing their own data to third parties through platforms as described above, it might offer a sense of safety to the data providers and consequently encourage data provision if the purpose of utilization and method of utilization are clarified for the provided data and utilized data and
VI “Data Sharing Type” Contracts

utilized services respectively (see Part VI-3-(2) below for the matters to be noted when stipulating the purpose of data utilization in the terms of use).

(6) Selection of platform operator

From the viewpoint of establishing a system which enables as many participants as possible to be involved with a sense of security and from the necessity of adjusting the interests between data providers and data users as described in Part VI-2-(3) (“Adjustment of interests between data providers and data users”) above, there can be cases where it is desirable to procure the neutrality of the platform operator (especially in the case of open type platforms).

If it is required to procure neutrality, it is conceivable to take (i) a method in which any third party other than the participants becomes an operator of the platform or (ii) a method in which all or part of the participants become joint platform operators, rather than a method in which one of the participants solely operates the platform. As to method (ii) above, possible methods include the participants jointly establishing a joint venture, partnership or general incorporated association (see Part VI-3-(5) below).

In either case, while the platform operator might not actively aim to gain profits in some cases from the perspective of procuring neutrality and in light of the purpose of adopting the platform type, etc., the appropriate operation of the platform requires expenses for system maintenance and other reasonable human resources and expenses, so it is often considered necessary to establish a mechanism for procuring revenue to maintain the stable operation of the platform.

(7) Necessity of terms of use

As it is assumed that a number of participants would be involved in the platform type, it is not practicable in terms of time and cost to individually negotiate and determine the contractual terms and conditions between data providers or data users and the platform operator, and it might cause operational problems if the terms and conditions greatly vary by participants. Accordingly, it is conceivable to prepare in advance the terms of use that sets forth the contractual terms and conditions which are commonly applicable, and the same terms of use would apply to the participants in the same position in principle (see Part VI-4 for the main clauses of the terms of use).

(8) Structure for promoting application of platforms

(i) Structure for promoting data provision

The platform type has a structure in which multiple business operators aggregate quantities of data into a platform, and the amount of data collected links directly to the value and competitiveness of the platform. Especially from the viewpoint of effective data application, as it is possible that data might be utilized by any method or for any purpose that had not been assumed at the time of provision, it is desirable that the platform is provided with as much data of as many different types as possible. In addition, an effect of enabling the platforms which could collect quantities of data to increase their utility value and thereby collect data from more participants (so-called, “network effects”) can be expected.

However, depending on the type and details of the data, it is often the case that the data is an important asset of each business operator for conducting business activities, and data providers
“Data Sharing Type” Contracts

tend to be cautious about permitting third parties to access the data (especially raw data or similar data) as described above and, even if permitting the third party access, wish to limit the scope of utilization. Therefore, it can be argued that the key factor of a successful platform business is whether the platform can offer incentives to data providers to provide as much data as possible so that the provided data may be shared or applied by as many methods and for as many purposes as possible. For example, it is conceivable to take measures such as making data providers who provide quantities of data able to receive the provision of utilized data or utilized services on better conditions.

In addition, from the perspective of data providers, the provided data would be stored outside the company framework in the platform type, so the data providers often have concerns about security issues (unauthorized access from outside, data divulgence, etc.). Therefore, also in terms of promoting data provision, it is advisable to establish a structure that eliminates such concerns as much as possible (see Part VI-3-(5)-(ii) below). It is assumed that such security issues would be addressed at the level of systems or technology to the extent possible at first, but there is a certain limit to such approaches. Accordingly, in order to complement those parts that could not be addressed at a systems level to a satisfactory extent for technical or cost reasons, it is possible to take measures such as clarifying the scope of data utilization in the terms of use, etc. of the platform, or imposing obligations relating to the safe management of data to the platform operator (see Part VI-3-(5)-(ii) and Part VI-4-(5)-(i)-a below).

(ii) Structure for promoting data sharing and utilization

Even if data are aggregated in the platform, the original purpose intended by the platform type cannot be fully achieved if such data are not effectively shared or applied. In addition, as described above, beyond the sharing of the provided data, the active development of new utilized services and generation of business opportunities, etc. are expected to be performed based on the results of processing or analysis of the provided data.

A conceivable system to promote data sharing and application is to delegate all or part of such development of new utilized services or generation of business opportunities, etc. based on the results of processing or analysis of the provided data to any third party other than the platform operator to make use of the knowledge and technologies of such third party and promote data application.

Regardless of whether to seek cooperation from such third party, it is important to grant appropriate incentives to the platform operator and such third party for data application by collecting or distributing appropriate consideration when data users utilize the utilized data and utilized services.

(9) Perspective of competition among platforms and internationalization

As the number of cases in which the platform type is adopted increases, disputes among platforms that handle data in the same or similar field might arise. The amount of data that a platform could collect links directly to the value and competitiveness of that platform, so taking into consideration the perspective of the network effects described in Part VI-2-(8)-(i), it is necessary for the platform to collect as much participants as possible to survive. In addition, it is also conceivable to increase the utility value of the platform by setting uniform standards regarding the provided data and facilitating the handling and application of data aggregated in the platform.
VI “Data Sharing Type” Contracts

Further, as cross-border distribution of data may be easily performed, such disputes among platforms tend to arise across borders rather than within the domestic markets. Therefore, it is considered desirable in some cases to monitor international trends on a continuous basis and consider whether to actively include overseas business operators in the platform participants depending on the field.

3 Main legal issues relating to platform type

(1) Necessity and type of terms of use

(i) Background to adoption of terms of use

The contracts to govern the participants in the platform type often take a form of terms of use, instead of individual contract. This is mainly because that there would be multiple contractual relationships due to the “n : 1 : n” structure centered on a platform and, as described in Part VI-2-(7) above, if there are different terms established in each contractual relationship, it would take time and money for the platform operator to individually negotiate and determine the contractual terms and conditions with a number of data providers and data users and it would also require costs for contract management, so the platform operator would be motivated and wish to take stereotypical and efficient measures by using the terms of use.

In addition, if the platform is built by individual contracts, there would be no means for data providers and data users to learn the details of individual contracts between other data providers and data users and the platform operator. On the other hand, if the terms of use with stereotypical contract details are adopted, the data providers and data users would be able to gain a sense of security to know that the terms and conditions stipulated in their contracts are not disadvantageous compared to those of other data providers and data users, so there is considered to be an advantage of making it easier for the data providers and data users to participate in the platform where contractual relationships are established based on the terms of use. Moreover, when any data provider or data user causes a breach of the terms of use or any other trouble, it would be easy for other data providers and data users to request the platform operator to pursue liability under the terms of use against such breaching party as described in Part VI-1-(3) above if they know which clause in the terms of use had been breached by such act.

Accordingly, this Paragraph describes the matters to be noted under laws and ordinances upon establishing the structure of the platform type on the premise that the terms of use would be adopted, which is often the case in the platform type.

(ii) Terms of use with data providers and terms of use with data users

With respect to the terms of use required in the platform type, there should at least be the terms of use between data providers and platform operator and the terms of use between data users and platform operator.

It would be decided based on the individual circumstances whether to prepare such two types of terms of use as separate and independent or as one integrated instrument. Generally speaking, it is considered unnecessary to prepare separate and independent terms of use if the data providers and data users are completely identical, but either way is possible if data providers and data users are not the same.
VI “Data Sharing Type” Contracts

(2) Significance of specifying scope of data utilization in terms of use

While data cannot be the subject of any property rights as described in Part III-1 above and it is necessary to form an agreement relating to the utilization rights (establishment of a relationship of claims and obligations) in order for the data to be utilized among multiple parties without dispute, it is considered common for the platform type to establish the relationship of claims and obligations relating to data sharing and application by specifying and agreeing to the scope of data utilization in the terms of use.

In addition, there are at least two conceivable cases as described below where the “scope of utilization” needs to be established in the terms of use for the platform type.

The first case is (i) the scope of utilization established in the terms of use between data providers and platform operator which specifies when, for what purpose, and in which form or method, the platform operator or other participants (business operators who perform processing or analysis utilizing the utilized data provided by the platform, business operators who develop utilized services, etc.) may utilize the provided data, and the second case is (ii) the scope of utilization established in the terms of use between data users and the platform operator which specifies when, for what purpose, and in which form or manner, the data users may utilize the utilized data or utilized services.

(i) Scope of utilization between data providers and platform operator

As platform operator and data users have a motive to widely share or apply data, it can be said that they tend to require the scope of utilization of provided data to be as broad or abstract as possible.

On the other hand, data providers have a strong interest in the way their provided data would be shared or applied, and sometimes wish to limit data users as described in Part VI-3-(3)-(i) below, so it can be said that they tend to require the scope of utilization of the provided data to be as specific or restrictive as possible. In other words, the scope of utilization can be said to make it possible for the data providers to predict by which data users or other participants and in what way the provided data provided to the platform would be shared or applied, and consequently to motivate the data providers to provide, or refrain from providing, their data.

As described above, since there can be conflicting demands between data providers and the platform operator (and consequently data users) with respect to the specificity of the scope of utilization of provided data, it is desirable, in terms of preventing future conflicts, to make adequate consideration on the details (specificity) of the scope of utilization when establishing the scope of utilization of provided data in the terms of use.

Accordingly, the terms of use between data providers and the platform operator would include the provisions relating to the scope of utilization within which the platform operator or third party delegated by the platform operator (partner) may utilize the provided data (the existence and scope of such third party, scope of provided data, purpose of utilization and form or method of utilization). In such case, if such provisions specify the scope of utilization within which the platform operator may utilize the utilized data or utilized services based on the provided data, then they might also restrict the scope of utilization for data users.
VI “Data Sharing Type” Contracts

(ii) Scope of utilization between data users and platform operator

Prescribing the purpose of utilization of utilized data or utilized services in the terms of use between data users and the platform operator would offer data users the criteria for judgment of the scope within which the utilized data or utilized services would be permitted to be shared or applied.

It should be noted that the platform operator needs to establish the scope of utilization of utilized data or utilized services to the extent of not breaching or conflicting with the scope of utilization established in the terms of use with data providers. From such perspective, even if the terms of use between data providers and the platform operator and the terms of use between data users and the platform operator are separately prepared, the scope of data utilization established in the respective terms of use can be said to correlate to each other.

As both the terms of use between data providers and the platform operator and the terms of use between data users and the platform operator generally prohibit any unintended utilization of data and provide for damages or the imposition of other sanctions against any breach of obligations in the platform type, the “scope of utilization” may be used to regulate acts of the platform operator or data users or to assist in determining whether an act is in breach of the terms of use. Therefore, if the scope of utilization is established to an extent of specificity such that predictability (as to which acts are permitted and which acts are prohibited) would be secured for the platform operator or data users, this could be said to contribute to the prevention of future disputes.

(3) Type, etc. of data and services handled on platforms

(i) Nature of data

As described in Part I-2, the combinations of multiple data across industries are expected to lead to open innovation, and it is important to broaden the subject and type of data to be utilized and utilize data in various combinations in order to improve the added value of the data and strengthen competitiveness.

However, in the platform type, it is possible that competitive business operators of data providers are included as data users not only in the case where data providers and data users are completely identical but also in the case where data providers and data users are not completely identical and there are also parties who only either provide or utilize data. In such case, the data providers often become reluctant to provide their data.

Therefore, when establishing the purpose of the platform business, for example, it is conceivable to make the parties benefit from common advantages for utilizing the platform even when competitive business operators are included among the participants in the aim of collecting more data within the platform.

On the other hand, it is also conceivable to separate the data which might reduce the competitiveness of the company if disclosed to other business operators (especially to competitive business operators of the company) and the data which would have no direct effect or have only a small effect on the competitiveness of the company even if disclosed to other business operators, and preferentially provide the latter as provided data, and impose certain limits on the scope of data users relating to the former data or require the former data to be processed or analyzed in a certain manner so that the business of the data providers would not be damaged or otherwise incur any adverse effects.
VI “Data Sharing Type” Contracts

In this regard, one of the advantages of the platform type is that, even with respect to data which might reduce the competitiveness of the company if disclosed to other business operators (especially to competitive business operators of the company), it would be possible to manage the data sharing or application by each business domain by dividing up the business domain. For example, in the case where, while certain data should be avoided from being shared or applied by other companies (even with restrictions) in business domain $a$, it can be concluded that there would be no “competitive business operator” in relation to such data in business domain $b$ and business domain $c$, the data providers may provide such data to the platform and make an agreement with the platform operator to limit the parties who may utilize such data so that the platform operator may select the parties to which such data may be provided (the parties who may utilize the data). This would make it possible to conduct separate management of data sharing or application by each business domain where such data or any utilized services using such data would not be provided to the data users in business domain $a$ but would be provided to the data users in business domain $b$ and business domain $c$.

In the case where data would be shared or applied separately for each business domain, it is necessary to establish restrictive terms and conditions of data sharing or application based on the type of the data in the terms of use between data providers and the platform operator.

(ii) Types of utilized data and utilized services

The product supplied by platform operators is considered to take the form of data (utilized data) or services (utilized services). The conceivable methods of providing utilized data are: (i) the provision of provided data in their original condition as utilized data; and (ii) the provision by the platform operator of the data acquired from processing the provided data or the results (data) acquired from analysis of the provided data by the platform operator or third party delegated by the platform operator. The conceivable methods of providing utilized services, meanwhile, include: (iii) the provision by the platform operator of services, application programs, solutions or business opportunities based on the results of analysis obtained from the utilization of the provided data by the platform operator or third party delegated by the platform operator to data users.
VI  “Data Sharing Type” Contracts

In the platform type, which aims for a broad range of data sharing and application, while there is demand for the provision of as much provided data as possible, the platforms also sometimes function as a filter between data providers and data users and impose restrictions on the manners of sharing or application of the provided data. Therefore, it is desirable, in terms of preventing future disputes, that the manner in which the provided data would leave the platform and the manner in which the provided data would be stored in the platform are arranged and specified in the terms of use from the perspectives of (i) through (iii) above and that the platform operator and data providers make an agreement with respect to the scope of the parties who may utilize the provided data that had been disclosed or provided in their original condition, purpose of utilization of the provided data, form and manner of utilization, manner of storage of the provided data and utilized data or utilized service, scope of data users and other matters.

It is also desirable, in terms of preventing future disputes, that the platform operator and data users specify in the terms of use and make an agreement as to whether the data users may receive from the platform operator the provided data in their original condition, processed data, data of the results of analysis, services, application programs, solutions or business opportunities based on the results of analysis, or any part or all of the above. If the items that the data users may receive from the platform operator differ by the type of the provided data or by period, the parties should organize, specify and make an agreement as to the items that the data users may receive by each data type and period.

(iii) Derived data and other derivative products

73
VI  “Data Sharing Type” Contracts

a  Derivative products in platform type

In the “data provision type,” it is necessary for data providers and data users to determine the handling of the utilization rights to derived data and other derived products generated as a result of data users utilizing the data provided. However, in the platform type, derived products (utilized data and utilized services) generated as a result of processing or analysis of the provided data or development of services based on the results of such analysis by the platform are planned to be utilized by data users, so the issue of how to determine the utilization rights to such derivative products emerges as an issue of how to specify the scope of utilization of the utilized data or utilized services.

In the case where the platform operator makes the derived data or derived services available to any party other than data users, it is advisable to expressly state in the scope of utilization to that effect and make efforts to prevent any future dispute.

b  Intellectual property rights, etc. generated by platform operators

As the handling of intellectual property rights and intellectual properties arising in the course of the generation of derivative products by the platform operator (utilized data or utilized services) cannot be unambiguously determined by establishing the scope of utilization of utilized data or utilized service, it is necessary to consider whether to establish a separate provision.

Upon specifying the intellectual property rights, etc. arising in the course of generating derivative products (utilized data or utilized services) in the terms of use, it is conceivable to determine that the intellectual property rights, etc. belong to: (i) the platform operator only, (ii) all data providers (shared by all data providers), or (iii) the platform operator and all data providers (shared by the platform operator and all data providers).

In this regard, even in case (ii) or (iii), if the platform operator obtains a license (including a sublicense as necessary) for all intellectual property rights, etc. under the terms of use, it can be considered that there would be no such issue as discontinuance or termination of the platform business due to infringement of intellectual property rights when the platform business operator provides utilized data or utilized services to data users.

c  Derivative products generated by data users

As the handling of the derivative products (including intellectual property rights, etc.) arising as a result of data users sharing or applying utilized data or utilized services provided by the platform cannot be unambiguously determined by establishing the scope of utilization of utilized data or utilized services, it is necessary to consider whether to establish any separate provision.

While there would be no problem in principle if the platform operator is granted a non-exclusive license for the intellectual property rights, etc. attributable to data users, it should be noted that a problem might arise under the Antimonopoly Act when it is specified in the terms of use between data users and the platform operator that the platform operator would be granted an assignment without consideration or exclusive license with respect to such intellectual property rights, etc.
VI “Data Sharing Type” Contracts

d Handling of derivative products generated from analysis using AI technology by platform operator or third party delegated thereby (partner)

See the AI Section for the handling of derivative products (training datasets, trained models, etc.) generated in connection with AI analysis of provided data such as, for example, when the platform operator provides provided data and requests for data analysis to a data analyzer using AI technology.

(iv) Distribution of profits

It is conceivable to establish in the terms of use between data providers and platform operators a provision regarding the distribution of profits gained from derived products generated by the platform.

However, it is often the case in the platform type that data providers also participate in the platform as data users, and in such case, it is possible to adopt a platform type with a structure in which data providers would not seek distribution of any further profits as data provider based on the understanding that the data providers already obtain certain profits by utilizing derivative products as data user.

In addition, when, for example, distributing profits gained from a streamlined business achieved by a data user based on the data analysis obtained from a data analyzer to which the data user has provided the data received through the platform for data analysis or any other case in the platform type where a number of participants are involved, it is often difficult to calculate the degree of contribution (contribution ratio) of the provided data to such profits and the scope of the parties to which such profits should be distributed. Therefore, it is often considered appropriate not to establish any provision regarding the distribution of profits.

(v) Data containing business secrets and know-how

It is possible that provided data contains trade secrets, so it is important for data providers to make examinations from the perspective of classifying the data into two types, i.e., the data to be provided to the platform as provided data and the data to be intentionally kept within the company.

In addition, even when data contains any trade secrets, it is conceivable to establish in the scope of utilization clause in the terms of use to the effect that, after such data is provided to the platform as provided data, the platform operator would divide data users into groups to be able to control the sharing or application of the provided data based on such groups. Data providers and the platform operator would agree by the terms of use to the restrictive terms and conditions of provided data such as, for example, the classification of the data users into three types, i.e., those who are permitted to share or apply the provided data containing trade secrets in their original condition, those who are not permitted to utilize or apply such provided data at all, and those who are permitted to share or apply such provided data upon certain processing, and the provided data would be controlled in the platform in accordance with such restrictive terms and conditions.

In the situation where any provided data containing trade secrets is provided to the platform and such provided data might be provided to data users through the platform operator as utilized data or utilized services, it is possible that, among other requirements of “trade secrets” under the Unfair Competition Prevention Act, the requirement of “confidentiality” or “non-public
VI  “Data Sharing Type” Contracts

nature” might not be particularly satisfied. Therefore, it is also sometimes necessary to consider from such point of view whether or not such provided data may be provided to the platform and, if so, the restrictive terms and conditions of such provided data.

(vi) Data containing personal information

As described in Part VI-1, since the platform type is expected to create new value by allowing multiple business operators to utilize or apply provided data across different business groups, the scope of utilization might be set as broadly as possible in some cases. On the other hand, if the scope of utilization is broadly set, it might be difficult for personal information handling business operators to satisfy the requirement of specifying the purpose of utilization under Article 15 of the Act on Protection of Personal Information and the requirement of obtaining principal’s consent relating to third party provision under Article 23 of the same Act. Therefore, when providing information through the platform, since it is not practicable for the platform operator to fully specify the purpose of utilization and the scope of third party provision in advance, it is sometimes desirable, in terms of complying with laws and ordinances, to adopt a system in which personal information would not be collected in the platform as provided data.

Accordingly, with respect to the handling of any provided data containing personal information, it is conceivable that such data would be made into anonymously processed information (Article 2(9) of the Act on Protection of Personal Information) or statistic information or any other non-personal information by the data provider in advance and then distributed through the platform. In such case, it is possible to make the data provider have certain responsibility for the fact that the provided data is non-personal information and not personal information.

(vii) Data subject to intellectual property rights

The data that are considered to be subject to intellectual property rights are as follows:

(i) rights relating to trade secrets (see (v) above);

(ii) copyrights (for example, in the case that the provided data is a creative image or video, copyrightable work of a database, or 3D data of a character figure, etc.);

(iii) design rights (for example, in the case that the provided data is a 3D data of a furniture for which the design registration has been filed);

(iv) patent rights (for example, in the case that the provided data is a program, etc. for which the patent rights (patent rights of the program, etc.) has been obtained); or

(v) circuit layout rights (for example, the provided data is a drawing or picture including the circuit layouts under the Act on the Circuit Layout of a Semiconductor Integrated Circuits).

Therefore, in the case where provided data contains any data that would be subject to intellectual property rights, it should be noted and handled so that any processing or analysis by the platform operator or data sharing or application by data users would not fall under an infringement of the intellectual property right.

However, with respect to any of the data listed in (ii) through (v) above, the parties should not be concerned that intellectual property rights might be immediately infringed just by utilizing
VI “Data Sharing Type” Contracts

the data subject to intellectual property rights, but instead it is necessary to specifically analyze what kind of act would be conducted or expected to be conducted, and carefully examine whether or not such act would infringe any intellectual property right depending on the form of the act and take measures therefor (see Part VI-3-(3)-(v) above for the trade secret in (i) above).

(4) Scope of participants

(i) When a data provider is also a data user

As shown above (Diagram 7), since all or some of the data providers are also data users, regulations regarding cartels might be applicable if the parties can determine the product price, production volume, etc. by sharing or applying data through the platform without directly communicating with other participants.

In addition, in the case where there are data users who cannot be said to have a value exchange relationship (one in which it is a result of the data users providing their own data that they are permitted to utilize other provided data), a clause concerning data users who are not data providers would be established in the terms of use. In other words, while it is construed that data users who are also data providers bear obligations to provide data with the platform operator, it is necessary to consider what kind of obligations the data users who are not data providers should bear under the contractual relationship with the platform operator (whether to establish a contractual relationship under which such data users bear any obligations other than the payment of usage fees).

(ii) Open type platform

In the case of an open type platform, it is desirable, in terms of preventing future disputes, to clarify in the terms of use that the platform would be an open type and specify in the provisions regarding the scope of utilization in the terms of use between data providers and the platform operator to the effect that the provided data might be broadly shared or applied by data users who are not data providers.

As described in Part VI-1-(2)-(i) above, there are cases where other platform operators participate as data users, which can be called an advanced form of open type platform. In such case, when it is assumed at least at the time of preparing the terms of use that other platform operators might participate as data users, it is advisable to specify in the terms of use to that effect and make efforts to prevent any future dispute.

(iii) Third party delegation by platform operator of processing, analysis, etc. of provided data

As shown in Diagram 8 above, there are many cases where the platform operator cooperates with a third party in the handling of provided data (in this Paragraph, such third party is referred to as “partner”), such as when the platform operator borrows a server or cloud of a third party for the storage of the provided data or delegates a third party with processing, analysis, etc. of the provided data or a third party directly provides application programs or services utilizing the provided data to data users.
VI  “Data Sharing Type” Contracts

If there is a partner, it is desirable to prevent any future dispute by specifying in the scope of utilization that the provided data might be provided to outside parties (the partner) or processed or analyzed by the partner.

It is often difficult from the perspectives of technical advancement, cost reduction and other factors to make a detailed prediction into the future as to which third party should be a partner, and it is considered that statements relating to the partner in the terms of use would often be abstract and blanket to some extent (in other words, the platform operator may retain discretion for partner selection from data providers by specifying certain blanket provisions in the terms of use to the effect that partners might utilize the provided data). In such case, it might be able to prevent future disputes by establishing terms and conditions, etc. that specify the scope of partners in order to give predictability regarding the scope of partners.

In addition, it is advisable to stipulate in the terms of use whether or not the platform operator should be primarily liable when any partner utilizes provided data in breach of the contract between the platform operator and such partner or otherwise and causes damage to data providers or data users (i.e., whether or not the platform operator should compensate for damage on behalf of the partner), and clarify the scope of liability that the platform operator would bear to data providers and data users.

(5) Which entity should be platform operator

(i) Neutrality and creditworthiness

The issue of who should be the platform operator is sometimes required to be decided from the perspectives of neutrality and creditworthiness in addition to the business perspective of “who is better to play the role.”

In the case where the platform operator is responsible for governing the rights, obligations and responsibilities of data providers and data users based on the details of the terms of use as described in Part VI-3-(1) above, it is often easier to procure neutrality and obtain creditworthiness if any third party who has no capital or business relationship with any of the data providers or data users becomes the platform operator or if a joint venture, partnership or general incorporated association is established between data providers and data users or among participants, rather than if one of the data providers or data users who are not data providers becomes the platform operator.

However, neutrality cannot be immediately procured just by adopting the form of establishing a joint venture, partnership or general incorporated association. For example, when data providers and data users or participants intend to establish a stock company as a joint venture by contributing funds, there are a number of matters to be considered and agreed to among the participants, such as the contribution ratio (which participant would hold how many shares, whether to create shares without voting rights or class shares including shares with different dividends, etc.), how many directors should be selected for operating the joint venture and from which participants, and how the allocation ratio of expenses required for the operation of the joint venture should be decided.

(ii) Safety (cyber security)
VI “Data Sharing Type” Contracts

As platform operators handle various types of provided data as described above, it is construed that they are required to take a certain extent of cyber security measures and have obligations for the safe management of provided data, utilized data and utilized services.

If any platform operator fails to perform a cyber security measure that is generally expected to be performed or is usually implemented by platform operators, the platform operator would be considered to be responsible when any security incident occurs. On the other hand, it can be said that it is impossible to have perfect cyber security measures, so it is necessary to consider prescribing an exemption for a certain extent of cyber security incidents.

(iii) (For reference) Establishment of “Certification System for Plan for Innovative Utilization of Data in Industries”

In order to support data aggregation or application or collaboration by business operators, the following measures, etc. are planned to be taken under the Act on Special Measures for Productivity Improvement established in May 2018.

a Establishment of recognition system and support through preferential tax treatment, etc.

Any platform operator who plans to collect and apply data for industrial activities may obtain certification from the competent minister with respect to the plan for business of industrial application of data (the Plan for Innovative Utilization of Data in Industries) on the condition of satisfaction of the procurement of security and other certain requirements, and, with such certification, the platform operator may receive preferential tax treatment (such platform operator, etc. would be granted with incentives).

b Cooperation from expert government institutions, etc. for protection of personal information and safety management of data

The competent minister will, upon giving the certification for the plan as above, (i) discuss with the Personal Information Protection Committee as necessary to confirm the status of compliance with the Act on Protection of Personal Information and make efforts to reduce anxiety and concerns of consumers, and (ii) make it possible to make requests for cooperation from the Information-technology Promotion Agency, Japan (Incorporated Administrative Agency) or other institutions in an attempt to procure the safety of data.

c Support through data provision request system

A platform operator, etc. which has obtained the certification for the plan as above may, when making an arrangement, provision, etc. of data to be applied by any other business operator, obtain security confirmation from the competent minister to request for a provision of data held by public institutions, etc.

4 Main items of terms of use

(1) Scope of license (scope of utilization) of provided data or utilized data or utilized services
VI  “Data Sharing Type” Contracts

As described in Part VI-3-(2) above, it is conceivable that (i) the scope of utilization of provided data would be set forth in the terms of use between data providers and the platform operator, and (ii) the scope of utilization of utilized data or utilized services provided by the platform would be set forth in the terms of use between data users and platform operator.

The scope within which the utilization of provided data or utilized data or utilized services is permitted would be determined in this manner.

In addition, as described in Part VI-3-(3)-(iii), the handling of utilized data and utilized services as derivative products would be determined by the provisions relating to the scope of utilization between data providers and the platform operator.

The scope of utilization is often specified by a combination of all or part of the following factors: (i) which provided data; (ii) by whom (attribution, scope and terms and conditions of the data users, scope and terms and conditions of the partners of the platform operator and other participants, etc.); (iii) when (period); (iv) where (for example, it might be requested not to record the provided data in a server outside the country); (v) for what purpose; and (vi) in what form or method the sharing or application would be performed.

In particular, when the platform operator might collaborate with a partner, as described in Part VI-3-(4)-(iii) above, it is desirable to specify in the scope of utilization clause as to with which partner the platform operator might conduct what kind of collaboration.

In addition, as described in Part VI-3-(3)-(i) above, there are cases where the parties establish a provision, etc. in the scope of utilization clause to the effect that the data users would be adjusted based on the type, domain and other attributes of the provided data.

Further, in the case of a platform which permits broad sharing or application of provided data, for example, the parties may set forth a blanket scope of utilization clause, such as “the data users may, or may cause any third party to, process or analyze the utilized data, license or assign the utilized data to a third party, or jointly utilize the utilized data with a third party,” and establish such clause in the terms of use between data users and platform operator and the terms of use between data providers and platform operator.

Moreover, when provided data consists of data that would apparently have no direct effect or have only a small effect on the competitiveness of the company even if disclosed to other business operators, etc., the parties may stipulate a blanket scope of utilization such as by leaving the sharing or application of provided data to the discretion of the platform operator.

As described above, whether it is stipulated specifically or broadly, the scope of utilization would determine the rights, obligations and responsibilities between data providers and platform operator and between data users and platform operator, and therefore such provision should be able to secure predictability for data providers and data users.

(2)  Responsibilities of data provider in respect of provided data (warranty/no warranty)

(i)  Including or not including provisions regarding responsibility

It is conceivable to set forth in the terms of use as to what kind of responsibility the data providers would or would not bear with respect to provided data. As described in Part IV-2-(2) above, the parties may sometimes prescribe that the amount, details, granularity, form, etc. of the data would not be warranted.
VI  “Data Sharing Type” Contracts

On the other hand, as described in (ii) below, the parties may make data providers responsible for their provided data in certain cases.

While the parties may make data providers responsible or not responsible or partially responsible in respect of their provided data as described above, the parties should not design the scope of responsibilities of data providers from the viewpoint of which is objectively preferable but from the business perspective of how to design the responsibility issues so that the platform can be operated continuously while procuring the necessary quantity of data providers with the necessary attributes.

It is possible in the platform type to establish an exemption clause in the terms of use to make data providers not responsible for the accuracy of data. However, in the case of industrial data, if, for example, there is any time axis variation, wrong unit conversion or falsification or fabrication of data just to pass examination or any other situation occurs, unpredictable damage might arise when multiple participants utilize such data through the platform. Even if seeking a guaranty for the accuracy of data, it is desirable to precisely specify the meaning of “accuracy” in the terms of use and clarify who would be responsible, if anyone, for such accuracy.

(ii) Data is not acquired through illegal or unauthorized means

a  If using a blanket provision

There are cases where data providers are made responsible for the fact that their data have not been acquired through illegal or unauthorized means by making general representations and warranties to that effect without referring to any specific details of law or ordinance or, conversely, it might be specified that data providers would have no such responsibility at all.

b  If mentioning specific laws and ordinances

For example, in the case that any provided data falls under a trade secret, the parties would establish a clause in which the data provider represents and warrants that it is the authentic holder of the trade secret or, if the trade secret is held by multiple parties, represents and warrants that it has obtained consent from, or is delegated by, other holders to share or apply such data in the platform.

In addition, in the case of trade secrets held by a third party, the parties would establish a clause in which the data provider represents and warrants that it has obtained consent from, or is delegated by, the third party to share or apply such data in the platform.

In the case of any other data which would be the subject of intellectual property rights, as described in Part VI-3-(3)-(vii), the parties would first closely examine (i) whether the provision of such data to the platform could be an infringement and (ii) whether the sharing or application of such data through the platform could be an infringement, and, if such act could be an infringement, the parties would establish a clause in which the data provider represents and warrants that (A) it has obtained consent from the holders of such intellectual property rights to provide such data to the platform, and (B) it has obtained consent from the holders of such intellectual property rights to share or apply such data through the platform.

When it is clear that (i) above would not be applicable, there appear to sometimes be cases where the data provider is made to represent and warrant that the provision of the provided data to the platform would not infringe any intellectual property rights of third party. In such case,
VI  “Data Sharing Type” Contracts

although it is difficult to find any legal effect, it might have the practical effect of intimidating the data provider.

In addition, in the case where the provided data contains personal information, for example, there are cases where the data provider is made to represent and warrant that it has obtained the principal’s consent to share or apply the data in the platform or that the provided data is non-personal information.

(3) Rights related to derived data and other derivative products

(i) Necessity of definition clause

First, while it is necessary to establish a clause which clarifies the basis for the definition of the term “derivative data” or “derivative products,” as described in Part VI-3-(3)-(iii), it is possible in the platform type to construe that the platform operator obtains the consent to the provision of derived data and derived services, among other derived products, to data users by virtue of such scope of utilization clause.

Therefore, in some cases, “derived data” and “derived services” are not separately defined and instead the relationship of utilized data and utilized services being derivative products is stated for confirmation. Needless to say, there are also cases where definition clauses for derived data and derived services are established.

In either case, attention should be paid so that there would be no discrepancy regarding the definition among the participants or so that the participants can share common recognition that derived data and derived services are equivalent to utilized data and utilized services.

(ii) Handling of intellectual property rights, etc.

As described above, it should be noted that (i) any intellectual property rights, etc. arising in the course of generating derived data or derived services by the platform operator and (ii) any intellectual property rights, etc. arising in the course of utilizing or applying utilized data or utilized services by data users should be separately organized.

While the handling of intellectual property rights, etc. arising as a result of analyzing the provided data by any other participant (for example, a partner) should be primarily determined by the platform operator and the partner, there are cases where the handling of the data by the platform operator and the partner are set forth in the terms of use between data providers/data users and the platform operator for confirmation.

(iii) Other derivative products generated by data users

For example, in some cases, it is stipulated that all derivative products generated by the utilization of any utilized data or utilized services by data users would be held by the data users in order to encourage data sharing or application, and in other cases, it is stipulated that data providers should be offered an opportunity to utilize any application program or service generated as a result of sharing or applying any utilized data by data users in order to encourage the data providers to provide their data.

(iv) Distribution of profits relating to derivative products
VI  “Data Sharing Type” Contracts

The distribution of profits needs to be organized by the types of profits such as (i) profits obtained by the provision of derived data or derived services by the platform operator; (ii) profits obtained by the implementation of intellectual property rights, etc. arising in the course of generating derived data or derived services by the platform operator; and (iii) profits obtained by the utilization of derivative products (intellectual property rights or application programs, etc.) arising in the course of sharing or applying utilized data or utilized services by the data users. With respect to (i) through (iii) above, the distribution of profits would be designed separately by platforms.

Considering the fact that it is difficult to calculate the degree of contribution (contribution ratio) of provided data to such profits or the scope of the parties to which such profits should be distributed as described in Part VI-3-(3)-(iv) above, there are cases where no profit distribution would be conducted.

In addition, in order to encourage the participation of data providers, even if it is difficult to calculate “profits,” in the case of (iii) above, there are cases where it is designed as closely as possible to the distribution of profits such as by stipulating that data providers must be offered an opportunity to utilize any application program or service generated as a result of data sharing or application by data users at lower cost than any third party.

(4) Audits and complaint and dispute settlement

For the purpose of maintaining the creditworthiness of the business management of the platform, there are cases where platform operator requires regular or irregular written reports or disclosure of certain documents from data providers and data users or, as applicable, it is provided for in the terms of use that the platform operator has a field audit right against data providers or data users, to confirm whether data providers provide their data and data users utilize utilized data or utilized services respectively in accordance with the terms of use.

Conversely, there are cases where it is stipulated that data providers or data users have an audit right against the platform operator.

There can be various forms of field audits as is the case of field audits under any contract other than a data contract, and the parties would determine issues such as how long the notice period should be, and whether the platform operator would enter the premises of the corporation of the data provider or data user, inspect event logs or access servers.

In addition, in terms of maintaining the creditworthiness of the platform business, matters such as a place where data providers and data users can file complaints or the means of resolution in case any dispute arises between data providers and data users would be prescribed in advance in the terms of use in some cases.

There are also cases where the response policy for complaints filed by third party (for example, demand for immediate suspension of provision of any data relating to the third party’s company that have been provided to the platform without consent, etc.) is prescribed in advance in the terms of use.

(5) Obligations and liabilities of platform operators (limitation of liability)

(i) Obligations of platform operators
VI  “Data Sharing Type” Contracts

a  Obligation relating to cyber security in storage of provided data, utilized data and utilized services

As platform operators are in the position to collect and store provided data, despite some difficult aspects of bearing an obligation to comprehensively confirm the details and quality of large quantities of provided data that they collect, the platform operators are required to take a certain extent of cyber security measures, and it is often considered appropriate to make them bear an obligation relating to safe management of provided data, utilized data and utilized services as long as they conduct the business of collecting and storing large amounts of various provided data.

In addition, as described in Part IV-3-(5)-(ii) above, it is not practicable to require absolute cyber security measures, so there are cases where it is provided for in the terms of use that liability for cyber security measures would be limited to a certain extent.

b  Obligation of data storage and deletion

The obligation of platform operators to store or delete provided data, etc. (an obligation to store the data for a certain period of time or to delete the data on certain conditions) might be established in some cases.

For example, since it is assumed that data users have an interest in the matters such as, with respect to certain utilized data, for how long the data have been stored in the past and would be available (how long a period the utilized data that may be available to data users cover), there are cases where the platform operator is obligated to determine the period of time for which the utilized data would be stored. In addition, since it is assumed that data providers have an interest in the matters such as, with respect to the provided data they have provided, in what cases the data would be deleted, there are cases where the platform operator is obligated to determine the conditions on which the provided data would be deleted.

c  Obligation relating to access to platform, etc.

Platforms are required to be accessible at any time, in other words, it is required to be able to provide provided data at any time and receive the provision of utilized data or utilized services at any time.

On the other hand, such obligation of provision, etc. may not be performed due to force majeure including communication failure, natural disaster, strikes of the platform operator or partner employees, or an order for suspension of business from a court or administrative agency. Therefore, it is also advisable to stipulate in the terms of use a limitation of liability such as by specifying the cases in which the platform operator would be exempted from the obligation of provision, etc. of utilized data or utilized service.

d  Obligation of confidentiality

Even if provided data do not fall under trade secrets, it is possible that, for example, data providers request that their provision of data to the platform is not disclosed or that data users request that their sharing or application of data through the platform is not disclosed, so there are cases where an obligation of confidentiality is provided for in the terms of use.
VI “Data Sharing Type” Contracts

In addition, if the platform operator is unwilling to disclose the details of the terms of use to any person other than data providers and data users, the platform operator may impose an obligation of confidentiality relating to the details of the terms of use to data providers and data users in some cases.

If any provided data fall under trade secrets, the platform operator would be obligated under the terms of use not only to manage the provided data in confidential but also to impose an obligation of confidentiality upon data users when disclosing or providing the provided data (see Part VI-3-(3)-(v) above).

e Obligation to disclose information

As it is generally argued that information disclosure is an effective way to gain or increase creditworthiness, it is conceivable that the platform operator might disclose the status of data sharing or application in the platform, status of implementation of cyber security measures and other matters to data providers and data users (and persons who wish to become data providers or data users) on a regular basis.

f Compliance with Antimonopoly Act

In the operation of platforms, attention must be paid so that the selection of participants and the details and management of the contracts with participants would not fall under private monopolization, unjust restrictions on transaction, unfair trade practices (abuse of superior bargaining position, restrictive trading, exclusive dealing, etc.) or any other breach of the Antimonopoly Act, depending on the scope of data providers and the nature of data to be handled. Although it is not considered necessary to require the platform operator to comply with the Antimonopoly Act or otherwise establish any such abstract provision in the terms of use, the Antimonopoly Act needs to be complied with as a public law regardless of such provisions.

(ii) Liabilities of platform operators (limitation of liability)

a Liability to data provider regarding handling of provided data

It is construed that platform operators have (i) a responsibility to generate utilized data or utilized services within the scope of utilization agreed to with data providers by the terms of use and (ii) an obligation to provide utilized data or utilized services to a certain scope of data users based on the type of the provided data within the scope of utilization agreed to with data providers by the terms of use. Therefore, it is sometimes provided for in the terms of use between data providers and the platform operator to the effect that the platform operator has such liability relating to the handling of the provided data.

In this regard, while it is anticipated that no one would want to provide their data if it is decided that platform operators bear no liability relating to the handling of provided data, it is also difficult in terms of costs to make platform operators bear all liabilities. Accordingly, it can be said that the liability is often limited to a certain extent under the terms of use between data providers and the platform operator.
VI “Data Sharing Type” Contracts

In addition, in the case that provided data contains personal information, platform operators must take security control measures (Article 20 of the Act on Protection of Personal Information).

b Liability regarding data sharing and utilization

As described in Part VI-3-(1)-(i) above, it is sometimes stipulated in the terms of use that data providers and data users have the right to demand the platform operator to effect a claim for damages or any other sanction upon breach of the terms of use by other data providers or data user (the right to demand the platform operator to pursue the default liability of the data users, etc.) so that they would be able to pursue the liability of such breaching party.

Even if it is not provided for in the terms of use, it might be able to be construed that the failure of the platform operator to claim liability against a breach of the terms of use between the platform operator and data users would constitute contractual default (omission) between the platform operator and data providers.

In addition, there are cases where it is stipulated that the platform operator would bear a certain liability or would not bear any liability when any third party claims for suspension of utilization of any data acquired through the platform against data user.

c Limitation of liability of platform operators

When it is intended to limit the liability of the platform operator, the maximum amount of damages to be borne by the platform operator might be stipulated.

However, as described in Part VI-4-(6) below, it is possible to prescribe in advance the calculation formula for the amount of damage based on the usage fee with data users, from which usage fee is collected, but with data providers, it is difficult to assume any case where the platform operator collect fee from them to receive their provided data. Therefore, it is necessary to consider the calculation method on based on which the amount of damage should be limited to a certain extent.

(6) Obligations and liabilities of data provider and data user (limitation of liability)

(i) Obligations of data provider and data user

Data providers might be obligated to provide their provided data for a certain period of time or in a certain amount, or data users might be prohibited to provide any utilized data to third party in some cases.

In addition, there are cases where prohibited acts, such as unauthorized access to the platform or interference with the operation of platform by the platform operator, are stipulated for both data providers and data users.

Further, there are cases where it is provided for that data providers have an obligation to take necessary measures under laws and ordinances with respect to joint utilization or third party provision through the platform of any provided data which contain personal information, or an obligation to prohibit any act of identifying individuals from anonymously processed information created from personal information or other obligations under laws.
(ii) Liabilities of data provider and data user (limitation of liability)

For example, it is possible to make the data providers liable, if they provide data containing trade secret, for ensuring that the data do not infringe any trade secret of third party, or not liable, if their provided data are image data, for ensuring that the data do not infringe any copyright of third party (limitation of liability).

In particular, with respect to the liabilities of data providers, it might be stipulated that data providers are liable for the accuracy, completeness, effectiveness and safety of the data in some cases or, conversely, no warranty is made with respect to the above to limit their liability in other cases.

In addition, with respect to the limitation of liability, as described in Part VI-4-(5)-(ii)-b above, there are cases where the amount of damage is limited to a certain amount. In this regard, with respect to data users, as it is considered that they often pay usage fee to receive the provision of utilized data or utilized services, it is possible to calculate the amount of damage based on the usage fee and prescribe in advance the amount in the terms of use. However, with respect to data providers, it is necessary to consider the calculation formula based on which the amount of damage should be limited to a certain amount, except when they pay fees to provide their provided data.

(7) Sanctions upon violation of terms of use

In order to maintain the creditworthiness of the platform operation, there are cases where it is stipulated that sanctions would be executed when any of data providers, data users or platform operator breaches the terms of use.

If the sanctions imposed upon breach of the terms of use would be stipulated, it is conceivable to establish, as premises, a provision regarding procedures relating to the method of certifying the breach of the terms of use.

(8) Handling of provided data and derivative products upon withdrawal and termination

(i) Scope of influence of withdrawal and termination

When any data provider or data user withdraws from the platform business, there might be an issue of how to handle the data provided by that party or derivative products, etc. generated as a result of data sharing or application by that party. In other words, there would be an issue of whether to terminate the provision of the data, application programs or services provided by the platform operator to data users upon processing or analyzing such provided data and the sharing or application of such provided data by data users as well.

If it is designed that the sharing or application of the provided data would be retrospectively invalidated upon withdrawal or termination, there would be a concern that the safety of the transactions conducted by data users and other participants who had already shared or applied such provided data might be harmed.

Therefore, it is conceivable to specify that even when any data provider withdraws from the platform, for example, the derivative products, etc. obtained by sharing or applying such provided data by data users would not be affected in any way.
VI “Data Sharing Type” Contracts

The sharing or application of the provided data of such data provider might be suspended either upon or immediately after the withdrawal or termination or after a certain period of time.

In addition, regardless of retrospective invalidation or prospective invalidation, the obligation of the platform operator, etc. to delete the provided data, etc. might be stipulated in some cases. In such case, the time of accrual and scope of the obligation to delete the data might be handled differently depending on the termination event (expiration of the contract term, termination by mutual consent, termination by the platform operator, etc.).

(ii) Claim for return of data

It is possible that data provider would require the platform operator to return all or part of the provided data upon its withdrawal from or termination of the platform business.

In this regard, unlike any case where the right to demand for return automatically arises based on ownership since data cannot be the subject of ownership as described in Part III-1, it is considered that the right to demand return of data would not automatically arise. Therefore, it is necessary to prescribe in advance in the terms of use as required whether or not data providers or the platform operator would be granted the right to demand return of data.

(iii) Data portability

Data portability means, mainly in relation to person related data, the right of that person to demand the platform operator to return the provided data in the format available in other platform or transfer the data provided by that person directly to another platform. It is considered that the same right might be claimed with respect to industrial data, in addition to person related data, in the future, so attention must be paid especially when there are overseas business operators included in the data providers.

For example, it is possible that, upon their termination of utilization of the platform, data providers demand the platform operator to return their provided data in the format used on another platform or transfer their provided data directly to another platform.

Therefore, in addition to the consideration on possible measure to be taken from the technical perspective, it may be necessary in some cases to consider whether to expressly prescribe in the terms of use whether the platform operator is required to comply with any such demands for return.
Draft model contract for data provision type contracts

Company [TBD] (the “Data Provider”) and Company [TBD] (the “Data Recipient”) enter into this agreement (this “Agreement”) as follows with respect to the provision of [TBD] data from the Data Provider to the Data Recipient.

Article 1 Definitions

In this Agreement, the following terms have the meanings set out below.

(i) “Provided Data” means data provided from the Data Provider to the Data Recipient pursuant to this Agreement and for which the Data Provider has utilization rights and the details of which are set forth in the Schedule; provided, however, that the Provided Data do not include any personal information under the Act on Protection of Personal Information.

(ii) “Purpose” means [TBD] by the Data Recipient.

(iii) “Derived Data” means data newly created through processing, analysis, editing, and integration, etc. of the Provided Data by the Data Recipient.

Points to Note:

- Define “provided data.”
- The details of the provided data such as subjects, items and number of cases of the provided data need to be identified. Identify the details of the provided data and other matters in schedules.
- Identify the purpose of contract (the purpose of providing data).
- Define “derived data” and other concepts with a wide range of interpretation.

Description:

1 In a data provision contract, it is important to clearly specify the details of the provided data such as subjects, items and number of cases of the provided data subject to the transaction in the contract. If the details of the provided data subject to the transaction have not been clearly specified, it is possible that the data recipient may only receive data that are different from those expected and thereby may not able to realize the business utilizing the provided data or achieve the purpose of the contract (the purpose of receiving data). In addition, if the details of the provided data subject to the transaction have not been clearly specified, the scope of obligation of confidentiality borne by the data recipient and the scope of provided data that require more prudent management would be unclear. Therefore, it is necessary to clearly specify the contents, etc. of the provided data subject to the transaction by the contract.

2 When specifying the details of the provided data subject to the transaction in the contract, since the contents of such provided data have to be clear for both parties, it is recommended, for example, to specify the subjects of the data (the outline of the provided data), items, quantity, granularity, updating frequency and other matters of the data.
VII Examples of Major Contractual Provisions

The provided data in the example provision above do not contain any personal information. However, in the case where personal information is included, it is desirable to at least establish the following provisions.

1. In the case that the Data Provider provides Provided Data containing personal information or anonymously processed information (“Personal Information, Etc.”) under the Act on Protection of Personal Information (the “Personal Information Act”) to the Data Recipient in effecting the Purpose, the Data Provider shall specify to that effect in advance.

2. In the case that the Data Provider provides Provided Data containing Personal Information, Etc. to the Data Recipient in effecting the Purpose, the Data Provider shall warrant that the proceedings under the Personal Information Act have been implemented with respect to the generation, acquisition, provision, etc. of the data.

3. The Data Recipient shall, if the Provided Data have been provided in accordance with Article 1, Paragraph 1, comply with the Personal Information Act and take any measures required for the management of the Personal Information, Etc.

Article 2 Method of Provision of Provided Data

The Data Provider shall provide the Provided Data to the Data Recipient by the method set forth in the Schedule during the effective period of this Agreement; provided, however, that the Data Provider may change the specifications and the method of provision in the Schedule by notifying the Data Recipient no later than [TBD] days prior to the data provision.

Points to Note:
- Form of provision of the provided data (paper or electronic file, and in the case of electronic file, the file format)
- Means of provision of the provided data (e-mail transmission, downloading from a server, grant of access right to a server or return of data recorded in recording media)
- Frequency of provision of the provided data

Description:
1. For smooth and stable data provision, it is desirable to agree in advance to the method of provision of the provided data and provide the provided data in accordance with the method of data provision so agreed. To this end, it is recommended, for example, to predetermine the form of provision of the provided data (paper or electronic file, and in the case of electronic file, the file format), the means of provision of the provided data (e-mail transmission, downloading from a server, grant of access right to a server or return of data recorded in recording media) and other matters. In addition, in the case of continuous data provision, it is also advisable to agree in advance to the frequency of provision of the provided data (“monthly,” “once in [TBD] months,” etc.).

2. Since it is possible that the method of provision of the provided data (the form, means and frequency of provision) would need to be changed due to a change in circumstances,
VII Examples of Major Contractual Provisions

it is conceivable to make it possible for the data provider to change the method of provision of the provided data by giving a prior notice to the data recipient.

Article 3 Permission for Utilization of Provided Data

<table>
<thead>
<tr>
<th>Article</th>
<th>Provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Data Provider shall permit the Data Recipient to utilize the Provided Data within the scope of the Purpose during the effective period of this Agreement.</td>
</tr>
<tr>
<td>2</td>
<td>The Data Recipient shall have no authority to disclose, correct the details of, add or delete, suspend the utilization of, erase or suspend the provision of, the Provided Data other than those expressly provided for in this Agreement.</td>
</tr>
<tr>
<td>3</td>
<td>The Data Recipient shall not process, analyze, edit, integrate or otherwise utilize the Provided Data for any purpose other than the Purpose or disclose, provide or divulge the Provided Data to any third party (in the case that the Data Recipient is a corporation, “third party” also includes its subsidiaries and affiliates) without prior written approval of the Data Provider.</td>
</tr>
<tr>
<td>4</td>
<td>Any intellectual property rights relating to the Provided Data (including, but not limited to, the rights relating to the database works) belong to the Data Provider, except for Provided Data the intellectual property rights of which belong to a third party.</td>
</tr>
</tbody>
</table>

Points to Note:
- Specify the category of data provision type contract (license, assignment or joint utilization)
- Prohibition of third party provision, etc.
- Prohibition of unintended utilization
- Prohibition of processing, analysis, editing, and integration, etc. of the provided data for any purpose other than the Purpose
- Owner of the intellectual property rights relating to the provided data

Description:
1 Upon providing provided data, it is necessary to clarify the category of data provision type contract. The example provision above applies in the case of permission of utilization of provided data. The example provision in the case that the category of data provision type contract is (i) assignment of provided data or (ii) joint utilization of provided data (mutual permission of utilization) are as described below. In the case of (i) assignment of provided data, as the data provider would lose all authorities relating to the provided data, including its status to control the utilization of the provided data, and therefore would not be able to restrict the manner of utilization of the provided data by the data recipient, the provision on prohibition of unintended utilization or prohibition of third party provision is not included.

2 In the case of permission of utilization of provided data, if the data recipient requests for exclusive utilization of the provided data, it is possible to specify that “(the Data Provider) shall permit (the Data Recipient) to exclusively utilize (the Provided Data)” in Article 3,
VII Examples of Major Contractual Provisions

Paragraph 1. In such case, it is desirable to also clarify whether or not to prohibit the utilization of the provided data by the data provider itself.

3 Article 3, Paragraph 3 prohibits unintended utilization of the provided data. By doing so, it would be able to prevent the provided data from being utilized against the intention of the data provider. It is advisable to clarify in the contract whether or not any subsidiaries, affiliates, etc. would be included in the scope of the “third party” who is prohibited to “disclose, provide or divulge” the provided data.

4 If the Revised Unfair Competition Prevention Act comes into effect and the provided data falls under the “limited provided data,” it would be able to receive civil remedies, including claim for damages, request for injunction and presumptive provision relating to damages, against any wrongful acquisition or use, etc. of such data. In order for any data to fall under such “limited provided data,” it is required to satisfy the requirement of “limited provision to outside parties,” and unlike “trade secrets,” which should be managed in confidence and utilized among the holders or disclosed to limited parties who have exceptionally executed confidentiality agreement, the data need to be contemplated by the data provider as being subject to selective provision to certain parties at their request. In order to procure the requirement of “limited provision to outside parties” and receive remedies against any act of unfair competition of the extreme bad faith type ((ii) of “Unfair competition activities regarding data” in III-2-(2) above) or any other type relating to “limited provided data,” it is desirable to establish a provision to prohibit third party provision in the data provision contract.

5 While provided data may be subject to intellectual property rights such as database copyright, trade secrets or design rights, it is confirmed in Article 3, Paragraph 4 that the owner of the intellectual property rights would not change in connection with the permission of utilization of the provided data.

[(i) In the case of assignment of provided data]

The Data Provider shall assign all authorities (including, but not limited to, the rights under Articles 27 and 28 of the Copyright Act) relating to the Provided Data to the Data Recipient.

[(ii) In the case of joint utilization (mutual permission of utilization) of provided data]

1 The Data Provider shall permit the Data Recipient to utilize the data retained by the Data Provider (the “Data Provider’s Data”), and the Data Recipient shall permit the Data Provider to utilize the data retained by the Data Recipient (the “Data Recipient’s Data”), only within the scope of the Purpose and during the effective period of this Agreement.

2 The Data Provider and the Data Recipient may not disclose, provide or divulge any data for which the other party has utilization rights to any third party or utilize such data for any purpose other than the Purpose without prior written approval of the other party.

Article 4 Consideration and Payment Conditions (* In the Case of Usage-Based Rate)

92
## VII  Examples of Major Contractual Provisions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Data Recipient shall pay a monthly fee of [TBD] yen per unit as set forth in the Schedule to the Data Provider as consideration for permission of utilization of the Provided Data.</td>
</tr>
<tr>
<td>2</td>
<td>The Data Provider shall aggregate the units utilized by the Data Recipient on the last day of each month and notify in writing (including electronic methods; the same applies hereinafter) the amount of consideration for the permission of utilization based on such units to the Data Recipient by the [TBD]th day of the immediately following month.</td>
</tr>
<tr>
<td>3</td>
<td>The Data Recipient shall, during the effective period of this Agreement, pay the amount set forth in Article 4, Paragraph 1 and any consumption tax and local consumption tax imposed thereon by transfer to the bank account designated by the Data Provider by the last day of the month in which the notice in Article 4, Paragraph 2 was received. The Data Recipient shall bear all transfer fees.</td>
</tr>
</tbody>
</table>

### Points to Note:
- Amount of consideration for the provided data and the calculation method thereof
- Payment method of consideration for the provided data

### Description:
1. The representative case examples of the amount of consideration for the provided data and the calculation methods thereof are (i) usage-based rate, (ii) fixed charge and (iii) sales distribution.

2. In the case of (i) usage-based rate, which is adopted in the example provision above, it is desirable to determine the units to be the basis for calculation of consideration in the contract. In particular, in the case of a contract which contemplates continuous data provision, it is convenient to adopt a method of determining the consideration for the provided data based on units. The units can be quantity of data, capacity of data, number of accounts, number of software licenses, number of API calls, etc. In the case of usage-based rate, as the value to be the grounds for calculation of consideration would be unclear for the Data Recipient, Article 4, Paragraph 2 in the example provision above makes the grounds for calculation of consideration clear by making the Data Provider notify the units utilized by the Data Recipient in writing.

3. The example provision in the case of (ii) fixed rate is as shown below. However, in the case of a monthly payment of a certain amount, a contract might be executed in the middle of a month in some cases, so it is possible to establish a provision regarding the calculation of consideration on a per diem basis.

4. The (iii) sales distribution case applies when the consideration for the provided data to be paid to the data provider changes according to the revenue earned by the business conducted by the data recipient utilizing the data. In such case, it is first necessary to clarify the scope of “business” which would be the basis for calculation of consideration for the provided data. Next, since it is necessary to secure the objectivity of the calculation of consideration for the provided data, the data recipient may be requested to submit materials indicating the grounds for calculation of consideration at the time of the payment of the consideration. It is also important to make such materials indicating the
VII  Examples of Major Contractual Provisions

grounds available to the data providers for review and inspection when the data provider has any doubt with respect to the contents of such materials.

[In the case of fixed charge]

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Data Recipient shall pay [TBD] yen per month as consideration for permission of utilization of the Provided Data by transfer to the bank account designated by the Data Provider by the last day of each month. The Data Recipient shall bear all transfer fees.</td>
</tr>
<tr>
<td>2</td>
<td>The consideration for permission of utilization of the Provided Data in Article 4, Paragraph 1 shall be calculated for a month starting from the first day to the last day of the same month, and if the period in which the Provided Data is available to the Data Recipient covers only part of the month, the consideration shall be calculated on a per diem basis for the period in which the Data Recipient utilized the Provided Data.</td>
</tr>
</tbody>
</table>

[In the case of sales distribution]

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Data Recipient shall, during the effective period of this Agreement, prepare a report regarding the amount of revenue earned by [TBD] and other matters designated by the Data Provider for each calculating period (April 1 to March 31 of the following year) and submit the report to the Data Provider within 15 days after the termination of the calculating period.</td>
</tr>
<tr>
<td>2</td>
<td>The Data Recipient shall pay [TBD]% of the amount of revenue earned by [TBD] by transfer to the bank account designated by the Data Provider as consideration for permission of utilization of the Provided Data by the last day of the month immediately following the month in which the report in Article 4, Paragraph 1 was submitted. The Data Recipient shall bear all transfer fees.</td>
</tr>
<tr>
<td>3</td>
<td>The Data Recipient shall prepare appropriate books with respect to the matters to be stated in the report in Article 4, Paragraph 1 and shall maintain and preserve such books during the effective period of this Agreement. The Data Provider or its agent may review and inspect such books as necessary.</td>
</tr>
<tr>
<td>4</td>
<td>The Data Provider shall not disclose or divulge to a third party any confidential matters of the Data Recipient obtained through the review and inspection of the books under Article 4, Paragraph 3. In addition, the Data Provider shall not utilize any confidential matters of the Data Recipient obtained through the review and inspection of the books for any purpose or use other than those set forth in Article 4, Paragraph 3 above.</td>
</tr>
</tbody>
</table>

Description:

It is necessary to determine the “amount of revenue earned by [TBD]” on a case-by-case basis to clarify the extensive scope of the amount. In doing so, it is necessary to have a perspective of how to specify the details and scope of the “service” stated herein, such as whether to limit such amount only to the revenue earned by the services utilizing the provided data and exclude any revenue earned by the services utilizing derived data, or include the revenue earned by the services utilizing the derived data.

Article 5  No Warranty regarding Provided Data

94
VII  Examples of Major Contractual Provisions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Data Provider represents and warrants that the Provided Data have been duly acquired in an appropriate manner.</td>
</tr>
<tr>
<td>2</td>
<td>The Data Provider does not warrant the accuracy, completeness, safety or effectiveness (compatibility to the Purpose) of the Provided Data or that the Provided Data do not infringe any intellectual property rights or other rights of a third party.</td>
</tr>
</tbody>
</table>

Points to Note:
- Warranty/no warranty regarding non-infringement of rights of third parties relating to the provided data
- Warranty/no warranty regarding the accuracy and completeness of the provided data
- Warranty/no warranty regarding the safety of the provided data (whether or not the provided data is infected with a virus)
- Warranty/no warranty regarding the effectiveness of the provided data (its compatibility to the Purpose)
- Warranty/no warranty regarding non-infringement of intellectual property rights of third parties relating to the provided data

Description:
1  Since the quality of the provided data described in the Points to Note above is likely to cause trouble, it is desirable to clarify in the contract whether or not the data provider would warrant the quality of the data.

2  While the data provider represents and warrants that the provided data have been duly acquired in an appropriate manner in the example provision above, it is possible to limit such representation and warranty by including the phrase “to the knowledge of the Data Provider.”

3  Although it is possible to make it an obligation of the data provider to make efforts to procure the accuracy, completeness, effectiveness, etc. of the provided data, it should be noted that even if it is an obligation to make efforts, it does not mean that default liability would not arise, and in the case where the data provider failed to make efforts to improve the quality of the provided data, such as irresponsibly providing the provided data when there was doubt regarding the accuracy, completeness, effectiveness, etc. thereof, default liability may arise. While the example provision above does not make the data provider responsible for warranting the quality of the provided data, it is possible that the data provider would bear responsibility to warrant all or part of the quality of the provided data taking into consideration the nature and details of the provided data, purpose of the contract, relationship of the contracting parties and other such matters.

Although the data provider does not warrant the safety of the provided data in the example provision above, it might cause direct damage to the systems, etc. of the data recipient if the safety of the provided data is not warranted. Therefore, it is often considered appropriate that the data provider warrants the safety of the provided data.

4  Even if it is provided for in the contract that the data provider would not warrant the accuracy, completeness, safety, effectiveness, etc. of the provided data, while such
VII Examples of Major Contractual Provisions

A provision can be considered effective in principle, it is considered that the data provider may not be able to be exempted from liability when the data provider provides data with quality problems due to its willful misconduct or gross negligence for the purpose of causing damage. Therefore, it is worth considering specifying to that effect in a proviso.

In the case that the data provider represents and warrants all or part of the matters regarding the quality of the data, a provision to limit the scope of the warranty liability (the scope within which the data provider bears an obligation to compensate for damage) to a certain maximum amount (for example, the amount of consideration received from the data recipient) might be established in some cases. While such provision would be considered effective in principle, it should be noted that in the case that the data provider has knowledge or is grossly negligent with respect to any quality problem in the provided data, the provision to limit the scope of the warranty liability of the data provider would become void, and the data provider may be made liable for any damage incurred by the data recipient that have an adequate causal relationship with the quality problem in the provided data.

Article 6 Limitation of Liability, Etc.

<table>
<thead>
<tr>
<th></th>
<th>The Data Provider shall not be liable for any claim, loss, damage or expense (including reasonable attorney fees) in relation to the utilization of the Provided Data by the Data Recipient or the utilization by the Data Recipient of any intellectual property rights relating to an invention, device, creation, trade secret, etc. generated based on the utilization of the Provided Data by the Data Recipient (including, but not limited to, patent infringement, design right infringement and any other similar infringement).</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>The Data Recipient shall, in the case that any dispute, claim or demand (“Dispute, Etc.”) with any third party arises from or in connection with the utilization of the Provided Data, promptly notify the Data Provider in writing and resolve such Dispute, Etc. at its own responsibility and expense. The Data Provider shall cooperate with the resolution of such Dispute, Etc. to a reasonable extent.</td>
</tr>
<tr>
<td>3</td>
<td>The Data Recipient shall, in the case that the Data Provider incurs any damage, loss or expense (including reasonable attorney fees; “Damage, Etc.”) arising from or in connection with the Dispute, Etc. set forth in Article 6, Paragraph 2 above (except in the case where such Dispute, Etc. is cause by any event attributable to the Data Provider), compensate the Data Provider for such Damage, Etc.</td>
</tr>
</tbody>
</table>

Points to Note:
- Responsibility to resolve disputes, etc. arising in relation to the provided data

Description:
1 Articles 6, Paragraphs 1 and 2 provide that the dispute, etc. arising in connection with the utilization of the provided data by the data recipient or the utilization by the data recipient of any intellectual property rights relating to an invention, device, creation, trade secret, etc. generated based on the utilization of the provided data by the data recipient shall be resolved at the expense and responsibility of the data recipient in principle. In addition,
VII Examples of Major Contractual Provisions

Article 6, Paragraph 3 obligates the data recipient to indemnify any damage incurred by the data provider in the dispute arising from or in connection with the provided data.

2 As another way to provide for this matter, it is also possible to make the data provider responsible for resolving disputes, etc. arising in relation to the utilization of the provided data in a form not breaching this Agreement. The specific details of such provision are as set out below. With respect to Article 6, Paragraph 1 below, the scope within which the data provider would be liable for damage, etc. may be limited to the amount of consideration received under Article 3.

[In the case that the Data Provider is responsible to resolve Dispute, Etc. in principle]

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any dispute, claim or demand (“Dispute, Etc.”) with a third party arising from or in relation to the utilization (limited to the utilization in a form not breaching this Agreement) of the Provided Data by the Data Recipient shall be resolved at the expense and responsibility of the Data Provider. In addition, the Data Provider shall, in the case that the Data Recipient incurs any damage, loss or expense (including reasonable attorney fees; “Damage, Etc.”) arising from or in connection with the Dispute, Etc., bear such Damage, Etc.</td>
</tr>
<tr>
<td>2</td>
<td>Notwithstanding Article 6, Paragraph 1 above, the Data Recipient shall resolve any Dispute, Etc. arising from or in connection with the utilization of the Provided Data in a form breaching this Agreement at its own expense and responsibility. In addition, if the Data Provider incurs any Damage, Etc. arising from or in connection with such Dispute, Etc., the Data Recipient shall bear such Damage, Etc.</td>
</tr>
</tbody>
</table>

Article 7 Status of Utilization

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Data Provider may request the Data Recipient to submit a report on the status of utilization which is necessary to verify whether or not the utilization of the Provided Data by the Data Provider conforms to the terms and conditions of this Agreement.</td>
</tr>
<tr>
<td>2</td>
<td>If the Data Provider determines that the report under Article 7, Paragraph 1 is not sufficient to verify the status of utilization of the Provided Data based on a reasonable basis, the Data Provider may carry out an audit of the status of utilization of the Provided Data by the DataRecipient at the business place of the Data Recipient once a year at the most upon [TBD] business days prior written notice. In such case, the Data Provider shall comply with the regulations regarding information security of the Data Recipient and other internal regulations separately established by the Data Recipient.</td>
</tr>
<tr>
<td>3</td>
<td>If, as a result of the audit in Article 7, Paragraph 2 above, it is discovered that the Data Recipient has utilized the Provided Data in breach of this Agreement, the Data Recipient shall pay expenses required for the audit and any additional consideration relating to the utilization of the Provided Data to the Data Provider.</td>
</tr>
</tbody>
</table>

Points to Note:
- Report and audit relating to the compliance with the terms and conditions of utilization of provided data
VII  Examples of Major Contractual Provisions

Description:

1. The data provider must be able to promptly confirm the status of utilization of the provided data by the data recipient if a divulgence or unintended utilization of the provided data by the data recipient is likely to occur or in similar circumstances.

2. As a means to confirm the status, the example provision above provides that the data provider may request a report on the status of utilization from the data recipient and, when the data provider reasonably determines that such report is not sufficient to verify the status of utilization of the provided data, it may audit the status of utilization of the provided data by the data recipient. In addition, if any breach of this Agreement by the data recipient is discovered by the audit, the data recipient is obliged to pay audit expenses and additional consideration.

3. There is a risk that trade secrets of the data user might become known to the data provider when the data provider carries out the audit of the status of utilization of the provided data by the data recipient. Therefore, it might be appropriate in some cases that a neutral third party who has executed a confidentiality agreement with the data provider and data recipient carries out the audit of the status of utilization of the provided data by the data recipient.

Article 8  Management of Provided Data

<table>
<thead>
<tr>
<th>Article 8 Management of Provided Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The Data Recipient shall manage and store the Provided Data with the due care of a good manager by clearly separating the Provided Data from any other information and take management measures of at least the same level as those taken for its own trade secrets by using appropriate management means.</td>
</tr>
<tr>
<td>2. The Data Provider may request the Data Recipient to submit a written report on the management status of the Provided Data at any time. In such case, if the Data Provider determines that the Provided Data is likely to be divulged or lost, the Data Provider may request the Data Recipient to rectify the method of management and storage of the Provided Data.</td>
</tr>
<tr>
<td>3. In the case that the request for report or rectification in Article 7, Paragraph 2 is made, the Data Recipient must promptly respond to such request.</td>
</tr>
</tbody>
</table>

Points to Note:

- Separate management of the provided data and duty of care of a good manager of the data recipient
- Request for report on the management status of the provided data and request for rectification of the management method of the provided data

Description:

1. Since it is necessary to prevent contamination of the provided data received from the data provider and other information held by the data recipient itself, the data recipient is obliged to manage and store the provided data received separately from other information. In order for any data to fall under “limited provided data” under the Revised Unfair Competition Prevention Act, it is required that the data had not been managed in
Examples of Major Contractual Provisions

1. As the data provider would not be able to know from outside whether the management of the provided data has been conducted appropriately by the data recipient in accordance with the contract, Article 8, Paragraph 2 specifies that the data provider may request the data recipient to submit a written report on the management status of the provided data. It also stipulates that, if the data provider determines that the provided data is likely to be divulged or lost based on the management status of the provided data by the data recipient, the data provider may request for rectification of the data management method, etc.

2. While Article 10 below provides for the details of obligation of confidentiality relating to the confidential information that are identified as confidential, the “providing data” is excluded from the “confidential information” under Article 10, and the data recipient bears an obligation to appropriately manage the “providing data” under Article 8 whether or not they are identified as confidential.

3. While this Agreement does not assume that the data recipient would disclose the provided data or make them available to any third party (also refer to Article 3, Paragraph 3), in the case that the data recipient is permitted to disclose the provided data or make them available to a third party (permitted recipient), it is conceivable to specify that the data recipient shall cause such third party to assume and comply with the equivalent obligations as those borne by the data recipient under this Agreement, and if the third party breaches such obligations, shall be directly liable to the data provider as if the breach was committed by the data recipient.

4. In the case that any know-how, etc. of the data provider included in the provided data is leaked, etc. due to breach of the data management obligation under this Article 8 or the provisions of Article 3, Paragraph 3 of this Agreement by the data recipient, the data provider may claim for damage caused by the breach of contract against the data recipient. However, as it may be difficult in some cases to calculate the amount of damage incurred by the data provider in relation to the leaks of know-how, etc., it is worth considering prescribing liquidated damages in the contract in advance. With respect to such liquidated damages, the parties determine upon agreement a reasonable amount which would serve as a deterrent for the for commitment of a breach of management obligation, etc. by the data recipient taking into consideration the importance and size of the provided data. However, it is construed that, if liquidated damages are set forth in the contract (even when the term “penalty” is used, it would be presumed to constitute liquidated damages (Article 420(3) of the Civil Code)), the data provider would not be able to claim for damages exceeding the liquidated damages unless the data provider verifies that it has been agreed that damages are not limited to the liquidated damages. Therefore, if the parties set forth liquidated damages or a penalty in the contract, they might also want to specify that if actual damages exceed the liquidated damages, the data provider may also claim for such excess.

[Reference: Example of a provision regarding penalty]

If the Data Provider incurs any damage due to divulgence, loss, third party provision or unintended utilization of the Provided Data or other utilization of the Provided Data in breach of this Agreement by the Data Recipient, the Data Recipient shall pay [TBD] yen to the Data Provider.

[Reference: Example of a provision regarding penalty]
VII Examples of Major Contractual Provisions

Provider as a penalty; provided, however, that if the amount of damage incurred by the Data Provider exceeds the amount of penalty above, the Data Provider may claim for such damage against the Data Recipient by verifying the actual amount of damage incurred.

Article 9 Duty to Mitigate Damage

1 The Data Recipient shall, when it discovers divulgence, loss, third party provision or unintended utilization of the Provided Data or other utilization of the Provided Data in breach of this Agreement (“Divulgence of Provided Data, Etc.”), promptly notify the Data Provider to that effect.

2 If Divulgence of Provided Data, Etc. occurs due to willful misconduct or gross negligence of the Data Recipient, the Data Recipient shall, at its own expense and responsibility, confirm whether or not the fact of the Divulgence of Provided Data, Etc. exists, and if the existence of the Divulgence of Provided Data, Etc. is confirmed, investigate the cause thereof and examine preventive measures and report the details thereof to the Data Provider.

Points to Note:
- Notification duty of the data recipient when divulgence, etc. of provided data is found
- Duty of data recipient to examine and report preventive measures, etc. upon occurrence of divulgence of provided data, etc.

Description:
As the damage arising from divulgence, loss, third party provision or unintended utilization of the provided data or other utilization of the data in breach of the contract might be exacerbated unless immediate and adequate measures are taken, the data provider also needs to promptly ascertain the situation of the data divulgence, etc. Therefore, Article 9, Paragraph 1 obligates the data recipient to immediately notify the data provider when it discovers any data divulgence, etc., and Article 9, Paragraph 2 obligates the data recipient to examine the investigation of the causes and preventative measures and report the details thereof to the data provider at its own expense and responsibility.

Article 10 Confidentiality

1 The Data Provider and the Data Recipient shall maintain strict confidentiality of any information acquired through this Agreement that the other party has disclosed upon identifying it as being confidential information, whether in writing, orally or any other form (“Confidential Information,” provided, however, that the Provided Data is not included in “Confidential Information” under this Article 10), and shall not disclose, provide or divulge the Confidential Information to any third party or utilize the Confidential Information for any purpose other than exercising the rights or performing the obligations under this Agreement without prior written approval of the other party; provided, however, that if a legally binding request for disclosure is made by any public agency, the receiving party may disclose the Confidential Information to the extent of
satisfying such request on the condition that it gives prompt notice to the disclosing party.

2 Notwithstanding Article 10, Paragraph 1 above, none of the following information is included in Confidential Information:
   (i) Information that was already in the possession of the receiving party at the time of disclosure;
   (ii) Information that was independently generated by the receiving party without relying on the Confidential Information;
   (iii) Information that was in the public domain at the time of disclosure;
   (iv) Information that entered the public domain through no fault of the receiving party; or
   (v) Information that was disclosed by a duly authorized third party without confidentiality obligations.

3 The receiving party may disclose the Confidential Information to its own officers or employees or its attorneys, accountants, tax accountants or other professionals who bear a duty of confidentiality under laws, only to the necessary extent to perform this Agreement and on the condition that the receiving party causes such persons to comply with the obligation of confidentiality under Article 10, Paragraph 1.

4 The obligation under this Article 10 shall remain effective for [TBD] years after the termination of this Agreement.

Points to Note:
- Definition of confidential information
- Details and exceptions of obligation of confidentiality
- Survival of obligation of confidentiality after termination of the contract

Description:
While Article 10, Paragraph 1 treats not only information provided in writing but also that provided orally or in any other form as “confidential information” as long as it is identified as such, there are cases where, in order to clarify the scope of the confidential information, it is set forth that “(information) identified as confidential in writing” falls under confidential information. Conversely, there are also cases where even any information not actively identified as confidential is broadly included in the definition of confidential information.

With respect to provided data, Article 3, Paragraph 3 prohibits the data recipient from disclosing or providing the provided data to any third party and Article 8, Paragraph 1 obligates the data recipient to manage and store the provided data with the due care of a good manager by clearly separating them from any other information. Therefore, the data recipient would be obliged to appropriately manage the provided data whether or not they are identified as confidential under Article 10, Paragraph 1.34

34 If an obligation of confidentiality imposed by a business operator in the superior bargaining position unjustly causes disadvantage to the other party of the transaction, this might be a problem under the Antimonopoly Act (Competition Policy Research Center, Fair Trade Commission of Japan, “Report by the
VII  Examples of Major Contractual Provisions

Article 11  Handling of Derived Data, Etc.

<In the case that the Data Provider does not have utilization rights to Derived Data or intellectual property rights arising from the Provided Data> [Version 1]

1 All utilization rights to Derived Data shall be retained only by the Data Recipient unless otherwise agreed by the parties.
2 Any intellectual property rights relating to an invention, device, creation, trade secret, etc. generated based on the utilization of the Provided Data by the Data Recipient belong to the Data Recipient.

<In the case that not only the Data Recipient but also the Data Provider has the utilization rights to Derived Data and intellectual property rights arising from the Provided Data> [Version 2]

1 The Data Recipient shall have the utilization rights to Derived Data and permit the Data Provider to utilize the Derived Data free of charge [for value] to the extent of [TBD] [to the extent of the purpose of [TBD]].
2 Any intellectual property rights relating to an invention, device, creation, trade secret, etc. generated based on the utilization of the Provided Data by the Data Recipient belong to the Data Recipient; provided, however, that the Data Recipient shall license such intellectual property rights to the Data Provider free of charge [for value].
3 The details of the terms and conditions of the permission of utilization from the Data Recipient to the Data Provider with respect to Derived Data and intellectual property rights relating to an invention, etc. generated based on the utilization of the Provided Data by the Data Recipient under Article 11, Paragraph 2 shall be determined upon separate consultation between the Data Provider and the Data Recipient.
4 If the Data Recipient earns revenue through business or services conducted by utilizing Derived Data, the Data Recipient shall pay [TBD]% of the revenue earned by the Data Recipient to the Data Provider. The terms and conditions of the payment shall be determined upon separate consultation between the Data Provider and the Data Recipient.

<In the case that the availability of the utilization rights to Derived Data and the owner of intellectual property rights will be determined upon consultation> [Version 3]

The availability of the utilization rights to Derived Data and the owner of intellectual property rights relating to an invention, device, creation, trade secret, etc. generated based on the utilization of the Provided Data by the Data Recipient shall be determined upon separate consultation between the Data Provider and the Data Recipient.

Points to Note:
- Availability of the utilization rights to derived data

Study Group to Discuss Human Resources and Competition Policy,”
http://www.jftc.go.jp/cprc/conference/index.files/180215jinzai01.pdf (February 15, 2018)).
Examples of Major Contractual Provisions

- Owner of intellectual property rights arising from the utilization of provided data by the data recipient
- Authorities of the data provider to utilize intellectual property rights arising from the utilization of provided data by the data recipient
- Distribution of profits obtained by the utilization of intellectual property rights arising from the utilization of derived data by data recipient

Description:

1. Since the availability and allocation of the utilization rights to derived data and the owner of the intellectual property rights arising from the utilization of the provided data by the data recipient would not be automatically determined under laws or clarified in an unambiguous manner, it is desirable to make such points clear in the contract.

2. With respect to derived data, Version 1 does not permit the data provider to utilize derived data. Version 2 permits the data provider to utilize derived data on a non-exclusive basis. It should be noted that, if the data provider receives an allocation of all rights (including, but not limited to, rights under Articles 27 and 28 of the Copyright Act) relating to derived data or the data provider is granted an exclusive license of derived data, this might fall under “unfair trade practices” under the Monopolization Prevention Act. In Version 3, the availability of the utilization rights to derived data is not specified in the contract but would be determined upon separate consultation.

3. The descriptions regarding derived data will also apply to the authorities of the data provider to utilize intellectual property rights arising from the utilization of the provided data by the data recipient.

4. As the data recipient would be able to freely utilize derived data if it has the utilization rights to the derived data, the act of the data recipient utilizing the derived data might not be in breach of the prohibition of unintended utilization imposed with respect to the provided data. Therefore, it is necessary to limit the utilization of the derived data by the contract if the data provider wishes to prohibit the free utilization of the derived data.

5. Article 11, Paragraph 4 in Version 2 provides that, if the data recipient earns revenue through business or services conducted by the data recipient utilizing derived data, the data recipient shall distribute a certain percentage of such revenue to the data provider. One aspect of establishing such provision is that it would make the economic benefits of the data provider’s providing its data clearer and thereby contribute to the market for data transactions.

Article 12 Effective Period

This Agreement shall be effective for [TBD] years after its execution; provided, however, that the period of this Agreement will be extended for [TBD] years under the same terms and conditions as those hereunder if the Data Provider or the Data Recipient does not notify the other party in writing of its intention to terminate this Agreement at least [TBD] months prior to the expiration of the effective period of this Agreement, and the same will apply thereafter.
VII Examples of Major Contractual Provisions

Article 13 Force Majeure

Neither the Data Provider nor the Data Recipient shall be liable for any delay in or failure of performance of all or part of this Agreement due to an act of providence, war, civil disturbance, insurrection, natural disaster, blackout, malfunction of communications facilities, suspension of provision or emergency maintenance of cloud services or other outsourcing services, revision or abrogation of laws and ordinances or any other event not attributable to the Data Provider or the Data Recipient during the effective period of this Agreement.

Points to Note:
- Designate blackout, malfunction of communications facilities or suspension of provision or emergency maintenance of cloud services or other outsourcing services as force majeure events

Description:
It is desirable to designate blackout, malfunction of communications facilities or suspension of provision or emergency maintenance of cloud services or other outsourcing services, etc. that might affect IT services as events of force majeure. However, potential force majeure events are not limited to the above, and the parties should flexibly prescribe the force majeure events according to the type of cloud services or other outsourcing services.

Article 14 Termination

(Omitted)

Article 15 Measures after Termination

1 The Data Recipient shall not utilize Provided Data for any reason after the termination of this Agreement and shall immediately destroy or delete all Provided Data already received (including reproductions thereof) in the manner separately designated by the Data Provider.
2 The Data Provider may request the Data Recipient to submit a written document certifying that all data have been destroyed or deleted.

Points to Note:
- Destruction or deletion of provided data after termination of the contract
- Submission of a certification of destruction or deletion of provided data

Description:
Since it is difficult for the data provider to confirm from outside that the provided data have been destroyed or deleted, it is provided that the data provider may request the data recipient to submit a written document certifying that the provided data have been deleted.
VII Examples of Major Contractual Provisions

Article 16 Elimination of Antisocial Forces
(Omitted)

Article 17 Surviving Provisions

| Article 3, Paragraphs 2 and 3 (Obligations of Data Recipient), Article 6 (Limitation of Liability, Etc.), Article 10 (Confidentiality), Article 11 (Handling of Derived Data, Etc.), Article 14 (Termination), Article 15 (Measures after Termination), Article 16 (Elimination of Antisocial Forces), Article 17 (Survival), Article 18 (Prohibition of Assignment of Rights and Obligations), 20 (Governing Law) and Article 21 (Dispute Resolution) shall remain effective after the termination of this Agreement. |

Article 18 Prohibition of Assignment of Rights and Obligations
(Omitted)

Article 19 Entire Agreement
(Omitted)

Article 20 Governing Law
(Omitted)

Article 21 Dispute Resolution
(Omitted)
VII Examples of Major Contractual Provisions

Schedule

1 Details of the Provided Data

<table>
<thead>
<tr>
<th></th>
<th>Subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Data of [TBD] relating to [TBD]</td>
</tr>
<tr>
<td>(2)</td>
<td>Items</td>
</tr>
<tr>
<td>(3)</td>
<td>Number of cases and units</td>
</tr>
<tr>
<td></td>
<td>A unit of the Provided Data shall be [TBD] cases</td>
</tr>
<tr>
<td>(4)</td>
<td>Frequency of updating of data</td>
</tr>
<tr>
<td></td>
<td>The Data Provider shall update data several times in a year</td>
</tr>
<tr>
<td>(5)</td>
<td>Others</td>
</tr>
</tbody>
</table>

2 Method of provision of the Provided Data

The Data Provider shall provide data by a method in which it uploads an electronic file in (file format) to the Data Provider’s server, and the Data Recipient downloads such electronic file from the server from time to time during the effective period of this Agreement.
VII  Examples of Major Contractual Provisions

2  Draft model contract for data generation type contracts

Company [TBD] (the “Data Provider”) and Company [TBD] (the “Data Recipient”) enter into this agreement (this “Agreement”) as follows with respect to the data generated, acquired or collected in a business jointly conducted by the Data Provider and the Data Recipient.

Article 1  Definitions

In this Agreement, the following terms have the meanings set out below.

(i)  “Business” means [TBD] conducted between the Data Provider and the Data Recipient.
(ii) “Applicable Data” means data generated, acquired or collected based on the Business.
(iii) “Processing, Etc.” means processing, analysis, editing, and integration, etc. of Applicable Data, and “Derived Data” means data acquired through such Processing, Etc.

Points to Note:

- Article 1 defines the terms used in the contract.

Description:

1  As data have no clear outer edge, it is not generally easy to clarify the scope of applicable data. It is desirable to identify the scope of “applicable data” to the extent possible by presenting sample data, etc. in an easy-to-understand form or in any other manner as necessary. For example, it is conceivable to separately define “sensors, etc.” which collect applicable data and “devices, etc.” in which such sensors, etc. are placed, and specify the applicable data as data acquired by such sensors, etc. from such devices, etc. or otherwise.

2 The example provision above does not limit the scope of “applicable data” based on the nature of the data, but it is possible to exclude certain data containing personal information from the definition of “applicable data” and have them governed by other provisions.

Article 2  Allocation of Data Utilization Rights

1  The details of the utilization rights to Applicable Data shall be determined for each type of the Applicable Data respectively in Schedule A.

[Version 1]
2  [The Data Provider or the Data Recipient] shall have all utilization rights to the Applicable Data not stated in Schedule A, including utilization, disclosure, assignment (including permission of utilization) and disposal of such data.

[Version 2]
2  The utilization rights to the Applicable Data not stated in Schedule A shall be separately determined upon agreement between the parties.
VII Examples of Major Contractual Provisions

3 The Data Provider and the Data Recipient may not utilize, disclose, assign (including permission of utilization) or dispose of Applicable Data beyond the scope of the utilization rights to such data approved for each party under Article 2, Paragraph 2 above and Schedule A.

Schedule A Utilization Rights to Applicable Data (In Relation to Article 2)

<table>
<thead>
<tr>
<th>Data name</th>
<th>Data item</th>
<th>Period</th>
<th>Utilization rights of the Data Provider</th>
<th>Utilization rights of the Data Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 [TBD]</td>
<td>[Name of the devices and sensors and other information sufficient to identify the data]</td>
<td>Data acquired during the period [from [TBD], 2018 to [TBD], 2019]</td>
<td>[Purpose of utilization] [Possibility of third party provision (assignment or permission of utilization)] [Possibility of Processing, Etc.]</td>
<td>[Purpose of utilization] [Possibility of third party provision (assignment or permission of utilization)] [Possibility of Processing, Etc.]</td>
</tr>
</tbody>
</table>

Points to Note:
- This Article provides for the utilization rights to applicable data.
- Identify the data by stating the name of devices and sensors, data acquisition period, etc. for each data. Then, specify the utilization rights allocated to the data provider and the data recipient with respect to data acquisition time, purpose of utilization, possibility of third party provision and possibility of the processing, etc. for each data.

Description:
1 With respect to the determination of the utilization rights, it is possible to adopt a method to classify applicable data into (i) data for which only the data provider has utilization rights (data utilized by data provider), (ii) data for which only the data recipient has utilization rights (data utilized by data recipient) and (iii) data for which both the data provider and the data recipient have utilization rights (data utilized by data provider and data recipient), and allocate the same authorities by each type. However, the example provision above adopts a method to determine the authorities by each individual data. In the case that only the Data Provider has the authorities, put “no utilization rights” or the like in the “Utilization rights of the Data Recipient” column.

2 With respect to any data which accrue continuously on a real-time basis, clarify the objective period in which such data will be acquired. If the end of the objective period is not to be established, it is conceivable to specify that the period would end upon termination of the contract.
VII  Examples of Major Contractual Provisions

3  The purpose of utilization would determine the scope of utilization of Applicable Data and it should be able to procure the confidentiality of the data. On the other hand, however, attention must be paid not to interfere with any business utilizing the data by excessively narrowing the purpose of utilization. Specifically, it is conceivable to set forth the purpose of utilization as “provision of services from the Data Provider to the Data Recipient in the Business,” “development of new products by the Data Recipient” or the like.

4  Since the value of data is often created only through processing, analysis, etc. thereof, it is considered reasonable not to limit the development or use of new analysis methods. The example provision above therefore does not limit the processing methods, but it is possible to only approve processing by a certain method in order to prevent any utilization in a manner that had not been expected by the parties.

In addition, it can be considered reasonable to make a prior agreement between the parties as to the specific analysis method in the cases where anonymously processed information or statistical information would be created with respect to personal information or industrial data would be processed so that no trade secret, etc. can be conjectured therefrom.

5  With respect to third party provision, while it is possible to simply designate it as “possible” and leave the determination of the terms and conditions of contract relating to third party provision of applicable data to the discretion of the party to which the utilization rights to such data is allocated, it is also possible to prescribe in advance the terms and conditions of the data provision (consideration, limitation of purpose of utilization, prohibition of provision to competitive business operators, etc.) between the parties, or otherwise permit the third party provision only when the other party gives its consent.

However, in the case where the data recipient collects data from a number of people including consumers and business partners and provides the aggregation of such data to any third party, it is considered reasonable to enable the data recipient to determine the terms and conditions of the provision only at its discretion since it is difficult to obtain consent individually from consumers, etc. Even in such case, attention must be paid to personal information and privacy rights of the consumers, etc. and trade secrets of the business partners, and it is advisable to prescribe in advance certain terms and conditions such as limiting the utilization by any third party to which the data would be provided or making the data subject to statistical processing before the provision.

6  Article 2, Paragraph 2 provides for the utilization rights that are not provided for in Schedule A. In Version 1 which allocates the utilization rights to either of the parties, the party would have general utilization rights to the data. In Version 2 which makes the parties determine the utilization rights upon separate agreement, the utilization rights would be determined for each individual data item upon consultation based on the specific utilization method and other matters between the parties.

7  Although the example provision above does not have any express provision regarding intellectual property rights relating to applicable data, it is conceivable to classify the intellectual property rights into those (i) which belong to the data provider, (ii) which belong to the data recipient, or (iii) which are shared by the data provider and the data recipient, as is the case in the utilization rights. In such case, the parties may be made unable to restrict the other party’s utilization rights to applicable data or derived data
VII Examples of Major Contractual Provisions

based on its intellectual property rights to the applicable data. In addition, in order to prevent the complication of rights and authorities and destabilization of legal status of the other party, it is also conceivable to impose the condition that the party who holds intellectual property rights may not assign such intellectual property rights to any third party.

Article 3 Data Processing, Etc. and Utilization Rights for Derived Data

[Version 1]
1 The provisions regarding the utilization rights to Applicable Data subject to Processing, Etc. shall apply mutatis mutandis to the utilization rights to Derived Data acquired through the Processing, Etc. conducted under the utilization rights to the Applicable Data set forth in Article 2.

[Version 2]
1 The utilization rights to Derived Data acquired through Processing, Etc. conducted under the utilization rights to Applicable Data set forth in Article 2 shall be specified by each type of the Applicable Data respectively in Schedule B; provided, however, that any utilization rights to any Derived Data not specifically stated in Schedule B shall be determined upon separate agreement between the parties.
2 The Data Provider and the Data Recipient may not utilize, disclose, assign (including permission of utilization) or dispose of Derived Data beyond the scope of the utilization rights to such data approved for each party under Article 3, Paragraph 1 and Schedule B.

Schedule B Utilization Rights to Derived Data (In Relation to Article 3)

<table>
<thead>
<tr>
<th>Data name</th>
<th>Data item</th>
<th>Period</th>
<th>Utilization rights of the Data Provider</th>
<th>Utilization rights of the Data Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>[TBD]</td>
<td>[TBD]/ [TBD] and [TBD]</td>
<td>Data acquired during the period [from [TBD], 2018 to [TBD], 2019] of [TBD]</td>
<td>[Purpose of utilization] [Possibility of third party provision (assignment or permission of utilization)] [Possibility of Processing, Etc.]</td>
<td></td>
</tr>
</tbody>
</table>

Points to Note:
- This Article provides for the utilization rights to derived data acquired through the processing, etc. of the applicable data by each party.
VII Examples of Major Contractual Provisions

Description:

1. It is not uncommon for parties to be unable to predict what kind of derived data would be generated and what kind of economic value would arise at the time of the execution of the contract. Therefore, Version 1 presents a method of conforming to the utilization rights to applicable data subject to processing, etc., and Version 2 presents a method of setting forth the utilization rights to derived data that are assumed to be generated by the same method as those of applicable data and determining the utilization rights to other derived data by separate agreement between the parties.

2. Since it is also often not clear how to determine the terms and conditions with respect to third party provision of derived data, it is conceivable to just state “as separately agreed by the parties” or the like.

3. Although the example provision above does not include any express provision regarding intellectual property rights relating to derived data, it is conceivable to classify the intellectual property rights into those (i) which belong to the data provider, (ii) which belong to the data recipient, or (iii) which are shared by the data provider and the data recipient, as is the case in the utilization rights. In such case, the parties may be made unable to restrict the other party’s utilization rights to applicable data or derived data based on its intellectual property rights to the derived data. In addition, in order to prevent the complication of rights and authorities and destabilization of legal status of the other party, it is also conceivable to impose the condition that the party who holds intellectual property rights may not assign such intellectual property rights to any third party.

Article 4 No Warranty regarding Applicable Data and Derived Data

<table>
<thead>
<tr>
<th></th>
<th>The Data Provider and the Data Recipient do not warrant to the other party the accuracy, completeness, safety or effectiveness (compatibility to the Purpose) of the data for which the other party has utilization rights under this Agreement (the “Data Accessible by the Counterparty”) or that the Data Accessible by the Counterparty do not infringe any intellectual property rights or other rights of a third party.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Data Provider and the Data Recipient do not warrant to the other party that the Data Accessible by the Counterparty will be certainly generated.</td>
</tr>
</tbody>
</table>

Article 5 Handling of Personal Information

<table>
<thead>
<tr>
<th></th>
<th>The Data Provider and the Data Recipient shall, in the case that Applicable Data contain any personal information or anonymously processed information (“Personal Information, Etc.”) under the Act on Protection of Personal Information (the “Personal Information Act”), expressly indicate to that effect in advance to the other party in accordance with the classification set forth in Schedule C.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Data Provider and the Data Recipient shall warrant that the proceedings under the Personal Information Act have been implemented with respect to the generation, acquisition, provision, etc. of Applicable Data in accordance with the classification set forth in Schedule C.</td>
</tr>
</tbody>
</table>
VII  Examples of Major Contractual Provisions

3  The Data Provider and the Data Recipient shall comply with the Personal Information Act and take necessary measures for the management of Personal Information, Etc. if any Applicable Data is provided pursuant to Article 5, Paragraph 1 above.

Schedule C  Proceedings to be Implemented by Each Party with respect to Personal Information (In Relation to Article 5)

<table>
<thead>
<tr>
<th>Data name</th>
<th>Party who makes the express indication under Article 5, Paragraph 1 and the warranty under Article 5, Paragraph 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Personal information relating to the Data Provider’s employees</td>
<td>Data Provider</td>
</tr>
<tr>
<td>2 Personal information relating to the Data Recipient’s customers</td>
<td>Data Recipient</td>
</tr>
</tbody>
</table>

Points to Note:
- This Article provides for warranty/no warranty regarding applicable data and derived data.
- This Article provides for warranty/no warranty regarding the continuous generation of applicable data.
- This Article provides that, if the applicable data contains personal information, the parties should warrant to the other party that the proceedings under the Act of Protection of Personal Information Act, including obtaining the principal’s consent to third party provision, have been implemented.

Description:
1  While this Article sets forth the availability of warranty regarding data, with respect to data generation, a utilization right is not something to acquire through permission of utilization by the other party but it is a right to freely utilize the data to the extent agreed between the parties. Therefore, each party would be respectively liable for any damage arising from data utilization, etc. or incurred as a result of infringement of third party rights (intellectual property rights, privacy rights, moral rights, etc.) in principle. However, if either party knew or did not know due to gross negligence that the data lacks accuracy, etc., the provision to limit the warranty liability might become void. It may be appropriate to clarify this matter in the provision.

Although Article 4, Paragraph 1 specifies that the safety of the data accessible by the counterparty would not be warranted, it might cause direct damage to systems, etc. if the safety of the data accessible by the counterparty is not warranted. Therefore, it may often be appropriate to warrant the safety of the data accessible by the counterparty.

2  However, in the case that any applicable data contain personal information or other information relating to any individual, it is desirable to make the parties bear such warranty liability as set forth in Article 5. Pursuant to such warranty clause, if the party who is mainly in charge of collecting applicable data (for example, if the applicable data consist of employee data of either party, the party to which such employees belong) fails to perform the procedures required by the Act of Protection of Personal Information
Examples of Major Contractual Provisions

(notification or publication of the purpose of utilization, obtaining consent for third party provision, performance of confirmation and recording obligation, etc.), such party shall be liable to the other party under the contract.

While data is not necessarily generated on a continuous basis, it is desirable to prescribe a warranty/no warranty regarding continuous generation if data utilization is assumed. In the case of operation data, etc. of machine tools, the operation data might not be generated depending on the order situation, etc. of the products manufactured utilizing such machine tools, and as it is not reasonable to make the user side of the machine tools liable in such case, continuous generation would not be warranted in principle. However, even in such case, if a party willfully takes off the sensors or leaves any failure in the sensors due to gross negligence, the provision to limit the warranty responsibility might become void, and it may be appropriate to clarify this matter in the provision.

Article 6  Consideration for Allocation of Data Utilization Rights

The Data Provider and the Data Recipient shall not have right to claim for expenses for assignment, consideration for permission of utilization and other consideration against the other party with respect to the allocation of utilization rights to Applicable Data and Derived Data to the other party pursuant to Articles 2 and 3.

Article 7  Distribution of Profits

Notwithstanding Article 6, if the Data Recipient provides Applicable Data or Derived Data to a third party and receives consideration therefor from such third party pursuant to Articles 2 and 3, the Data Recipient shall pay [TBD]% [of the assignment fee or license fee] as a distribution of [assignment fee or consideration for permission of utilization of data] to the Data Provider.

Article 8  Payment of Contribution

The Data Provider shall pay the amount of money separately determined by the Data Provider and Data Recipient upon consultation as a contribution of [data storage costs] to the Data Recipient.

Points to Note:
- This Article provides for the method of distribution of the profits to be obtained from third party provision of data, etc. and expenses relating to data storage, etc.

Description:
1 The parties would not only utilize data by themselves but they would also provide data to gain profits in some cases. In such case, it is necessary to specify how to distribute the profits and expenses between the parties.

2 As a profit distribution method, the example provision above presents a model of distributing the consideration obtained by providing applicable data or derived data to
Examples of Major Contractual Provisions

VII

third party. However, there might be a profit model in which the data recipient creates an analysis model (sales forecast model, accident frequency forecast model, etc.) utilizing data generated by the data recipient and provides such analysis model to third party by ASP service or any other method. In such case, it is conceivable to adopt a method of distributing a certain percentage of the profits gained from such analysis model to the data provider. In addition, it is also possible to take a method by which the data recipient pays a fixed charge to the data provider regardless of the sales, etc. on the assumption that the data recipient assumes the risks and returns of the profit model.

3 It is also conceivable that, on the condition that the data provider approves that the data recipient has utilization rights to applicable data generated, the data recipient provides derivative products (including consulting services) created based on such applicable data to the data provider. In such case, it would be provided for that the data provider would receive such advantage instead of money.

Article 9 Measures in Case Data Utilization is Restricted by Right of Third Party

The Data Provider and the Data Recipient shall, when it is discovered that the Data Accessible by the Counterparty contain data subject to intellectual property rights of a third party or the utilization of such data by the other party might otherwise be restricted, cooperate with each other to obtain permission from the third party, take measures to eliminate such data or otherwise make efforts to make it possible for either party to exercise the utilization rights to the data upon immediate consultation between the parties.

Points to Note:
- This Article applies in the case where utilization of data is restricted due to attachment of third party rights, etc.

Description:
1 In the case that the data accessible by the counterparty contain intellectual property rights of a third party, etc. or in any other similar case, the utilization of such data might be restricted when any necessary permission, consent, etc. has not been obtained upon utilizing such data. The example provision above obligates the parties to make efforts to take measures against such issue.

2 In particular, Article 9 is considered to be applicable in the following cases.
- In the case that data subject to third party right is included:
  Pattern A In the case that a third party other than the contracting parties is involved in the data generation
  Pattern B In the case that a third party other than the contracting parties is involved in the provision of machines
  Pattern C In the case that the analysis algorithm has been provided by a third party other than the contracting parties
### Article 10  Data Management

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Data Provider and Data Recipient shall manage and store the Data Accessible by the Counterparty with the due care of a good manager by clearly separating the Data Accessible by the Counterparty from any other information and take management measures at least the same level as those taken for its own trade secret by using appropriate management means.</td>
</tr>
<tr>
<td>2</td>
<td>The Data Provider and the Data Recipient may request the other party to submit a written report (including electronic manner; the same applies hereinafter) on the management status of the Data Accessible by the Counterparty at any time. In such case, if the Data Provider or the Data Recipient determines that the Data Accessible by the Counterparty is likely to be divulged or lost, the Data Provider or the Data Recipient may request the other party to rectify the method of management and storage of the Data Accessible by the Counterparty.</td>
</tr>
<tr>
<td>3</td>
<td>In the case that the request for report or rectification in Article 10, Paragraph 2 is made, the party who received such request must promptly respond to such request.</td>
</tr>
<tr>
<td>4</td>
<td>The Data Provider and the Data Recipient shall, when providing the Data Accessible by the Counterparty to any third party pursuant to Article 2 or 3, make such third party bear the same obligations as those borne by itself under this Article by executing a confidentiality agreement with such third party or in any other manner.</td>
</tr>
</tbody>
</table>

### Article 11  Confidentiality

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Data Provider and the Data Recipient shall maintain strict confidentiality of any information acquired through this Agreement that the other party has disclosed upon identifying it as being confidential information, whether in writing, orally or any other form (“Confidential Information”; provided, however, that the Data Accessible by the Counterparty is not included in “Confidential Information” under this Article 11), and shall not disclose, provide or divulge the Confidential Information to any third party or utilize the Confidential Information for any purpose other than exercising the rights or performing the obligations under this Agreement without prior written approval of the other party; provided, however, that if a legally binding request for disclosure is made by any public agency, the receiving party may disclose the Confidential Information to the extent of satisfying such request on the condition that it gives prompt notice to the disclosing party.</td>
</tr>
</tbody>
</table>
| 2         | Notwithstanding Article 10, Paragraph 1 above, none of the following information is included in Confidential Information:  
(i) Information that was already in the possession of the receiving party at the time of disclosure;  
(ii) Information that was independently generated by the receiving party without relying on the Confidential Information;  
(iii) Information that was in the public domain at the time of disclosure;  
(iv) Information that entered the public domain through no fault of the receiving party; or  
(v) Information that was disclosed by a duly authorized third party without confidentiality obligations. |
| 3         | The receiving party may disclose the Confidential Information to its own officers or employees or its attorneys, accountants, tax accountants or other professionals who bear a duty of confidentiality under laws, only to the necessary extent to perform this... |
VII Examples of Major Contractual Provisions

<table>
<thead>
<tr>
<th>Agreement and on the condition that the receiving party causes such persons comply with the obligation of confidentiality under Article 10, Paragraph 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 The obligation under this Article 11 shall remain effective for [TBD] years after the termination of this Agreement.</td>
</tr>
</tbody>
</table>

Points to Note:
- This Article sets forth the obligation to perform safety control and the obligation of confidentiality with respect to the data accessible by the counterparty

Description:

1 This Article sets forth the obligation to perform safety management and the obligation of confidentiality with respect to the data accessible by the counterparty, and it is assumed that any data for which only one party has utilization rights would be managed at such party’s responsibility. The “data accessible by the counterparty” are excluded from the “confidential information” subject to the obligation of confidentiality under Article 11, and each party would be obliged to appropriately manage the “data accessible by the counterparty” pursuant to the provisions of Article 10 whether or not they are identified as confidential. In addition, regardless of the provision regarding the effective period of the obligation of confidentiality under Article 11, the management obligation of each party relating to the data accessible by the counterparty would remain effective as long as the party retains such data accessible by the counterparty (refer to Article 16, Paragraph 2).

2 While Article 11, Paragraph 1 treats not only information provided in writing but also that provided orally or in any other form as “confidential information” as long as it is identified as such, there are cases where, in order to clarify the scope of the confidential information, it is set forth that “(information) identified as confidential in writing” falls under confidential information. Conversely, there are also cases where even any information not actively identified as confidential are broadly included in the definition of confidential information.

3 With respect to safety control measures, it is required to take measures at an appropriate level based on the nature, risk, etc. of the data. In particular, if the data may contain any personal information, it is necessary to take into consideration the safety management in accordance with the Act on Protection of Personal Information, etc., and it is required to comply with the guidelines, etc. of the Personal Information Protection Commission.

4 When providing data to a third party, it is reasonable to make such party bear the same obligations as those borne by the party itself.

5 In the case that leaks, etc. of the data accessible by the counterparty occurs due to breach of the data management obligation under this Article 11 or provisions of Articles 2.3 and 3.2 by the data provider or the data recipient, the party whose data was leaked, etc. may claim for damage caused by the breach of contract against the party who committed such leaks, etc. However, as it is difficult to calculate the amount of damage incurred by the party in connection with the data leaks, etc., it is worth considering prescribing liquidated damages in the contract in advance. See Item 5 of the Description of Article 8 in the
VII Examples of Major Contractual Provisions

draft model contract for the data provision type contracts for the matters to be noted when drafting the provisions and specific examples of the provisions.

6 It is required that data that has not been managed in confidence falls under “limited provided data” under the Revised Unfair Competition Prevention Act, so if handling the data accessible by the counterparty as “limited provided data,” it is assumed that Article 10, Paragraph 1 will include a statement such as “the Data Provider and the Data Recipient shall manage and store the Data Accessible by the Counterparty with the due care of a good manager by clearly separating the Data Accessible by the Counterparty from any other information,” and that the phrase “by executing confidentiality agreement with such third party or any other manner” will be deleted from Article 10, Paragraph 4.

Article 12 Change of Scope of Applicable Data

1 The Data Provider and the Data Recipient may, when either party comes to know that new data the generation, acquisition or collection of which could not have been assumed at the time of execution of this Agreement can be generated, acquired or collected and requests for utilization of such data, notify the other party to that effect and request to change the scope of the Applicable Data.

2 The Data Provider and the Data Recipient shall, when either party receives the notification under Article 12, Paragraph 1 above, separately consult with each other as to whether or not it is necessary to change the scope of Applicable Data, and if it is decided to be necessary, change the scope of Applicable Data and determine the allocation of utilization rights to Applicable Data in accordance with the proceedings agreed by the Data Provider and the Data Recipient.

Points to Note:
- This Article provides for the proceedings to take when changing the scope of applicable data for which the party has utilization rights.

Description:
In the example provision, applicable data is defined as “data generated, acquired or collected based on the Business,” and as a certain method to identify specific applicable data, it defines “sensors, etc.” and “devices, etc.” and presents the example of a method to designate the data acquired by the sensors, etc. from the devices, etc. as applicable data (see Article 1). In actual transactions, there is a considerable possibility that data that could not have anticipated at the time of execution of the contract may be generated, acquired or collected due to performance improvements of the sensors or other such reasons. Accordingly, it is necessary to predetermine additional proceedings to make such data the subject of utilization rights in such case. The example provision requires an agreement of the parties to change the scope of applicable data and determine the allocation of utilization rights to such applicable data.

Article 13 Effective Period

This Agreement shall be effective for [TBD] years after its execution; provided, however, that the period of this Agreement will be extended for [TBD] years under the same terms and
VII Examples of Major Contractual Provisions

conditions as those hereunder if the Data Provider or the Data Recipient does not notify the other party in writing of its intention to terminate this Agreement at least [TBD] months prior to the expiration of the effective period of this Agreement, and the same will apply thereafter.

Article 14 Force Majeure

Neither the Data Provider nor the Data Recipient shall be liable for any delay in or failure of performance of all or part of this Agreement due to an act of providence, war, civil disturbance, insurrection, natural disaster, blackout, malfunction of communications facilities, suspension of provision or emergency maintenance of cloud services or other outsourcing services, revision or abrogation of laws and ordinances or any other event not attributable to the Data Provider or the Data Recipient during the effective period of this Agreement.

Points to Note:
- Designate blackout, malfunction of communications facilities or suspension of provision or emergency maintenance of cloud services or other outsourcing services as force majeure events

Description:
It is desirable to designate blackout, malfunction of communications facilities or suspension of provision or emergency maintenance of services, etc. that might affect IT services as events of force majeure. However, potential force majeure events are not limited to the above, and the parties should flexibly prescribe force majeure events according to the type of cloud services or other outsourcing services.

Article 15 Termination
(Omitted)

Article 16 Handling of Data upon Termination

1 The Data Provider and the Data Recipient shall, upon termination of this Agreement, immediately destroy or delete data that are expressly specified to be destroyed or deleted upon termination of this Agreement in Schedule D in accordance with the procedures separately determined by the Data Provider and the Data Recipient.

2 The Data Provider and the Data Recipient shall have the utilization rights to Applicable Data and Derived Data other than those for which the parties bear an obligation to destroy or delete under Article 16, Paragraph 1 above, and shall utilize them in accordance with Article 2, Article 3 and Article 10, Paragraphs 1 and 4.

Schedule D Data to be Destroyed or Deleted upon Termination of this Agreement (In Relation to Article 16)
VII Examples of Major Contractual Provisions
(Omitted)

Points to Note:
- Predetermine the rules for destruction, deletion, etc. of data when they are required to be destroyed or deleted after termination of the contract. Provide for the preparation of evidence of the destruction or deletion as necessary.

Description:
It is possible to specify that each party may, after the termination of the contract and at its discretion, continue to utilize, and voluntarily dispose of, the data for which it has had the utilization rights. However, it would not necessarily be unreasonable to limit some data to be utilized only during the effective period of the contract (data relating to maintenance and operation of machines, etc.). The example provision assumes such cases, and identifies the data which are required to be destroyed or deleted upon termination of the contract and requires the destruction and deletion of such data only.

The example provision lists data to be destroyed or deleted and specifies that the parties continue to have utilization rights to other applicable data and derived data even after the termination of this Agreement. Conversely, if it is difficult to list the data to be destroyed or deleted, it may be appropriate to list the data for which the parties will continue to have utilization rights after the termination of the contract and require other applicable data and derived data to be destroyed or deleted after the termination of the contract.

Article 17 Elimination of Antisocial Forces
(Omitted)

Article 18 Survival

| Articles 9 (Measures in Case Data Utilization is Restricted by Right of Third Party), 11 (Confidentiality), 15 (Termination), 16 (Handling of Data upon Termination), 17 (Elimination of Antisocial Forces), 18 (Survival), 19 (Assignment), 21 (Governing Law) and 22 (Dispute Resolution) shall remain effective after the termination of this Agreement. |

Article 19 Assignment
(Omitted)

Article 20 Entire Agreement
(Omitted)

Article 21 Governing Law
(Omitted)
VII Examples of Major Contractual Provisions

Article 22 Dispute Resolution
(Omitted)
Information Economy Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry

The Data Team within the AI and Data Contract Guidelines Review Working Group consists of the following members:

- Atsushi Okada, attorney (leader)
- Masami Akutsu, attorney
- Makoto Uchida, attorney
- Ryosuke Ojiro, attorney
- Chiaki Satou, associate professor
- Keiji Tonomura, attorney
- Takashi Nakazaki, attorney