経済産業省
Ministry of Economy, Trade and Industry

Guidance for DATA Utilization

SOCIETY 5.0

Let's create new value through appropriate data utilization!

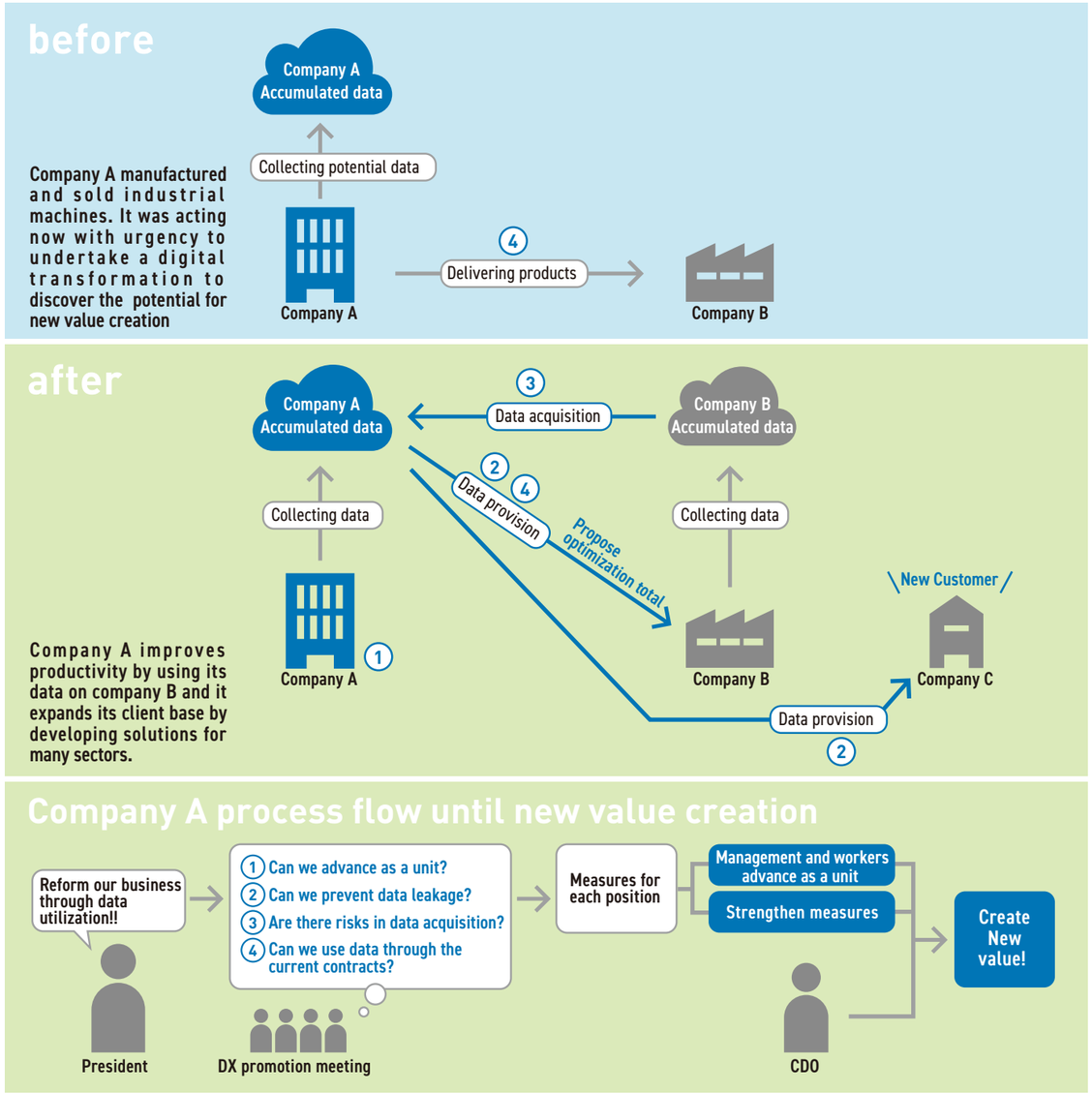
CONTENTS

IP Policy Office, Economic and Industrial Policy Bureau
https://www.meti.go.jp/english/policy/economy/chizai/chiteki/index.html
E-mail: ip_policy_office@meti.go.jp
Tel: +81-3-3501-3752 (Direct) FAX: +81-3-3501-3580

Published 2021.01

01 What is benefit of data utilization?

Let's find new corporate value through data utilization!



1 Can we advance as a unit? ▶ Managerial leadership and hiring CDO establish environment (P03)

2 Can we prevent data leakage? ▶ Ensure data is protected as “shared data with limited access” under the UCPA (P06)

3 Are there risks in data acquisition? ▶ Managing internal data and other parties’ data separately (P08)

4 Can we use data through the current contracts? ▶ Verify details of the current contract and stipulate range of use, etc. (P10)

Cases of success through data utilization

"Useful Points on Data Utilization", which is published by METI, includes a FAQ, other cases and contract clauses relevant to data utilization in addition to material from this Guidance. Reading both documents will provide a deeper understanding.

1 Dealing with a new customer's needs by presenting a visualization of know-how!

【Manufacturer E】
Consulted with a consulting company regarding whether data can be used for factory production schedule
(→ Page 23 in the Useful Points)

Challenges

- There were no documents regarding know-how related to workers or trends of customers or regions.
- There were no electric data for the above items, or data that was accumulated in an analyzable format.
- It was difficult to optimize information in accordance with changes in business.

Measures

- Manufacturer E consulted with a consulting company, and its expert team of mainly data scientists understood manufacturer E’s operations.
- The team extracted statistical data to represent its operations.
- Additionally, the team extracted operational patterns through analyzing past operation history.

Results

- By extracting previously overlooked data, the team reduced the burden of senior staffs and solved the problem of handing down know-how to the next generation of workers, so the team provided customer E with an excellent proposal.
- After introducing the system for manufacturer E, regular system updates allow manufacturer E to deal with changes in business.

2 Contribution to solutions to societal problems by collecting and managing data on entire construction process!

【Construction company F (manufacturing and selling construction machinery)】
Operated platform that optimizes entire construction process (→ Page 16 in the Useful Points)

Challenges

- There were construction industry-specified challenges related to "mismatch of supply and demand". (Population aging and young people's lack of interest in construction, shortage of labour supply despite expansion of demand in construction for significant projects such as updating deteriorating social infrastructure)
- Company F had been introducing ICT, but could only acquire a portion of the data it needed because many construction operators were involved in each project and each operator managed its own data.

Measures

- Company F cooperated with other companies and then established and operated a platform which could undertake "data acquisition, accumulation, and analysis"

Results

- Company F was able to supply fuel to construction machinery in a timely manner and allocate staff appropriately through utilization of data on the entire construction process, improving productivity. Moreover, company F enhanced site safety by sharing details of its operations
- This system led to a win-win situation, that is, data providers and customers were able to obtain benefits in the system that provided solutions and applications to the platform under strict control of access to data.

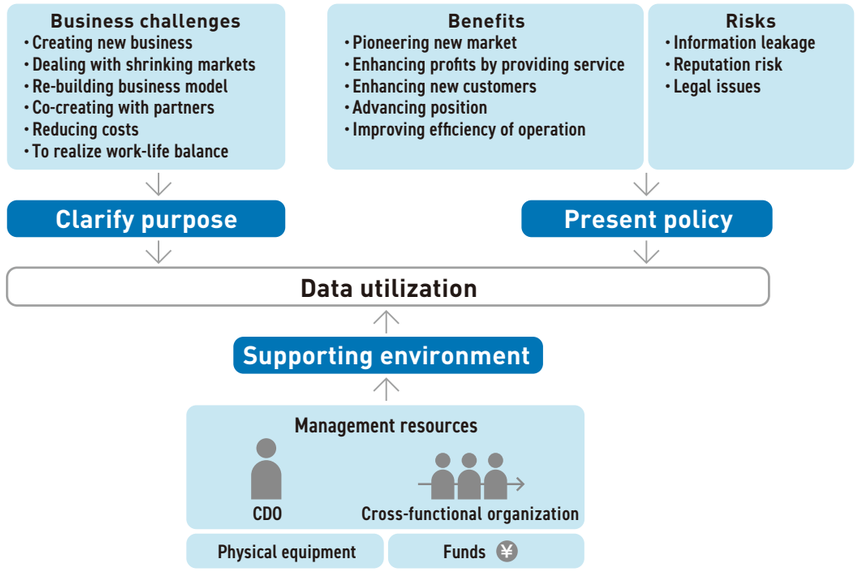
【Current situation in Japan】
Data utilization is investment-oriented in that it aims to provide benefits by creating new opportunities for profit through risk-taking and the better investment of management resources, the improvement of added value from the existing businesses and improvements to productivity.

02 Roles in company

Management establishes the environment

◆To strengthen internal control, and establish an environment that supports workers

Management should clarify purposes for data utilization based on the company's business challenges and present policy that takes into account the benefits and risks associated with data utilization. Moreover, management should support the environment for data utilization including the human resources, physical equipment and funding necessary to develop the fundamental capacity of the organization in terms of data utilization.
As data utilization is somewhat of a trial and error process, it is important to realize that significant results might not appear immediately, and to assess efforts in the long run as data utilization has great potential and will be the basis for growth.



Successful case

Workers feel rewarded through involvement of management

The president established a new organization for data utilization and became the general manager of the organization.
Then, he broke down the barriers to data utilization in the company. As a result, workers could consult with the president frequently and directly to confirm the direction of projects.
Moreover, workers started to rapidly tackle projects with a sense of mission because the president announced the policy on promotion of data utilization both inside and outside the company.

Sharply increased sales thanks to precise risk-taking by the president!

The company invited our supplier's planning and development departments to participate in a study group that provided purchase data to the participants.
Thanks to the measures that minimized the risk of legal issues, the president was able to analyze the level of risk presented. A series of popular products were produced through collaboration across industries and sales increased by several times. Furthermore, this initiative led to a new business, that is, data-consulting.

Failure case

Management leaves everything to workers

The president does not show goals or policy for data utilization, but order workers to use data in its business. In this situation, however, no one can advance anything in the business for several reasons. For example, if there is no clear policy on data utilization and decision making, situations in which no one can decide whether to provide or share data between departments in the company arise.
Consequently, there are many roadblocks and obstacles to efficiency. Moreover, if workers cannot ask for advice from IP and legal departments, they cannot confirm their understanding of potential legal issues, and the potential for data leakage or other data-related problems can lead to worsening relationships with partners and negative attention on the internet and subsequent reputational damage.

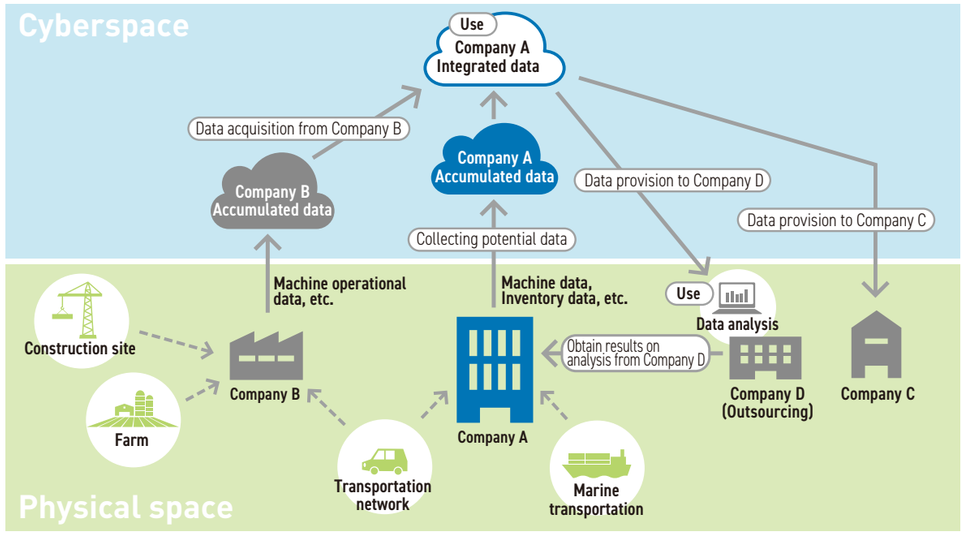
Workers assess data

◆ Identify the data that is necessary to achieve companies' goals

Workers need to consider whether necessary data can be acquired/accumulated in the company, and if it is not possible, they should consider how to acquire data from other companies. Also, they need to identify data availability, that is, what kind of data is necessary, who owns it, how much is there, and how much is available for use by the company.

◆Consider the best actions for the company in terms of data utilization, that is, should they "Provide", "Acquire/Accumulate", or "Use" data, depending on their situation

Workers need to consider contracts, IT systems, laws, etc. based on their specific situation, such as the company provides data to other companies to have the data analized, or the company acquires data from other companies including trade secrets, or the company integrates its data with data from other companies and uses it.



Types of data utilization	Benefits	Points
Provision	・Improving performance and efficiency of in-house products through feedback on results of data analysis ・Expanding customer base across industries and obtaining new customers through establishing new relationships with data users ・Building new business models by preparing infrastructure and database	Refer to P05-06
Acquisition/ Accumulation	・Acquiring/Accumulating data continuously for new service and expanding business ・By building new scheme for acquiring data, improving the value of existing products and providing additional service	Refer to P06-07
Use	・Developing and improving items/services by using feedback information and operational data ・Recognizing characteristics of data through processing, such as integrating internal data with improved data from other companies	Refer to P09-10

【Property of data】
Data, which is an intangible asset, is not subject to rights of ownership, possession, usufruct, or security interests, and ownership of data depends on an agreement of parties. Contracts, therefore, are very important in determining ownership of data. While license agreements on IPR such as patent rights, etc. mainly include that a party will not excise exclusive rights granted legally, data is not granted exclusive legal rights. For these reasons, please note that it is important for a party to make an agreement in contracts regarding the authority to use data and there is difference in contracts between IPR and data. (METI, "Contract Guidelines on Utilization of AI and Data", (2019), page 16)

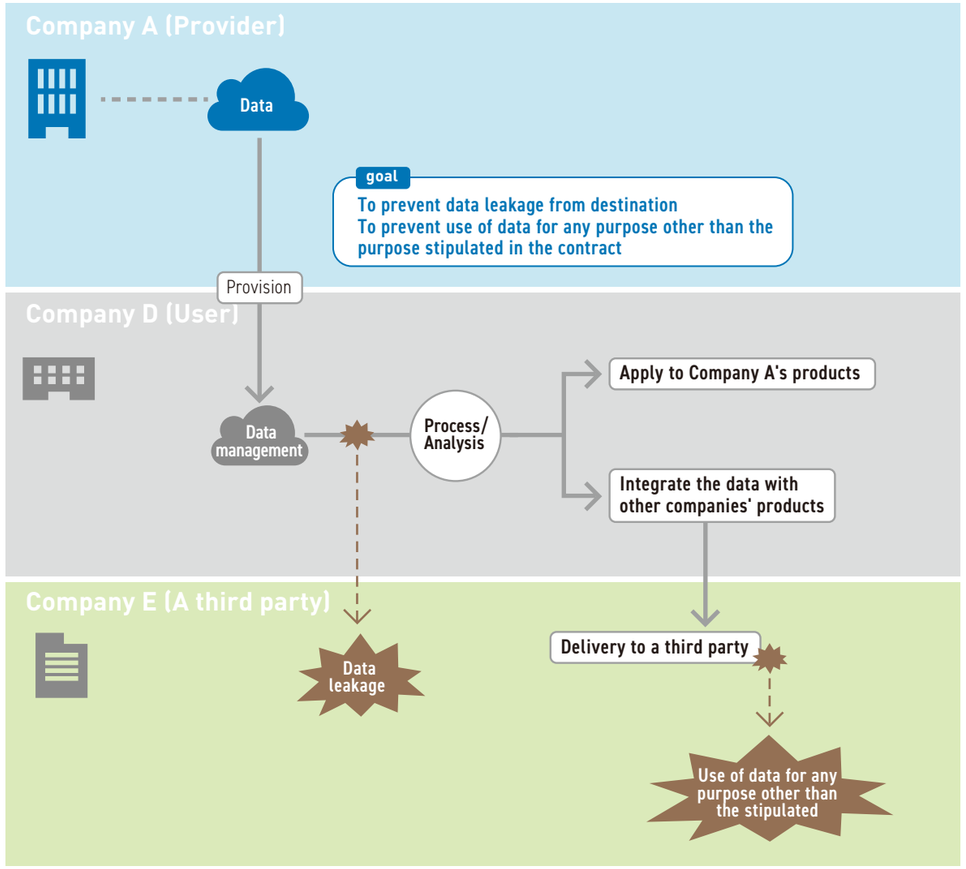
03 Important points for workers ①Provision

How can we prevent data leakage from within a data user or any unintended utilization?

The benefits of data provision are as follows:
- Improving performance and efficiency of in-house products through feedback on results of data analysis
- Expanding customer base across industries and obtain new customers through establishing new relationships with data users
- Building new businesses by installing necessary infrastructure and databases

On the one hand, if data is provided without establishing appropriate countermeasures, it might be used for a purpose other than the purpose stipulated in the contract, causing data leakage, representing a disadvantage for data providers. Therefore, it is important to consider potential risks regarding data provision.

Chronological flow of data provision



Customize measures based on characteristics of data!

point 1 Measures in contracts

Stipulate prohibition of provision of targeted data to a third party (→Q.1, Q.8 in the Useful Points)

It is necessary to make an agreement in contracts regarding the authority to use targeted data because data is not subject to rights of ownership, etc.
In other words, if there is no agreement to the contrary in contracts, the data user can provide the data to a third party freely.
Therefore, it is desirable to stipulate specific data use obligations in principle. However, it is conceivable to prohibit specific forms of data provision, for example permitting partial data provision or prohibiting data provision to competitors.

Stipulate prohibition of use of provided data for any purpose other than the purpose in contracts (→Q.2, Q.6 in the Useful Points)

Using the provided data for a purpose other than the purposes stipulated in contracts might create disadvantages for data providers, such as cases where the user provides derived data or services using provided data to competitors. It is, therefore, important to define the acceptable purposes of data usage clearly and to prohibit the use of the data for any purpose other than the purposes stipulated in contracts.

Stipulate the obligation to discard the data at end of a contract (→Q.1, Q.11 in the Useful Points)

If the user does not discard the provided data, instead preserving it in a server at the user company, there is a possibility that the data would be distributed to a third party unintentionally. The obligation to return or discard targeted data at end of a contract, etc. could reduce risks of data leakage.

point 2 IT system Measures

Not to provide data directly, but to grant access rights to the cloud
(→Q.1, Q.2 in the Useful Points)

The act of providing data may in itself increase the risks of data leakage. The data provider, therefore, should consider keeping the data in the cloud and controlling access in a manner that is appropriate to specific contracts. Granting the user access to the cloud and having the user conduct operations on the data from the cloud may itself reduce the risks associated with data leakage.

point 3 Measures to protect data legally

To provide access to data with ID/password, etc. to specified parties (→Q.1, Q.5 in the Useful Points)

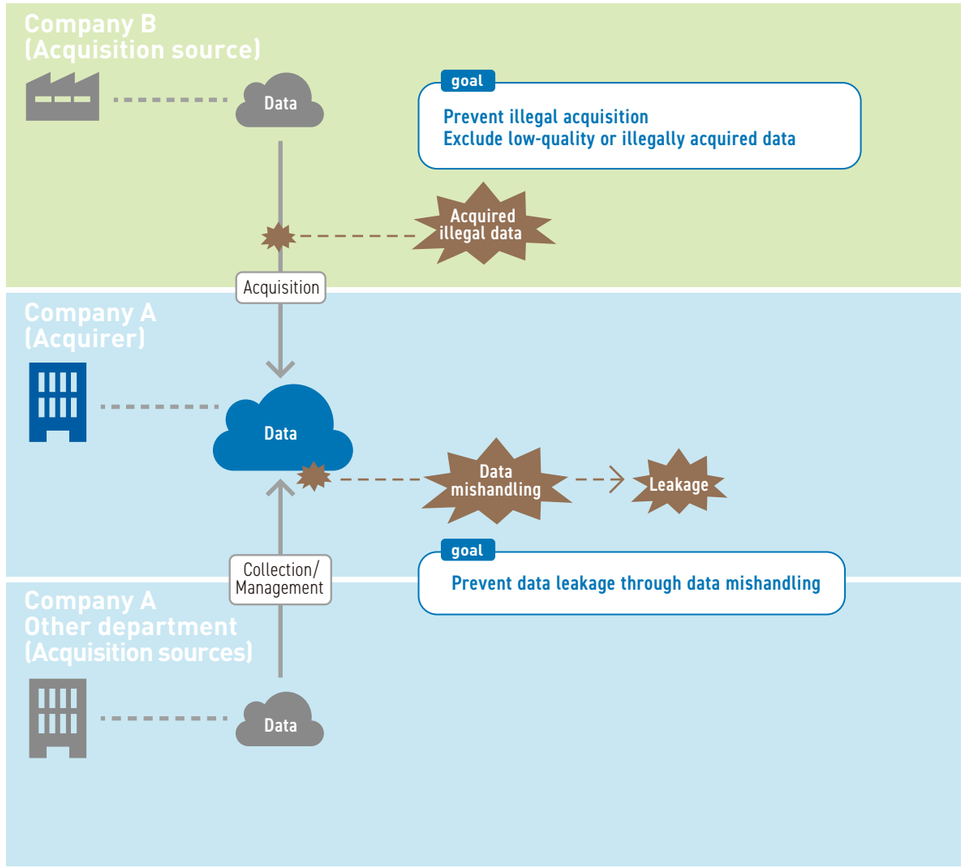
These data can be protected as "shared data with limited access" under the UCPA. Please note that it is necessary to satisfy requirements to receive protection and it is important to manage data appropriately in terms of three requirements under the UCPA. (Please refer to page 11-12 in this guidance regarding the UCPA)

【In case where data leaked from a third party】
In cases where data which falls into "shared data with limited access" under the UCPA is leaked from a third party, the "shared data with limited access" owner can file a claim for injunctions, etc. against unauthorized acquisition/use/disclosure of "shared data with limited access" and a part of use/disclosure of "shared data with limited access" rightfully acquired under civil measures such as contracts. In addition, the "shared data with limited access" owner can file a claim for injunctions, etc. against a part of acquisition/ use/disclosure of "shared data with limited access" by a subsequent acquirer under the UCPA.
Even if the claim is covered under the contracts or the UCPA, it is expected that it will be difficult to substantiate that the provided data is the same as leaked data. Based on these characteristics of data, therefore, it is recommended that data owner add digital watermarks to all provided data. (Please refer to page 41 in the Useful Points)

How can we take measures to avoid losing public trust due to unexpected illegal acts?

As for data acquisition, there are cases where operational status data is acquired from products that are manufactured and sold, and cases where data is acquired from other companies.
Data acquisition from other companies might include data that is protected under the law. If your company leaked the data illegally, other companies may file claims against your company for injunctions or compensation for losses or damage, eroding public trust. Therefore, when data is acquired, it should be confirmed that the data is legally safe and has not been acquired illegally.
Also, when you accumulate data, you should consider concrete methods of managing the data.

Chronological flow of data acquisition/accumulation



Let's avoid troubles by performing advanced countermeasures!

point 1 Measures in contracts

To find common ground between parties on the quality of acquired data (→Q.13 in the Useful Points)
Quality of data might be regarded as the accuracy, completeness, validity, safety, but due to the nature of data, it is difficult for the source of the data to guarantee the quality of the data in many cases. Therefore, the data acquirer (user) should not expect to demand guarantees of the quality of the data, but rather the data acquirer (user) and the data acquisition source (provider) should agree on common ground between themselves in terms of the quality of the acquired data. On the other hand, it is possible for the acquisition source to guarantee that providing such data is not illegal and that there is no deliberate falsification of data. In addition, it is considered reasonable for the data acquirer (user) to ask the acquisition source (provider) to guarantee that the data does not include trade secrets or "shared data with limited access".

Sign the contracts after verifying requested methods of data management
(→Q.12 in the Useful Points)
Each company has its own respective point of view on data security, and it is important to confirm what security level is requested. Moreover, in cases where data leakage has occurred due to the failure to follow the contractual data managing methods, the data acquirer (user) can be contractually liable. To avoid this situation, it is desirable to negotiate terms of contracts after determining that the company is capable of fulfilling the contracts.

point 2 IT system Measures

Separate internal data folders from external companies' data folders (→Q.12 in the Useful Points)
If acquired data has been mixed with internal data, it will be difficult to manage data appropriately, which can lead to unintentional data leakage. It is therefore considered prudent to separate internal data folders from folders containing data from other companies and to restrict access to members who are in charge of projects.

Use cloud services that are appropriate for accumulated data (→Q.23 in the Useful Points)
Different cloud operators provide different services with various specifications, so it is important to choose an appropriate cloud service. Companies seem to think that these cloud services somehow unsecure, but in fact these cloud services are highly secure and compatible with analysis software, etc. because IT experts maintain them. For these reasons, many companies actively use these cloud services.

point 3 Measures against legal risks

To confirm that the acquisition does not fall under unauthorized acquisition under the UCPA (→Q.8, Q.14 in the Useful Points)
In cases where a person, through illegal access, fraud, or similar illegal activity, acquires data that satisfies requirements for trade secrets or "shared data with limited access" under the UCPA, this act could fall under acts of unfair competition, and he/she could be sued for suspending service or compensation for loss or damage. Therefore, it is important to confirm in advance that the act of acquisition does not constitute wrongful acquisition.
(Please refer to page 11-12 in this guidance regarding the UCPA)

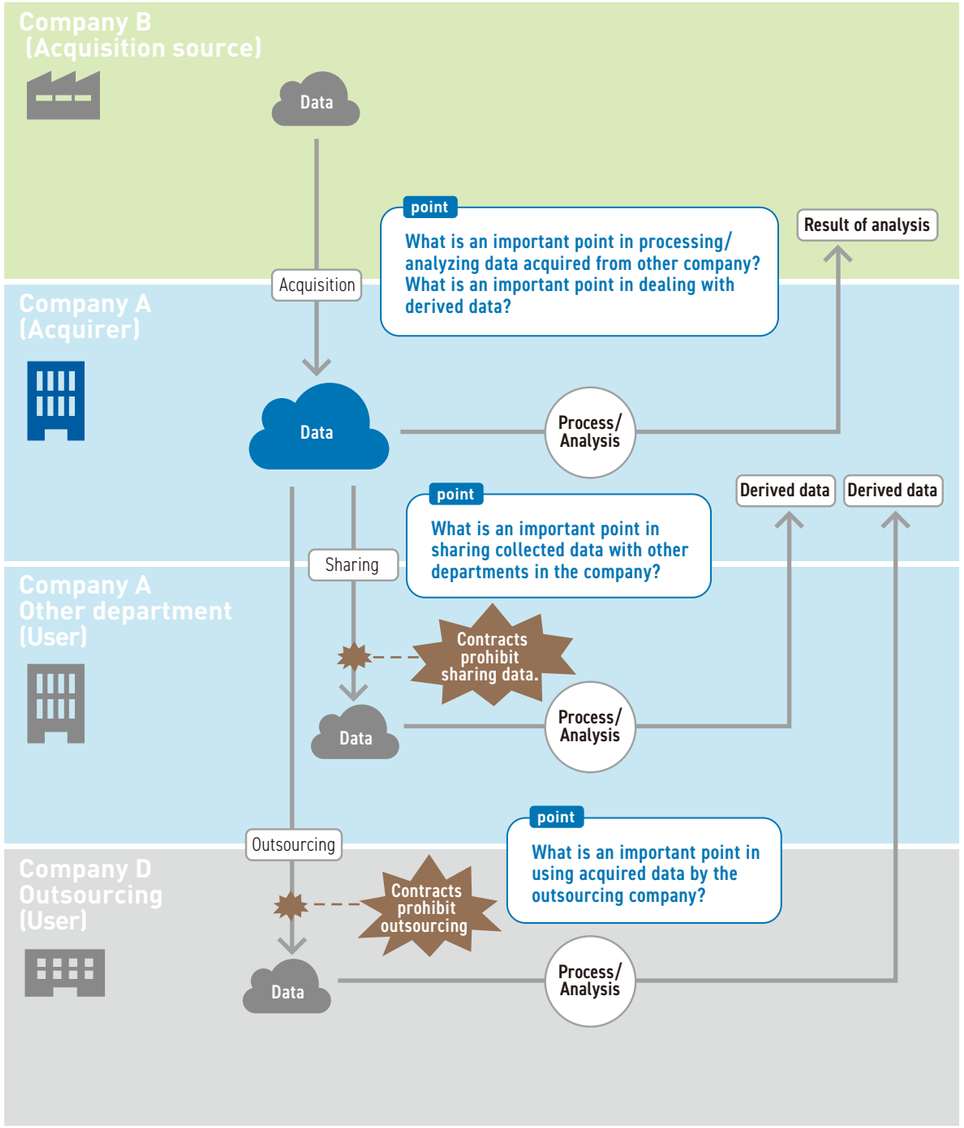
To enhance awareness of characteristics of data (→Item 4-5. in the Useful Points)
It is important to raise awareness in companies of classification of data or how data is to be managed. As for data management, it is requested that employees have an appropriate understanding of the classification of data, that is, specified data are to be classified into specified categories. Therefore, it is important to implement training so that employees can classify data appropriately.

【Managing internal data in a company】
In cases where a company collects data from various departments in the company, it is important to confirm how to manage the situation properly because some departments manage the data as trade secrets. (Please refer to Q.18 in the Check points)
Also, as for existing data in the company, though a balance between potential importance and managing costs for data need to be maintained, if the data has potential future value, it is conceivable to protect it as trade secrets or "shared data with limited access".
(Please refer to Q.19, 20 in the Useful Points)

Can you check contracts based on actual assumed use cases?

Data use includes cases of processing data, such as processing data for internal corporate analysis, processing for deriving data for other companies, and cases where data processing is outsourced. Contracts can stipulate managing methods for derived data or prohibit the use of provided data for any purpose other than the purpose in contracts. Therefore, you can reduce risks by checking contracts carefully in using provided data.

Chronological flow of data use



Think of "Data use" and "Checking contracts" as a set!

point 1 Measures in contracts

Check contracts with other companies before using acquired data (→Q.24 in the Useful Points)

There are cases where the acquired data is provided to other departments in the company. However, this could be a breach of contract if it falls under "use of the data for any purpose other than the purpose in contracts." Therefore, it is important for users to check the contracts in using the acquired data.

Check contracts for management methods for data derived from the acquired data (→Q.25 in the Useful Points)

As the right to use derived data is given by contracts, it is important to check the contracts for management methods for the derived data. Moreover, it is important to find common ground between parties if the management method for the derived data was not stipulated in the contracts.

Check contracts to verify whether there are any problems to ask an outsourcing company to use the acquired data (→Q.27 in the Useful Points)

There is a possibility that use by outsourcing companies could be a breach of contract if the contract includes a non-disclosure agreement regarding acquired data . Therefore, it is important to verify whether the contracts allow for providing the data to an outsourcing company for their use. Also, it is conceivable to sign contracts that do not categorize the outsourcing company as a third party if you have decided on the need for outsourcing in advance.

point 2 IT system Measures

Separate internal data from data from other companies according to the contracts (→Q.24 in the Useful Points)

In cases where multiple data sets are integrated, data leakage resulting from confusion is possible. As for data that is necessary to identify, it is important to take measures such as restricting the range of use or access, etc.

point 3 Measures for legal risks

Confirm that the use does constitute unauthorized use under the UCPA (→Q.25, Q.27 in the Useful Points)

The act of a third party that is contractually unrelated to the data owner acquiring "shared data with limited access" and then using and disclosing it while aware that wrongful acquisition or unauthorized disclosure is involved could constitute acts of unfair competition, and there is a possibility that suspension of service or activity will be requested or that claims for compensation for losses or damages could be filed.
(Please refer to Page 11-12 in this guidance regarding the UCPA)

Enhance awareness of the status of data (→Item 4-5. in the Useful Points)

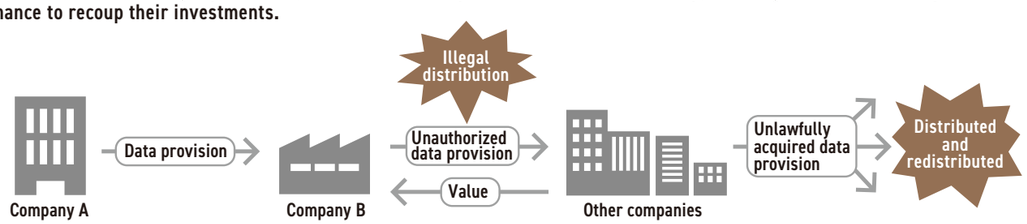
It is important to raise awareness of the status (classified or other) of data or how to manage data in companies. As for data management, employees are requested to appropriately understand the status of data, that is, specific data is classified into a specific category which governs its handling. Therefore, it is important to implement training programs so that employees can both classify and handle data appropriately.

【About deriverd data】
The term "derived data" refers to data that is newly generated through processing, analysis, editing, integration, etc. of any data within the scope of purpose in "Data Provision Type" contracts. Taking for examples, the data from images of dashboard cameras to identify obstacles or locations of retail outlets, or machine operation data to identify malfunctions or causes of such.
(Please refer to Q.4. in the Useful Points)

What is "shared data with limited access"?

Protecting Data from illegal distribution

Weather data, map data, machine operational data, consumption trend data, and similar information are being shared and used to create new enterprises, resulting in the creation of high value that can drive the Japanese economy. We need an environment that rewards the efforts of creators, collectors, analyzers, and controllers of data, but useful data is easy to duplicate and, once illegally obtained, can be immediately redistributed in its entirety, meaning that investors may lose the chance to recoup their investments.



Revision of the UCPA to guard against illegal distribution of data

In the revision, in view of the fact that data is to be widely provided as a product, shared within consortiums, and to be supplied to third parties by business operators through transactions or other operations, the UCPA provides a definition of "shared data with limited access" and defines unauthorized acquisition, use, and disclosure of "shared data with limited access" as unfair competition. These actions are subject to civil measures (plaintiffs may file for injunctions, plaintiffs may file for compensation for losses or damage).

Three criteria for receiving legal protection as "shared data with limited access"

Article 2 (7) in the UCPA
The term "shared data with limited access" as used in this Act means technical or business information that is accumulated in a reasonable amount using electronic or magnetic means (meaning an electronic form, magnetic form, or any other form that is impossible to perceive without the use of a computer or similar display technology; the same applies in the following paragraph) as information provided to specified persons on a regular basis and that is managed (excluding information that is kept secret).

Three requirements for "shared data with limited access"

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

"On a regular basis" refers to cases where data owner provides data repeatedly and continuously (including cases where the intention of the data owner to provide the data repeatedly and continuously is recognized even if data owner does not actually provide it). "Specific persons" refer to those who receive data under certain conditions.

Example "On a regular basis": where data owner provides data repeatedly (including cases where data is provided to each person once)
"Specific persons": members allowed to access members-only databases

2 "Accumulated in a reasonable amount by electronic or magnetic means" (Significant accumulation)

In light of socially accepted conventions, data has value as a result of its accumulation using electronic or magnetic means.
"A reasonable amount" is determined depending on the nature of each data type, but the following and other factors are considered: value added to the data as a result of accumulation using electronic or magnetic means; possibility of utilization; transaction prices; and labor, time, costs, etc. used for collection and analysis. Note that the concept of significant accumulation applies to cases where labor, time and costs are used to collect or analyze data, resulting in value being created for that data.

Example If a business operator that accumulates information on mobile phone locations nationwide extracts information for specific areas and sells it, data for those specific areas satisfies this requirement (if data is considered to have value from the commercial viewpoint as a result of the data being accumulated using electronic or magnetic means)

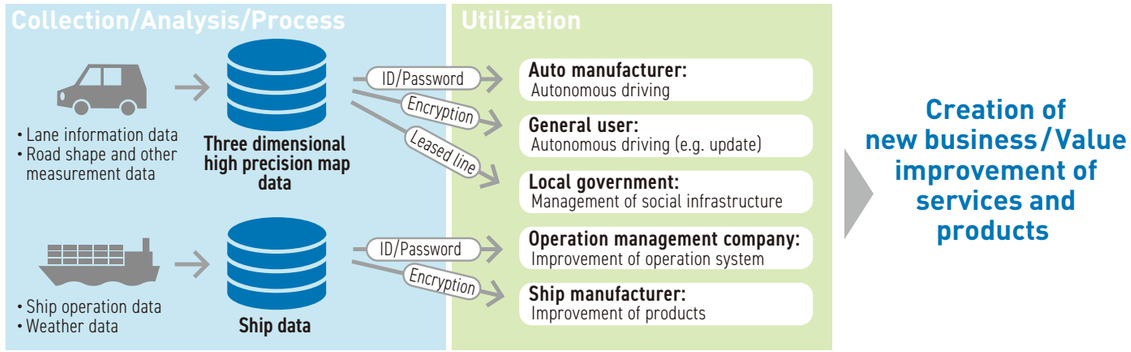
3 3 "Managed using electronic or magnetic means" (Electromagnetic management)

The owner's intention of managing data to provide the data only to specific persons is made clear to outside parties.
More specifically, it is necessary to take measures such as implementing technologies that restrict access, such as ID and password settings.

Example Access restriction using IDs, passwords, smart cards, specified terminals, tokens or biometric authentication.

Image of "shared data with limited access"

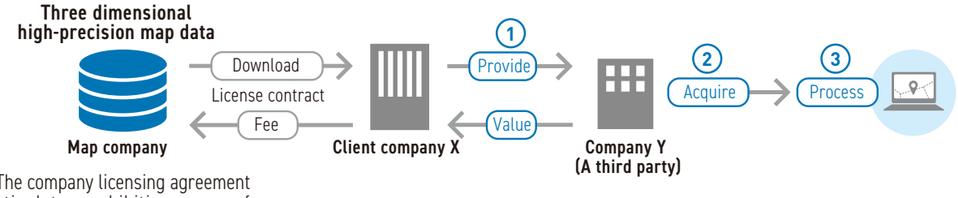
- Technical information: map data, machine operational data, data sets for developing AI-based software, learned models obtained through machine learning, and other information.
- Business information: consumption trend data, market research data, and other information.
  * "Data" in the Guidelines includes text, images, audio, video, and similar information.



Acts of "Unfair Competition"

Malicious and inappropriate actions that interfere directly with the profit of the owner of "shared data with limited access" are defined as "unfair competition". For acts to be defined as "unfair competition", the acts of "acquisition," "use," and "disclosure" must be definite and the target of such acts must be the "shared data with limited access" in question.

Examples of unfair competition



The company licensing agreement stipulates prohibition on use of provided data for any purpose other than the purpose in contract and contains a non-disclosure agreement. Also, it restricts access rights with ID/Passwords for authorized users.

Acts of unfair competition on "shared data with limited access" are classified into the following patterns:

① ⇒**Unauthorized Disclosure** under the UCPA
(Ex.) Company X disclosed some of the "shared data with limited access" to clients through a company's service while being aware that its disclosure to a third party was prohibited.

② ⇒**Wrongful Acquisition** under the UCPA
(Ex.) Company Y asked Company X, for whom data sharing with external entities is prohibited by the data owner, to provide Company Y with the data in return for material benefit while aware of the above fact.

③ ⇒**Wrongful Use** under the UCPA
(Ex.) Company Y used acquired data in developing software based on AI technology while being aware that unauthorized disclosure by Company X was involved.

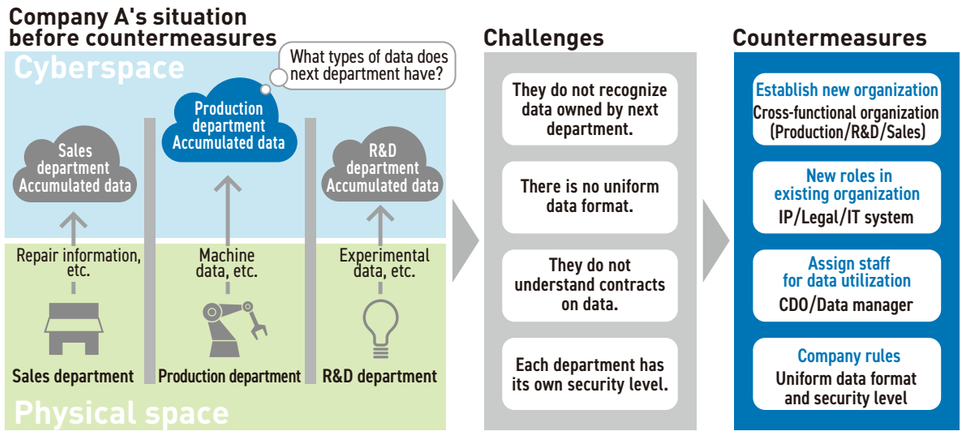
Unauthorized acquisition, use, disclosure, etc. of "shared data with limited access" are subject to civil measures (claims can be filed for injunctions, and for compensation for loss or damage) under the UCPA.

【About Guidelines on "shared data with limited access"】
METI published Guidelines on "shared data with limited access" as "easy-to-understand guidelines" presenting the ideas behind each requirement and specific examples of applicable actions, etc. with regard to "unfair competition" related to "shared data with limited access", a concept introduced as a result of the revision of the Unfair Competition Prevention Act in 2018.
(https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/guidelines_on_shared_data_with_limited_access.pdf)

04 What actions can companies take?

If it is impossible for departments to handle,...

Some companies do not share data among departments, and thereby they cannot proceed company-wide data utilization. On the other hand, companies sometimes do not uniformly regulate their data management, causing wasteful procedures in integrating data and even breaches of contracts in cases of inter-departmental data exchange.



It is important to create a corporate structure for data utilization as follows:

- Establish cross-functional organization
- Provide new role in IP/Legal/IT system/Security department
- Assign staff based on necessary skills
- Raise awareness by establishing company rules and training

◆ Ensure data use is systematic

- In order to implement cross-functional operation, management should envision the employees as the champions of data utilization.
- The management could permit workers to use/share data across departments. Moreover, the management could change the internal review process for new business, etc. to incorporate agile development, thereby promoting new business through data utilization.

◆ Active participation of IP and Legal department

- As IP department needs to provide IP strategies, it is important to collect information, etc., that is, to join to company-wide management meetings and planning meetings, and to coordinate with R&D and other departments that are responsible for new business and new products/services.
- The legal department needs to be actively involved in preparing for issues such as data leakage, etc.
- It is important provide training to raise awareness regarding the management of trade secrets and “shared data with limited access” under the UCPA.

◆ Assign staff to advance data utilization

- It is important to improve the knowledge and skills of workers in various positions to promote data utilization and to hire data scientists, etc. when necessary.
- As decisions take longer without a responsible person in charge, it is desirable to appoint a director or to hire person from the outside as CDO (Chief Data Officer/Chief Digital Officer) who has expertise and final responsibility for data utilization in the company.

How can we prepare for such illegal activity?

◆ Maintain proof of legally appropriate conduct

- In joint-research and development and on consignment, other companies might disclose their data, and such data might become incorporated into internally owned data.
  Therefore, both the usefulness and also the risks in acquiring data from other companies should be weighed against the potential risks, and unnecessary data acquisition should be avoided. Finally, the scope of data that is to be managed as confidential information should be clear.

- In order to defend against potential accusations of wrongful acquisition and use of data including confidential information by the opponent, it is important to separate internally owned data from the other company's data.

◆ Immediate action is critical in an emergency situation

- Neglecting to act immediately in cases of data leakage, etc. can harm the company's image and expand the scope of damage. It is important to take appropriate actions to prepare for prompt and appropriate legal responses.
- Determining actions to be taken and preparing the organization for potential legal challenges is critical.

	If your data is leaked from a client
When	It is difficult to determine the exact timing of a data leak from an external party. Instead, you can grasp suspicions of a data leakage, a point of time when recognizing the fact on the leakage, ground of the recognition and history on the recognition.
Who	Even if you recognized that an external party leaked your data, it is not easy to determine exactly who leaked the data. Therefore, you must inform the external party of details regarding "when" and "what" occurred and to ask the external party to investigate.
What	It is difficult to grasp the range of data leakage if an external party leaked your data. Providing concrete information on the leaked data that was provided, along with when, and on what medium the data was provided, is useful. Digital watermarks and other such digital tools also enhance objectivity in such cases.
How	Even if a data leak is detected, it is not easy to identify how the data was leaked in detail from the outside. It is useful to inform the destination of the facts regarding "when" and "what" was leaked and to ask the destination to investigate further.