

Manual on Cross-Border Industrial Data Management

January 27, 2025

Ministry of Economy, Trade and Industry

Table of Contents

1	Introduction	3
1.1	Background and Objectives	3
1.2	Assumed Readers and Points to Consider	4
2	Scope and Positioning of the Study	5
2.1	Scope of the Study	5
2.1.1	Assumptions of the Study	5
2.1.2	Subjects of Analysis (Process, Data, Risks)	6
2.2	Positioning of the Study and Relevant Guidelines.....	9
3	Three Steps in Cross-Border Data Management.....	11
3.1	Overall Picture and the Study Framework	11
3.2	First Step (Risk Visualization)	12
3.2.1	Organizing Transactions.....	12
3.2.2	Organizing Risk Scenarios.....	13
3.3	Second Step (Risk Assessment)	14
3.4	Third Step (Implementation of Actions)	16
3.5	Organizing Risks and Actions.....	17
4	Major Related Laws and Regulations (EU, China, U.S.)	20
5	Anticipated Risks and Actions	24
5.1	Restriction on Data Transfer and Business Activities (Data localization)	24
5.2	Forced Access to Data (Government Access).....	27
5.3	Mandatory Data Sharing and Disclosure	29
6	Conclusion	32
	Industry Data Sub-Working Group Member List	33

Reference Materials

Reference Material A: List of actions

Reference Material B: Collection of materials submitted to the industry data sub-working group (corporate case studies and related theme trends)

1 Introduction

1.1 Background and Objectives

- With the spread of IoT and digital transformation (DX) technologies, as well as increasing demands for supply chain transparency, international data sharing and utilization by companies are expanding. In addition, the development of cross-industry data platforms and infrastructures, such as the EU's GAIA-X, is accelerating. In Japan, the “Ouranos Ecosystem” project has been promoted as an initiative to enable data collaboration across companies, industries, and national borders.
- As international data sharing and utilization expand, countries and regions are also developing data-related laws and regulations. Some of these regulations¹ encompass all types of industrial data held by companies, regardless of whether they obtain personal information, and include rules that restrict cross-border data transfers (data localization) and enable data access by government (government access). These trends are expected to accelerate.
- Such regulations might become restrictive factors in global corporate activities and affect the enhancement of competitiveness of Japanese industry as a whole and the establishment and spread of cross-company digital infrastructure in the medium to long term.
- In light of these developments and considering the progress of rulemaking for industrial data in various countries and regions, there is a growing need to discuss current situations and appropriate responses focusing on data-related laws other than the Act on the Protection of Personal Information, which has been the primary subject of discussion thus far.
- In response to this, this manual (hereinafter referred to as “the manual”) was created to serve as a guideline for data management related to the cross-border and international distribution of industrial data by companies (hereinafter referred to as “cross-border data management”), aiming to realize safe and secure data sharing and utilization by companies and to promote the creation of added value.
- The manual aims not only to identify major risks for companies in cross-border data sharing and utilization, but also to deepen understanding about appropriate cross-border data governance concepts and processes to create business value and strengthen competitiveness through data sharing and utilization. In addition, it also seeks to contribute to the enhancement of medium- to long-term competitiveness and the establishment of a cross-business digital infrastructure by promoting data sharing and utilization at individual companies.

¹ Refer to Chapter 4, “Major Related Laws and Regulations (EU, China, U.S.) ”

1.2 Assumed Readers and Points to Consider

- Assumed readers of the manual include practitioners in business, risk and compliance, legal, and data management departments across a wide range of industries, including manufacturing and IT services, regardless of the size of the company. The manual is also intended to be used as a step toward understanding the data management concept and process and its importance when sharing and utilizing data internationally, even in small and medium-sized companies where the number of departments and personnel involved in data management is limited.
- Discussions on industrial data has not yet been fully systematically examined, and discussions focusing on cross-border data management are a new area of study. The manual does not include exhaustive discussions but aims to provide appropriate information by presenting steps of cross-border data management and some assumed risks.
 - Assumed risks and examples of corporate responses are listed in Chapter 5, “Assumed Risks and Actions.” However, they are assumed typical risks and actions based on Chapter 4, “Major Related Laws and Regulations (EU, China, U.S.),” and are not necessarily applicable to all companies and operations.
- The manual is not intended to establish mandatory rules like laws and regulations or to provide official interpretations of laws and regulations in each country. Rather, it is intended to provide some concrete examples of risks and actions that may arise in the current cross-border data management and to promote a common understanding across companies and industries.

2 Scope and Positioning of the Study

2.1 Scope of the Study

2.1.1 Assumptions of the Study

- The manual focuses on situations where data is shared and utilized internationally.
 - It covers not only situations in which data generated or acquired in Japan or overseas is transferred to overseas or third countries, but also cases where data generated or acquired overseas is shared or utilized in the same region or country without cross-border data transfer.
- The Japanese government promotes the DFFT (Data Free Flow with Trust), a concept that “aims to promote the free flow of data while ensuring trust in privacy, security, and intellectual property rights.²” The manual defines value to be realized (the elements needed to materialize DFFT); “free distribution and use,” “confidentiality and rights protection,” and “trustworthiness assurance,” as the “values to be realized” (Figure 1).

Figure 1

Value to be Realized (Elements Needed to Materialize DFFT)



Free distribution and use
(ability to freely access and control data)

Freely access, use and manage company data and necessary business data anytime



Confidentiality and rights protection
(ability to protect important data)

Protect data from access by other countries' governments, cyber-attacks, and unauthorized access

Remedies are available in case of infringement of IP rights, etc.



Trustworthiness assurance
(ability to use data reliably)

Data integrity and authenticity are guaranteed (source of data is legitimate and not tampered)

² Digital Agency, 「DFFT」 <https://www.digital.go.jp/policies/dfft>

2.1.2 Subjects of Analysis (Process, Data, Risks)

- Data sharing and utilization in companies can, by its nature, cover a wide range of corporate activities. As the scope of study in the manual, “target processes,” “target data,” and “target risks” have been defined.
- “Target processes” (Figure 2) include data sharing and utilization in each stage of the data lifecycle.
 - The data lifecycle refers to the process of “generation/acquisition,” “processing /usage,” “transfer/provision,” “storage,” and “disposal” of data. “Disposal” includes making data inactive or invisible, as well as deleting data.

Figure 2

Scope of Study in the Manual: Target Processes

Data lifecycle ¹	Generation/ Acquisition	Processing/ Usage	Transfer/ Provision ²	Storage	Disposal
Description of each step	Generate new data automatically or manually, and place under company control	Extract and process data for viewing and analysis	Transfer/share data for free or for a fee to other organization/ departments for use	Store and control data securely and efficiently for use as needed	Delete data or make it inactive (unusable/ invisible)
E.g. of cross-border data transfer for each process	Acquire data generated abroad	Refer to and use data analyzed in Japan at the company's overseas sites	Transfer data held in Japan to overseas sites	Store data on servers hosted overseas using a global cloud service	Data stored overseas is deleted
<div style="text-align: center;">+</div> <div style="border: 1px solid black; padding: 5px; display: inline-block;">General cases where each process occurs or is implemented overseas</div>					

1. The data lifecycle refers to a series of processes from data generation to disposal

2. Since cross-border data transfer occur in each process, data transfer in “transfer/provision” does not include cross-border transfer in “generation/acquisition”, “processing/usage”, “storage”, and “disposal”

- “Target data” (Figure 3) covers all industrial data that can be handled in international data sharing and utilization³. Compared to “personal data,” which has been discussed from the perspective of personal information protection, the manual focus on the domain of “non-personal data,” where systematic study has thus far been limited, and conduct an in-depth examination of relevant case studies.
 - In the manual, “personal data” include personal, pseudonymized, anonymous processed information, personal-related information, and other data that are subject to protection under Japan's Personal Data Protection Act and the personal data protection legislation of each country and region. “Non-personal data” refers to data in general that does not fall under “personal data,” including data

³ For information on how each country's privacy laws govern cross-border data management, see, for example, Personal Information Protection Commission Japan, “Survey on cross-border transfers of personal data by private companies and compliance with overseas laws,” Dec. 2023

<https://www.ppc.go.jp/enforcement/international_materials/?_ga=2.261802949.956306041.1737598960-1996458472.1737598960>

collected and accumulated through corporate activities, such as “safety and security-related data,” “sales data,” “technical data,” and “other business data.”

- In practice, the above classification between “personal data” and “non-personal data” can be relative and fluid, depending on laws and regulations of each country and region. Therefore, it is necessary to be careful to comply with the personal data protection laws of Japan and other countries and regions for “non-personal data.”

Figure 3

Scope of Study in the Manual: Target Data

Data categories	Data category overview	Data examples	
Non-personal data ¹	Safety and Security data	Information highly important for national/ industrial security, incl. military, critical infra and specific critical goods	<ul style="list-style-type: none"> • Data for security trade control • Technical/op data on critical infrastructures for social infra • Supply chain and other data on specific critical goods
	Sales data	Information collected and accumulated through sales activities	<ul style="list-style-type: none"> • Business partners data (transaction prices, partners' info) • Contract data with partners (data obtained by licensing, NDA) • Limited access data obtained from partners
	Technical data	Technical activity information in general, incl technical knowledge, data, know-how	<ul style="list-style-type: none"> • Technical data, know-how (combination of parts, ingredients of new materials, manufacturing know-how) • Data protected by IP rights: data recognized as originality (source code, algorithms, contents such as photographs and music) • Other company's data (shared data with limited access)
	Other business data	Business activity information other than safety and security, sales/tech data generated and stored by a company	<ul style="list-style-type: none"> • Management strategy data (data for business/investment plans) • Corporate security data (data on infrastructure, BCP, etc.)
Personal data	Information including personal data, pseudonymized/anonymized data, and personal-related info	<ul style="list-style-type: none"> • Personal info (can identify an individual) • Pseudonymized info (cannot identify an individual without checking other info) • Anonymized processed info (cannot identify an individual by processing personal info) • Personal-related info (info on a living individual, not falling under the above) 	

1. Non-personal data refers to data in general not classified as “personal data”

- “Target risks” include “inability to freely access and manage data stored in other countries and regions,” “inability to protect important data (confidentiality and rights),” and “inability to trust data,” as a flip side of “values to be realized” (Figure 4).

Figure 4

Scope of Study in the Manual: Target Risks



Inability to freely access and manage data stored in other countries/regions

Company data or data necessary for business operations cannot be freely accessed, used, or managed



Inability to protect important data (confidentiality and rights)

Confidentiality/rights of the critical data cannot be protected due to forced access by other countries' governments, cyber-attacks, and unauthorized access



Inability to trust data

Accuracy and completeness of data is not ensured (source of data or data without tampering is not ensured)

2.2 Positioning of the Study and Relevant Guidelines

- The manual is compiled based on the results of discussions by the “Industrial Data Sub-Working Group” from May to December 2024.
- The Industrial Data Sub Working Group is positioned under the “International Data Governance Advisory Committee” and the “International Data Governance Study Group” (both under the Digital Agency and METI).
 - The “Data Governance Guidelines (draft)” to be released by the Digital Agency based on the discussions of the “International Data Governance Advisory Committee” and the “International Data Governance Study Group” take a broad view of data governance in general from a management perspective. The manual focuses on practical aspects and aligns with the “practical business processes for cross-border transfers” in the “Data Governance Guidelines (Draft)”.
- In addition, there are several guidelines that summarize related content (Figure 5). The manual also refers to the contents of these related guidelines.
 - Representative guidelines include the “Data Management Framework for Collaborative Data Utilization⁴,” “Handbook for Protection of Confidential Information⁵,” “Contract Guidelines for AI and Data Use⁶,” and “Guidelines on Shared Data with Limited Access⁷”.
 - In line with the structure of the manual, chapters and sections from each relevant guideline that may be useful have been compiled as key references (Figure 6). In addition to the key references, these guidelines also contain many other useful ideas and insights, so it is recommended to review in their entirety.

⁴ https://www.meti.go.jp/policy/netsecurity/wg1/DataManagement-Framework_1_1.pdf

⁵ <https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf>

⁶ https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20200619002.pdf

⁷ <https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf>

Figure 5

Overview of Relevant Guidelines

	Objectives	Assumed target readers	Contents related to this manual	Year issued
1 Data Management Framework for Collaborative Data Utilization (Cybersecurity Division, Commerce and Information Policy Bureau, METI)	Ensure security and trustworthiness of data as cyber and physical spaces merge • Provide a framework for appropriate data management in the entire lifecycle	Persons in charge at organization that manage/use data Engineers involved in system design and operation Guidelines/ rules developers	Data management model • Visualization of data status and risks and security assurance in the lifecycle External reference of standards and guidelines for security measures	2022 • Last revised in 2024
2 Handbook for Protection of Confidential Information (Intellectual Property Policy Office, METI)	Strengthen protection against leakage of confidential info and mitigate legal risks	Corporate executives Corporate information control managers, legal/compliance departments	Evaluation of data held by a company • Data evaluation and determination of confidential info Selection of measures for data leakage Organization structure for data management	2016 • Last revised in 2024
3 Contract Guidelines on Utilization of AI and Data (Digital Economy Division, Commerce and Information Policy Bureau, METI)	Summarize general contractual matters and considerations for operators in contracting for data	Corporate business promoters and personnel Corporate contracting and legal personnel	Legal points in data sharing contract • Points to consider in cross-border transactions Examples of major contract clauses	2018 • Last revised in 2019
4 Guidelines on Shared Data with Limited Access (Ref) (Intellectual Property Policy Office, METI)	Clarify requirements and concept of legal protection as “shared data with limited access” under the Unfair Competition Prevention Act	Corporate business promoters and personnel Corporate contracting and legal personnel Corporate information control managers	Introduction of unfair competitive practices and countermeasures	2019 • Last revised in 2024

Figure 6

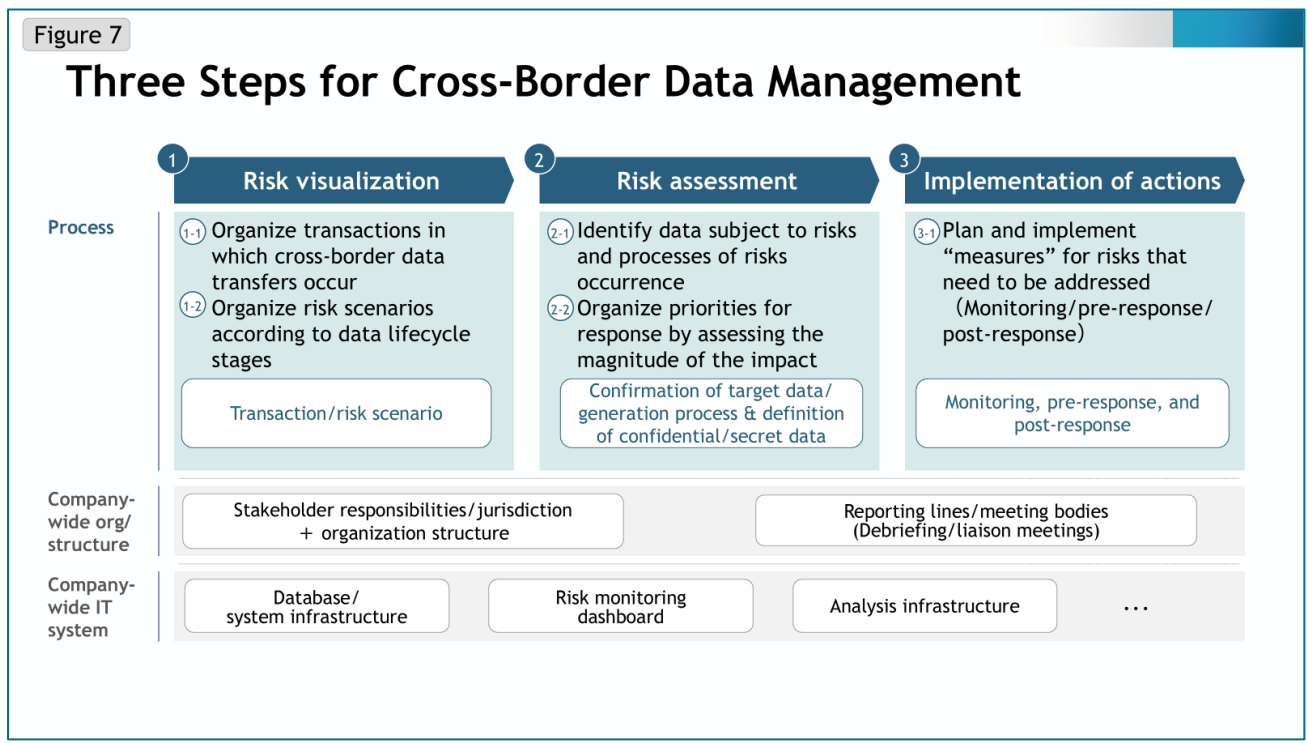
Key References for Relevant Guidelines to the Manual

This manual (ch.)	Relevant guidelines	Key references	Overview
3 Three Steps in Cross-Border Data Management	3.2 1st Step (Risk Visualization)	1. Data management model of this framework • 2-2-1 Modeling (“Events”)	Definition of data lifecycle and description of typical risks
	3.3 2nd Step (Risk Assessment)	III. Acts of “unfair competition” (general) Ch. 2: Recognition and assessment of information owned by companies • 2-2 Decision of confidential information	Definition of unfair competitive practices in the data lifecycle Criticality assessment of confidential info (trade secrets, personal data, sensitive tech info) and examples of considerations in determining confidential info
4 Major Related Laws and Regulations (EU, China, US)	1 Data Management Framework for Collaborative Data Utilization	2. Data management model of this framework • 2-2-1 Modeling (“Domains”)	Examples of data norms • Laws and regulations of each country/region, internal rules of the org
	3 Contract Guidelines on Utilization of AI and Data	4. “Data provision” contract (one-side data offer) • (5) Points to consider in cross-border transactions	E.g. of overseas laws/regs to be considered in cross-border transactions • Cross-border transfer reg, foreign exchange laws, governing laws
5 Assumed Risks and Actions	2 Handbook for Protection of Confidential Information	Ch.3: Classification of confidential info/Selection of measures for info leakage and rule making • 3-2: Selection of info leakage measures by category • 3-3: Rule making on how to handle confidential info • 3-4: Examples of specific measures against leakage	Examples of measures to protect/address unintentional disclosure of confidential data by data holders
	3 Contract Guidelines on Utilization of AI and Data	7. Examples of major contract clauses	Description of proposed model contract (data provision/creation contract)

3 Three Steps in Cross-Border Data Management

3.1 Overall Picture and the Study Framework

- In this chapter, a framework will be presented to show the overall picture and items to be considered for cross-border data management. The framework defines three steps, (1) risk visualization, (2) risk assessment, and (3) implementation of actions, and processes in each step (Figure 7).
 - In addition to the above processes, the development of organizational structure and IT systems are also important for cross-border data management. However, since these should be considered from the perspective of overall corporate activities as well as cross-border data management, the manual does not provide a systematic review of these issues.
 - The said “Data Governance Guidelines (draft)” describes data maturity and security as well as business processes for cross-border transfers as pillars to achieve data governance.



3.2 First Step (Risk Visualization)

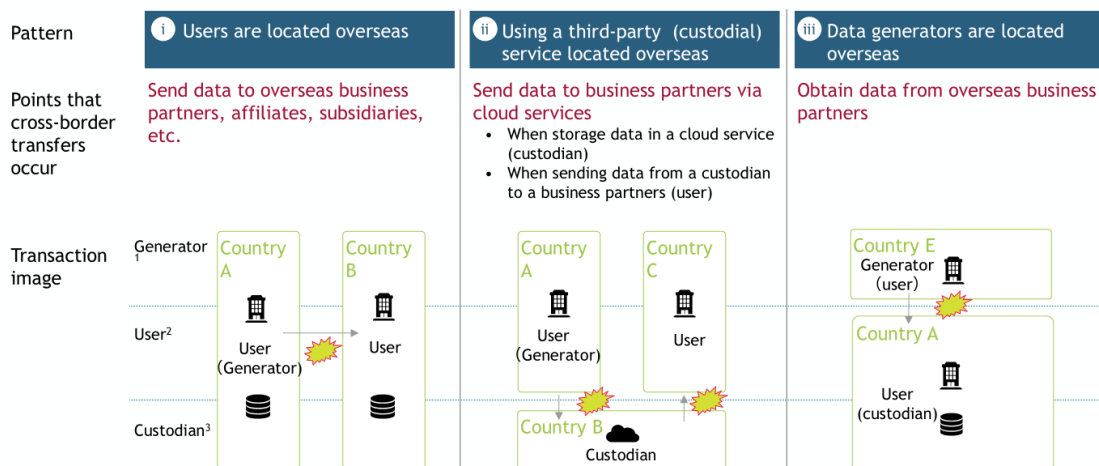
3.2.1 Organizing Transactions

- In risk visualization, one first organizes the relevant stakeholders, the data and its locations in the anticipated data sharing and utilization, to understand where international sharing and utilization take place and where cross-border transfers may occur.
- In data sharing and utilization, stakeholders are categorized as “generator,” “user,” and “custodian.”
 - In the manual, “generator” refers to a natural or legal person who generates data through manual data input or automatic generation from devices or systems, “user” refers to a person who uses data through data sharing or processing, and “custodian” refers to a person who manages and operates data storage (services). However, the classifications and terms defined in the manual do not necessarily correspond to those in the laws and regulations of each country.
 - Depending on the transaction, the same stakeholder may play multiple roles as “generator,” “user,” and “custodian,” or different stakeholders may play these roles.
- There are countless transactions in practical business operations. It is important to organize the transactions (what data is shared, at what stage of the lifecycle, from whom, to whom, and by what means) based on the classification of stakeholders, and to identify the data location, including whether there are any overseas companies or service providers and in which countries they are located.
- Patterns of cross-border data transfers include “users are located overseas,” “using a third-party (custodial) service located overseas,” and “data generators are located overseas” (Figure 8).

Figure 8

First Step (Risk visualization: ① Organizing Transactions)

~ Transactions that cross-border data transfer occurs ~



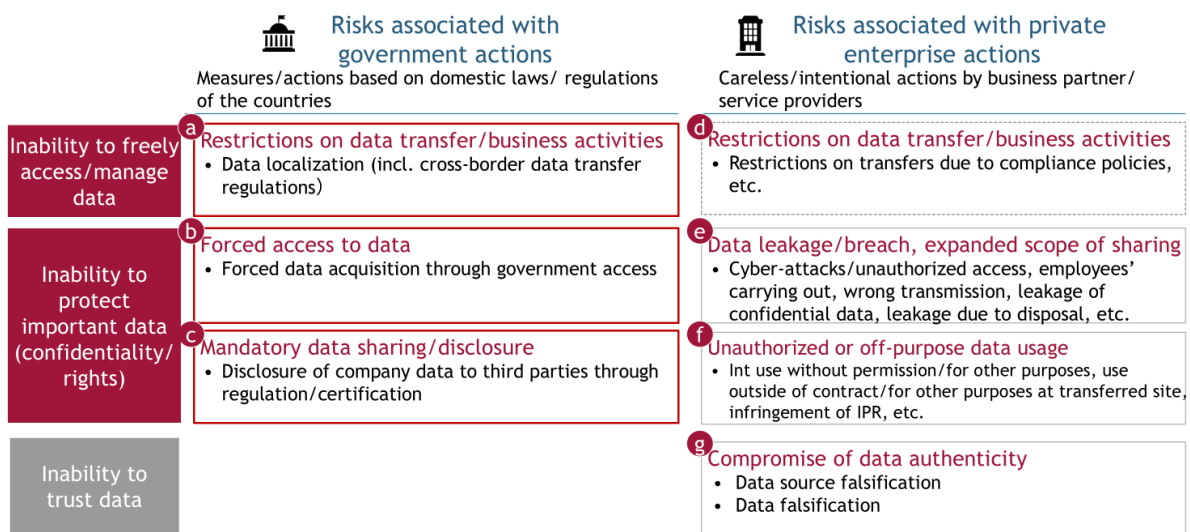
1. “Generator” is a person who creates data through manual data entry or automatic generation from equipment or systems
 2. “User” is a person who actually use data through data sharing, processing, etc.
 3. “Custodian” is a person who manages/operates a data storage location or storage service

3.2.2 Organizing Risk Scenarios

- This step is to organize assumed risk scenarios based on the data location, data content, and data lifecycle identified in 3.2.1 “Organizing Transactions.”
- As described in 2.1.2 “Subjects of Analysis (Process, Data, Risks),” target risks in the manual are “inability to freely access and manage data stored in other countries and regions,” “inability to protect important data (confidentiality and rights),” and “inability to trust data.” There are risks from measures and actions based on domestic laws and regulations of the relevant country (hereinafter referred to as “risks associated with government actions”), and risks arising from actions by private enterprises such as business partners and service providers, whether through negligence or intentional conduct (hereinafter referred to as “risks associated with private enterprise actions”).
- These risks are classified into seven categories: “a. Restrictions on data transfer and business activities,” “b. Forced access to data,” “c. Mandatory data sharing and disclosure,” “d. Restrictions on data transfer and business activities,” “e. Data leakage and breach, expanded scope of sharing,” “f. Unauthorized or off-purpose data usages,” and “g. Compromise of data authenticity” (Figure 9).

Figure 9

First Step (Risk visualization: ②Organizing Risk Scenarios) ~ Typical assumed risk categories ~



3.3 Second Step (Risk Assessment)

- Since it may be difficult for companies to address all risks due to limited resources, it is considered effective to assess and prioritize risks visualized in the first step.
- Regarding assumed risks, identify the target data (what data is at risk in the transaction) and the process of risk occurring (processes and conditions of actions causing risks, existence of relevant safeguards, etc.).
- Assess the impact of the risk and determine the priority to address based on the target data and the process of risk occurring.
 - In the manual, confidential and secret data is defined as data that is highly confidential to the company and data that is subject to a non-disclosure agreement. It is recommended that companies define the confidential and secret data they need to protect and check whether any data at risk includes confidential and secret data.
 - The determination of confidential and secret data varies among companies (Figure 10). For example, the Information-technology Promotion Agency, Japan (IPA) describes the evaluation criteria for confidential information in Chapter 2 (8), “Detailed risk analysis methods” of the “Information Security Guidelines for SMEs, version 3.1⁸.” In addition, examples of criteria for determining confidential information are provided in Chapter 2 “Recognition and assessment of information owned, and decision on confidential information” of the “Handbook for Protection of Confidential Information⁹ .” Furthermore, based on the risk generation process, it is recommended to confirm and evaluate the foreseeability of risks (whether the occurring process and conditions are clear) and the existence and applicability of safeguards (availability of objections, negotiations, and damage coverage, etc.).
 - In general, the higher the level of confidentiality, the more considerations must be made for data sharing and utilization.

⁸ <https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf>

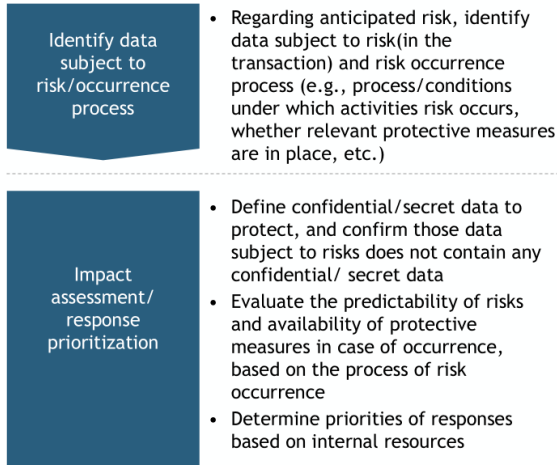
⁹ <https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf>

Figure 10

Second Step (Risk Assessment)

~ Risk assessment process & perspectives to consider when determining confidential data ~

Risk assessment process



E.G. of perspectives to consider when determining confidential/secret data

-
- Sales data**
- ❑ Whether the data is proprietary to the company and if it is leaked, competitiveness will be compromised (e.g., sales prices, data on clients, customer service manuals, pre-publication designs, etc.)
 - ❑ Whether the leakage will constitute a violation of laws/regulations or a breach of contract with other company, cause a decline in the social credibility, or damage the relationship of trust (e.g., personal information of customers, limited provision data disclosure on a limited basis through contracts such as NDAs in commission/license contracts and M&A negotiations, etc.)
- Technical data**
- ❑ Whether the technologies used in the product can be easily identified by analyzing the products on the market, and other company can quickly catch up with
 - ❑ Whether it is difficult to detect and prove infringement of rights even if rights have been acquired
 - ❑ Whether the leakage will constitute a violation of laws/regulations or a breach of contract with other company, damage the relationship of trust
 - ❑ Whether it is technical data that serves as social infrastructure or technical standards (e.g., communication technologies or testing methods), and market expansion of the technology is required to maximize the company's profit



3.4 Third Step (Implementation of Actions)

- Develop and implement actions to address priority risks determined in the second step.
- Major categories of actions include “monitoring” to detect signs and occurrences, “pre-response” to prevent risks and reduce impact when they occur, and “post-response” to recover and prevent recurrence (Figure 11).
 - Monitoring: Identifying suspected or predicted risk occurrence, identifying whether risk occurs or not
 - Pre-response: Reduction and prevention of the probability of risk occurrence, Reduction of impact when occurring
 - Post-response: Protective measures, Pursuit of liability (appropriate and timely reporting to stakeholder), Prevention of recurrences
- Actions categories are further divided into organizational measures (guideline development, storage location selection, etc.), legal measures (contracting, etc.), and technical measures (encryption, access restrictions, etc.).
- For details, please refer to chapter 5 “Anticipated Risks and Actions” and Reference A “List of actions.”

Figure 11

Third Step (Implementation of Actions)



~ Main action categories ~

Legend:  Organizational measures
 Legal measures
 Technical measures




Monitoring

Identify suspicions or early indications of risk occurrence

-  Identifying early signs caused by laws/regulations (e.g., policy consideration)
-  Identifying early signs caused by the private enterprise (e.g., suspicious behavior)




Identifying whether risk has occurred

-  Understanding number of risk occurrences and track record (e.g., number of law enforcement cases/internal occurrences, etc.)






Pre-response

Prevention/ reduction of the probability of risk occurrence

-  Guideline development, storage location/service selection, alternative data/operation, etc.
-  Conclusion of a contract for data sharing and usage
-  Access restrictions, take-out controls, prevention of unauthorized access



Reduction of impact when occurring

-  Guideline development, ensuring accountability and transparency
-  Conclusion of a contract for data sharing and usage
-  Data protection and encryption






Post-response

Protective measures Pursuit of liability

-  Assess the impact of risk, initiate initial response
-  Protective measures and liability enforcement based on contracts or applicable laws

Prevention of recurrence

-  Review of internal operations, business partners, and services used
-  Review of contracts
-  Review and identification of issues in technical measures

3.5 Organizing Risks and Actions

- This section organizes the potential measures considered effective for typical risk categories defined in 3.2.2, “Organizing Risk Scenarios.”
- The direction of effective measures depends on whether the risks are associated with government actions or private enterprise actions (Figure 12).
- “Risks associated with government actions” include direct regulations to restrict and intervene such as data localization and government access and indirect regulations to require companies’ such as mandatory data sharing and disclosure (Figure 13). Among measures related to data localization, domestic storage and processing requirements, and regulations prohibiting cross-border transfers¹⁰ fall under risks from direct government action, while regulations allowing conditional cross-border transfers fall under risks from indirect government action.
 - While it is difficult to avoid the occurrence of risks associated with direct government actions, it is possible to take measures by correctly understanding (monitoring) the relevant laws and regulations and their impact. Pre-responses (decentralization of data, and careful examination and selection of storage locations) to reduce the probability of risk occurrence and impact, and early post-responses in the event of risk occurrence are considered effective. Details are provided in 5.1 “Restrictions on Data Transfer and Business Activities (Data Localization)” and 5.2 “Forced Access to Data (Government Access).”
 - Against risks associated with indirect government actions, it is effective for companies to grasp (monitor) the content and impact of relevant laws and regulations and take pre-responses such as appropriate contracts/arrangements with business partners (e.g., reporting obligation in case of risk occurrence and disclaimers in case of negligence). Details are provided in 5.3 “Mandatory Data Sharing and Disclosure.”
- While it is difficult to comprehensively identify risks associated with private enterprise actions due to diverse factors and targets involved, flexible measures can be taken through agreements and decisions among companies. Effective measures include pre-responses of preventing occurrence through technical and security measures (e.g., restricting access, controlling exportation, protecting and encrypting data)¹¹ and concluding appropriate contracts with partner companies, as well as post-responses such as early notification and announcement to stakeholders of the occurrence and date of the incident. Risks associated with private enterprise actions are often caused by carelessness or lack of governance in a company. Although indirect effects from increased transactions with foreign companies with different business practices and management systems are expected, they are not risks directly caused by international data sharing and utilization or cross-border transfers.
 - In contracts between companies, it is useful to consider appropriate and necessary conditions from both side: from data generators (providers), for data

¹⁰ For the classification of data localization measures, see Yukiko Konno, “An Examination of Data Localization: A focus on its impact on businesses and policy objectives (March 2024) <[RIETI - An Examination of Data Localization: A focus on its impact on businesses and policy objectives](#)>, and details are provided in 5.1, “Restrictions on data transfers and business activities (data localization).”

¹¹ For Japan’s Act on the Protection of Personal Information, see examples in 10-6 Technical safety control measures in the “Guidelines for the Act on the Protection of Personal Information (General Rules)” of the Personal Information Protection Commission Japan.
<https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/>

protection, and from data users (recipients), for ensuring the use and disclosure of data necessary for their business.

- “Disposal” in the data lifecycle includes making data inactive or invisible. In practice, it is often difficult to grasp the status of data, and particular care must be taken to avoid leaks or misuse.
- Since the scope includes the international sharing and utilization of data as well as cross-border transfers, the manual focuses on “risks associated with government actions.” Accordingly, the following chapter - 4 “Major Related Laws and Regulations (EU, China, U.S.)” and 5 “Anticipated Risks and Actions”-provide detailed explanations of these risks.

Figure 12

Risk and Measures ~Overview~

	Risk overview/characteristics	Direction of effective measures
Risks associated with government actions	Direct a Restrictions on data transfer/business activities (data localization) ¹ b Forced access to data (government access)	Monitoring Pre-response Post-response • Properly understand relevant laws and regulations and their impact • Consider post-response to avoid or reduce the risk (e.g., decentralization of data, examination/selection of storage locations, etc.) • If a risk occurs, take early post-response (e.g., notify/publicize to stakeholders on matters and dates of occurrences, etc.)
	Indirect c Mandatory data sharing/disclosure	Monitoring Pre-response Post-response • Properly understand relevant laws and regulations and impact • Make appropriate agreements/arrangements with partners (e.g., reporting obligations in case of risk occurrence, disclaimers in case of negligence, etc.) in case of occurrence
Risks associated with private enterprise actions	d-g Restrictions on data transfer and business activities Data leakage/breach Use without permission/for other purposes Authenticity	Monitoring Pre-response Post-response • Prevent occurrence itself through technical/ security measures, etc. • Make appropriate contracts/arrangements with business partners in case of risk occurrence • If a risk occurs, take early post-response (e.g., notify/publicize to stakeholders on matters and dates of occurrences, etc.)

1. This could include regulations that conditionally allow cross-border transfers, but in that case since these measures are indirect regulations in which the govt orders company, actions against "risk from govt actions(indirect)" become effective (e.g., agreements between companies that address the conditions of cross-border data transfers)

Figure 13

Risk and Measures ~ Risks associated with government actions and e.g. of measures ~

Legend	Organizational Prevention/reduction of the probability	Reduction of impact	Legal	Technical
Direct a Restriction on data transfer/business activities (data localization) ¹ b Forced access to data (government access)	Decentralize/duplicate critical data • Confirm storage location/services • Decentralize critical data Respond to requests • Establish local data center • Establish local management team Comply with and handle exceptional measures	Review alternative data/operations • Reduce impact by reviewing alternative data and operations	Conclude contracts with business partners • Obligation to obtain approval for transfer and storage • Disclaimer and indemnification details in case of negligence	Store encryption keys • For cases where the storage of encryption keys can meet regulation requests
Indirect c Mandatory data sharing/disclosure	Examination/ Selection of Storage Location • Confirm storage location/services • Select storage location/ data transfer Process/anonymize stored data Establish internal guidelines for data transfer	—	Conclude contracts with business partners • Reporting obligation in the event of government access • Disclaimer/indemnification details in case of negligence	Encrypt data • Encrypted so that content cannot be understood in the event of forced access
	Review strategies/operations on the assumption of data disclosure	Conclude contracts with business partners • Reporting obligation in the event of government access • Disclaimer/indemnification details in case of negligence	Establish contracts/guidelines with business partners • Define target data, scope of disclosure, terms of use, etc. • Include legal requirements	Use digital watermarking/blockchain • Prevent unauthorized copying or improvement of data protection

1. This could include regulations that conditionally allow cross-border transfers, but in that case since these measures are indirect regulations in which the govt orders company, actions against "risk from govt actions(indirect)" become effective (e.g., agreements between companies that address the conditions of cross-border data transfers)

4 Major Related Laws and Regulations (EU, China, U.S.)

- Laws and regulations related to data vary widely by country and region, and new regulations are being considered and implemented daily. This section summarizes the regulations in EU, China, and the U.S., which are particularly important in relation to Japan.
- In the EU, comprehensive data-related law and regulation is being developed not only for personal data but also for wide range of industrial data to promote the data utilization and protect rights within the region (Figure 14).
 - To protect personal information, the GDPR¹² stipulates that cross-border data transfers (including re-transfers from a third country outside the European Economic Area (EEA) or international organization to another third country) are, in principle, prohibited (Article 44). Exceptionally, cross-border data transfers are allowed when the transfer is made based on an adequacy decision (Article 45), when based on appropriate safeguards such as Standard Contractual Clauses (SCC) or binding corporate rules (Articles 46/47), and when based on the exceptions in Article 49.
 - For industrial data, the Data Governance Act¹³ was adopted in May 2022 as a legal framework to promote data flow in the region and ensure its trustworthiness.
 - In addition, the Data Act¹⁴, entered into force in January 2024 and to be applicable in phases from September 2025, stipulates that data generated by connected products and related services must be accessible by users and provided to third parties on FRAND terms (fair, reasonable and non-discriminatory terms) upon request by users. In principle, data holders must make product data and related service data that are legally and readily available accessible to users, including metadata, in the same quality as is available to the data holder, free of charge and, where technically feasible, on a continuous and real-time basis (Article 4.1). Upon request by users, data holders shall provide readily available data to third parties (Article 5.1). As a condition for data provision, if B2B data sharing is mandatory, it is stipulated that the data holder shall provide the data to third parties in a transparent manner under FRAND terms (Article 8). In addition, the concept of consideration for making data available is stipulated in Article 9. It also stipulates that data must be made available to public authorities in emergency or exceptional cases (Article 14/15).
 - With the development of international sustainability and environmental regulations, such as the EU Battery Regulation¹⁵, the Corporate Sustainability Reporting Directive (CSRD)¹⁶, and the Corporate Sustainability Due Diligence

¹² Personal Information Protection Commission, “EU (foreign regulations) ”
<https://www.ppc.go.jp/enforcement/infoprovision/EU/>

¹³ National Diet Library, “[EU] Data Governance Law”
https://dl.ndl.go.jp/view/download/digidepo_12360274_po_02930205.pdf?contentNo=1

¹⁴ European Commission “Data Act” <https://digital-strategy.ec.europa.eu/en/policies/data-act>

¹⁵ European Commission “Batteries” https://environment.ec.europa.eu/topics/waste-and-recycling/batteries_en#law

¹⁶ European Union “EN - CSRD Directive” <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464>

Directive (CSDDD)¹⁷, there are more cases where disclosure of traceability-related data is required.

- In China, the “Comprehensive National Security Concept” proposed by President Xi Jinping outlines fundamental policies for maintaining national security (including economic and social development)¹⁸, and is embodied in the National Security Law. As part of data control by the state, the so-called three data laws (Cybersecurity Law, Data Security Law, and Personal Information Protection Law) define cooperation with government intelligence gathering activities and data localization (Figure 15).
 - The Cyber Security Law stipulates that personal information and critical data collected and generated by critical information infrastructure operators during their operations in China must be stored in the country (Article 37). When it is necessary to provide the information outside the country for business purposes, a security assessment must be conducted based on the regulation jointly formulated by the national network information department with the relevant departments of the State Council (Article Ibid.).
 - The Data Security Law stipulates that security management of cross-border transfer of critical data collected and generated in China by critical information infrastructure operators shall be governed by the provisions of the Cybersecurity Law (Article 31). Penalties for illegal cross-border transfers of critical data (Article 46) are even stricter than those in the Cybersecurity Law¹⁹.
 - The Personal Information Protection Law defines the necessary measures and requirements for the cross-border transfer of personal data (Chapter 3).
 - There is some ambiguity in the interpretation and operation of the scope of those regulated by the three data laws and the scope of data subject to such obligations. In September 2022, the “Security Assessment Measures for Cross-border Data Transfer” was promulgated, defining critical data as “data that, once tampered with, destroyed, leaked, or illegally acquired or used, may threaten national security, economic operation, social stability, public health, and safety” (Article 19). In March 2024, the Cyberspace Administration of China (CAC) promulgated and enforced the “Regulations on promoting and standardizing cross-border flows of data” for the implementation of the three data laws²⁰. This regulation requires data handlers to identify and declare critical data based on the relevant provisions, but in cases where the relevant department or region has not notified, published, or announced the criteria of critical data, they are not required to declare the security assessment for cross-border transfers of critical data (Article 2). For example, in the automotive sector, the “Regulation on Management of Automobile Data Security (trial)” (entered into force in October 2021) has been established.

¹⁷European Commission “Corporate sustainability due diligence” https://commission.europa.eu/business-economy-euro/doing-business-eu/sustainability-due-diligence-responsible-business/corporate-sustainability-due-diligence_en

¹⁸ 新華網「习近平主持召开中央国家安全委员会第一次会议强调 坚持总体国家安全观 走中国特色国家安全道路 李克强张德江出席」(April 2014) http://www.xinhuanet.com//politics/2014-04/15/c_1110253910.htm

¹⁹ JETRO “Overview of the data security law” https://www.jetro.go.jp/ext_images/_Reports/01/580a6448fa87f0bb/20210056_04.pdf

²⁰ Research department, JETRO Shanghai, “Recent developments in China’s regulations on cross-border transfers of data and personal information (as of March 2024)” (April 2024) https://www.jetro.go.jp/ext_images/_Reports/01/690307ed2a411652/20240004_02.pdf

- In the U.S., free economic activity and data flows in the market are generally respected and emphasized, and there are few laws and regulations to impose restrictions on cross-border data transfers, but some state-level personal information protection laws and data regulations for national security purposes exist (Figure 15).
 - For example, the CLOUD Act²¹ clarifies that in cases involving criminal investigations or national security, U.S. government may, by warrant or otherwise, compel providers subject to U.S. jurisdiction to store, back up, or disclose data held outside the U.S. (103(a)(1), 18 U.S.C. Sec. 2713).
- It is important to regularly check and understand the latest trends in data-related laws and regulations, as they are changing rapidly due to diverse means of data access and the expansion and extension of the interpretation of laws and regulations.
 - It is also recommended to check the original text of descriptions and survey results of each country's system on the websites of METI and JETRO²², as needed. When identifying problems with laws and regulations, it is also recommended to check their consistency with existing international rules, such as WTO agreements and economic partnership agreements agreed to by the counterpart countries. In addition, for laws and regulations expected to have a significant impact, it is recommended to consult with experts.
 - If public comments gathering are solicited during the development of the system, companies can participate in them and visualize their concerns.

Figure 14

Major Related Laws and Regulations (EU)

	Purpose etc.	Key requirements regarding data	Anticipated risks	Status
Data Governance Act (EU)	<ul style="list-style-type: none"> Facilitate the circulation of data in the EU Economic Area and ensure trustworthiness 	<ul style="list-style-type: none"> A legal framework for promoting data flows and ensuring trust within the region has been defined and presented 	–	<ul style="list-style-type: none"> Enter into force in Jun 2022 Start to apply in Sep 2023
Data Act (EU)	<ul style="list-style-type: none"> Ensure data utilization/fairness, esp. for industrial data 	<ul style="list-style-type: none"> Data generated from the use of connected products or related services within the EU must be accessible to the user When it is necessary to respond to a public emergency, Data must be provided to public sector agencies etc. 	<ul style="list-style-type: none"> Data sharing/disclosure obligation Additional man-hours or disclosure of confidential data may be required to meet data disclosure requirements Government access In an emergency, there is the possibility of government access 	<ul style="list-style-type: none"> Enter into force in Jan 2024 Start to apply in phases from Sep 2025 onwards
Battery Regulation (EU)	<ul style="list-style-type: none"> Enhance sustainability, recycling, and safety over the entire life cycle of storage batteries (batteries) 	<ul style="list-style-type: none"> Disclosure of data to ensure transparency and sustainability of the battery is mandated <ul style="list-style-type: none"> Rate of carbon footprint/recycled materials over the entire life cycle Battery passport (incl. model info, performance, chemical composition, life expectancy, etc.), etc. 	<ul style="list-style-type: none"> Data sharing/disclosure obligation In order to release battery-related data, additional man-hour, disclosure of sensitive info or info directly related to competitive advantage may be required 	<ul style="list-style-type: none"> Enter into force in Aug 2023 Start to apply in phases from Feb 2024 onwards

²¹ Nishimura & Asahi, Nishimura Institute of Advanced Legal Studies (“NIALS”) Report by the “CLOUD Act Study Group” (Ver. 2.0 April 2023) <https://www.nishimura.com/en/knowledge/publications/92692>

²² One example is the “Unfair trade report” compiled by the Trade Policy Bureau, METI https://www.meti.go.jp/policy/trade_policy/wto/3_dispute_settlement/32_wto_rules_and_compliance_report/321_past_report/compliance_report.html

Figure 15

Major Related Laws and Regulations (China/the U.S.)

	Purpose etc.	Key requirements regarding data	Anticipated risks	Status
National Security Law (China)	<ul style="list-style-type: none"> Maintain national security (incl. economic and social dev) 	<ul style="list-style-type: none"> It primarily embodies principles related to national defense and establishes basic principles Specific requirements for data are supported by three data laws (cybersecurity, data security, and personal information protection laws) 	—	<ul style="list-style-type: none"> Start to apply in 2015
Cybersecurity Law (China)	<ul style="list-style-type: none"> Manage overall security in cyberspace (focus on network infra protection) 	<ul style="list-style-type: none"> Personal information and "important data" must be stored in China Obligation to provide technical cooperation and data to the government as necessary, for criminal investigations conducted by public or national security agencies 	<ul style="list-style-type: none"> Localization <ul style="list-style-type: none"> If the data concerns national security, transfer out of the country is prohibited Government access <ul style="list-style-type: none"> May be asked to provide various data in criminal investigations 	<ul style="list-style-type: none"> Start to apply in 2017
Data Security Law (China)	<ul style="list-style-type: none"> Focus on data protection, defining/protecting important data 	<ul style="list-style-type: none"> For cross-border transfers of "important data" from China, the provisions of Law must be complied with Data processors must implement security control to address security risks 	<ul style="list-style-type: none"> Localization <ul style="list-style-type: none"> Data positioned as important data to China may be difficult to transfer cross-border out of the country 	<ul style="list-style-type: none"> Start to apply in 2021
Personal Information Protection Law (China)	<ul style="list-style-type: none"> Of Data Security Law, complement the regulation of personal data 	<ul style="list-style-type: none"> Companies and organizations are required to obtain individual consent/ensure security requirements for cross-border transfers of personal information from within China 	<ul style="list-style-type: none"> Localization <ul style="list-style-type: none"> If the requirements cannot be met, the data cannot be transferred 	<ul style="list-style-type: none"> Start to apply in 2021
CLOUD Act (the U.S.)	<ul style="list-style-type: none"> Strengthen int'l investigation cooperation and enhance national security 	<ul style="list-style-type: none"> Cloud service providers based in the U.S. may be obligated to access/provide the data upon request by the U.S. government, even if the data is stored outside the U.S. 	<ul style="list-style-type: none"> Government access <ul style="list-style-type: none"> Companies' info may be subject to government access via U.S.-based cloud service providers 	<ul style="list-style-type: none"> Start to apply in 2018

5 Anticipated Risks and Actions

5.1 Restriction on Data Transfer and Business Activities (Data Localization)

- In visualizing risks in “a. Restrictions on data transfer and business activities,” understand concerns that authorities may impose domestic storage requirements, prohibition of transfers out of the country, and mandatory use of data centers in the country.
 - Data localization measure can be classified into, for example, domestic storage requirements, domestic processing requirements, and prohibition of cross-border transfers²³. Domestic storage requirements specify the location of data storage and are intended to allow overseas transfer and processing (use, editing and changing) if a copy is stored in the country. Domestic processing requirements specify the location where data is primarily handled, and are intended not to allow processing (use, editing and changing) outside of the country. Prohibition of cross-border transfers is intended to prohibit cross-border transfers, including overseas access, (including cases allowing cross-border transfers with conditions).
 - In China, for example, the so-called three data laws (Cybersecurity Law, Data Security Law, and Personal Information Protection Law) define data localization of industrial data, but the defined scope and targets are broad and unclear²⁴. The cybersecurity law, for example, targets broad range of entities, such as operators of critical information infrastructure in China and data processors who handle personal information of more than one million people. The targets include a wide range of sectors, including automotive, military, industrial, etc., and the definition is unclear. The Cyberspace Administration of China (CAC) evaluates whether the data is important or not upon application and if the data is judged important, it is not allowed to be transferred across border.
- In risk assessment, it is recommended to identify data and processes subject to laws and regulations, examine impact and content of risks, and determine the impact to the company and the priority of response (Figure 16).
 - It is recommended to check whether any data subject to regulations could result in losses for the company, such as confidential or secret data.
 - It is also recommended to grasp what restrictions and exceptions are available for the legal application processes, based on the said categories of data localization measures.
 - In particular, if authorities have broad discretion in determining whether the data is subject to the restrictions on cross-border transfers which resulting in low predictability regarding the scope and interpretation of the regulations, it becomes more difficult for companies to determine whether transfer is allowed, necessitating caution. It is also necessary to pay attention to the stability of the system, such as the frequency of operational changes and the possibility of repeal of the law.

²³ Yukiko Konno, “An Examination of Data Localization: A focus on its impact on businesses and policy objectives (March 2024)” [RIETI - An Examination of Data Localization: A focus on its impact on businesses and policy objectives](#)

²⁴ Same as the above

Figure 16

Anticipated Risks and Risk Assessment

~ Related laws/regulations and perspectives for identifying risk ~

	Related laws and regulations (e.g.)	Perspectives for identifying risk	Legal application process
a Restriction on data transfer/ business activities (data localization)	Cybersecurity Law (China) Data Security Law (China)	<input type="checkbox"/> Does this involve data (such as confidential or secret data) that could lead to loss for the company? - Undisclosed proprietary data - Data can be misused by third parties - Leakage may lead to breach of contracts, etc.	<input type="checkbox"/> What are the extent of restrictions? - Domestic storage requirements - Domestic processing requirements - Prohibition of cross-border transfer, etc. <input type="checkbox"/> Are there any exceptional measures?
b Forced access to data (government access)	Data Act (EU) Cybersecurity Law (China) CLOUD Act (the U.S.)	<input type="checkbox"/> The data subject to the requirement has not been explicitly defined; could it potentially include a wide range of data?	<input type="checkbox"/> Are the grounds/procedures for data access clearly defined? <input type="checkbox"/> Are there any provisions outlining protective measures, such as lodging objections or holding consultations?
c Mandatory data sharing/ disclosure	Data Act (EU) Battery Regulation (EU) Corporate Sustainability Due Diligence Directive (EU)		<input type="checkbox"/> What are the extent of the scope of disclosure and sharing? <input type="checkbox"/> How will the data be used after sharing?

- Possible measures include designing business operations to minimize or eliminate impact from data transfer restrictions and establishing business schemes without cross-border transfer (Figure 17).
 - To design business operations to minimize or eliminate impact from data transfer restrictions, measures such as data decentralization, data substitution, and business alternatives are expected to be taken so that business can continue even if the data is subject to transfer restrictions. If domestic storage requirements (no restrictions on cross-border transfers) are imposed, data can be duplicated and dispersed to locations outside of the country. If the data use outside of the country is restricted by domestic processing requirements or prohibiting cross-border transfers, similar data can be used as a substitute for the data and operations. As an example of the latter case, consider the case in global supply chain management in which production data (e.g., capacity tightness, production lead time, defective rate) is shared from production bases in each country to the head office, and a global supply plan is developed at the head office. In this case, if the relevant data in the country cannot be obtained due to restrictions on cross-border transfers, the accuracy of the plan is assumed to be reduced, but a prospective plan is assumed to be developed based on the past supply volume as alternative data. In addition, if cross-border transfers are permitted under certain conditions, measures to comply with those requirements are also needed to be taken. In recent years, the Intra Group Data Transfer Agreements (IGDTAs), which incorporate provisions compliant with these regulations into a single agreement, have become widely used to simultaneously comply with regulations of multiple countries. It would also be useful to incorporate measures needed to comply with the requirements into the contract in advance, not only for the company, but for suppliers.
 - As an example of the measures to establish a business scheme without cross-border data transfer, companies may have to consider transferring generation,

use, and storage of data in the country to another, instead of sharing and utilizing the relevant data in that country, when that country is under consideration for the introduction of legal regulations. In this case, it should be noted that significant changes in business structure and operations will be required.

- When providing data analysis services, for example, there may be no other way but to set up a local team to complete the process of generation, utilization, and storage in the country and provide services to meet the domestic storage and processing requirements. Companies may consider such an option if that country intends to impose mandatory data localization or other regulations that pose serious legal or business risks to the interests of the business or shareholders. In this case, it should be noted that complex business decisions will be required as well.

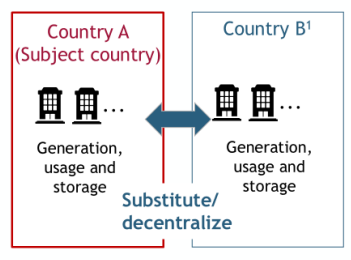
Figure 17

Measures to Address the Anticipated Risks

~ Restriction on data transfer/ business activities (data localization) ~

Design business operations to minimize or eliminate impact from data transfer restrictions

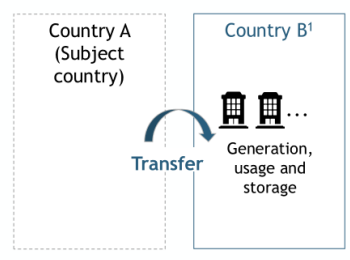
- Take measures to ensure business continuity even if subject to data transfer restrictions
 - Decentralize data
 - Substitute data/operations
 - Comply with conditions (in case of conditional cross-border transfers are permitted)



Establish a business scheme without cross-border data transfer

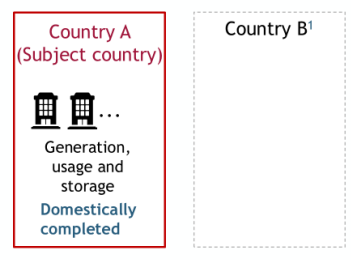
No related data sharing/utilization in the subject country

- Transfer the generation, usage, and storage of data subject to data localization/local processing requirements to another country
- This represents a significant change in business structure and operations; must examine the constraints and feasibility of implementation



Related data sharing/utilization in a manner closed to the subject country

- Complete the generation, usage, and storage within the subject country
 - Build a data center in the subject country and set up an operation unit
 - Use local services, etc.
- A study of cost/talent feasibility for business benefits is recommended



1. Country B refers to any country other than Country A (the subject country), incl not only the home country of the business but also any other country in general where data transfer may be executed

5.2 Forced Access to Data (Government Access)

- In visualizing risks in “b. Forced access to data,” identify concerns that authorities may impose access and disclosure requirements on confidential and secret data, mainly for emergency response, criminal investigations, and national security.
 - The EU Data Act, China’s Cybersecurity Law, and the U.S. CLOUD Act, include provisions on government access for emergency response, criminal investigation, national security, etc.
 - On the other hand, for example, under the WTO’s Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), member states are internationally obligated to ensure effective protection against disclosure or use of undisclosed information in a manner contrary to fair commercial practice without the consent of the owner.
- In risk assessment, it is recommended to identify data subject to regulations and application processes and determine the impact to the company and the priority for response.
 - It is recommended to check whether any data subject to regulations could result in losses for the company, such as confidential or secret data.
 - As a legal application process, it is recommended to confirm the basis and procedure for government access to occur, and the existence of safeguards, such as objections and consultations.
 - In addition, to understand the characteristics of the anticipated government access, it is recommended to verify the aspects: compulsory nature (e.g., whether it involves enforcement regardless of penalties, or voluntary/discretionary provision), the target data life cycle (e.g., whether derived from data generation/acquisition, or data processing/usage), and the destination of data (e.g., whether directly to the government, or to a government-designated organization (including private entities)).
 - The Center for International Economic Collaboration (CFIEC) has compiled an analysis of the disciplinary elements and examples of government access in its “Report of the Study Group on Government Access and Trade Rules” (revised November 2022)²⁵, which can be referred to for further details. However, this area is frequently updated, requiring a separate confirmation for the latest information.
- Possible measures include restricting data transfers to avoid government access within the subject country and preparing for cross-border government access from other countries (Figure 18).
 - To restrict data transfers to avoid government access within the subject country, one possible measure would be to control and restrict transfer, provision, and storage of data subject to government access. It is recommended to identify and understand the important data that is both beneficial and at risk to the company, and to take necessary measures. Possible measures include, for example, selecting storage locations and services that are assumed to have low risk (e.g., no relevant regulations, no or few enforcement records, clear rationale and implementation process, defined protective measures), restricting transfers to the subject country and transactions with companies from such countries.

²⁵ <https://www.cfiec.jp/jp/pdf/gov/gov-2022-11-complete.pdf>

- To prepare for cross-border government access from other countries, protection measures can be considered for data that may be subject to cross-border government access. As domestic protection measures and restrictions on data provision to other governments, it is anticipated to check and consider whether there are any applicable provisions in existing domestic laws or international trade agreements, as well as international government access rules and principles discussed at the OECD, G7, and G20. As a example, undisclosed test data for medical and agricultural chemicals submitted to the government as a condition of marketing approval are protected under Article 39.3 of the TRIPS Agreement. In addition, the chapter on electronic commerce in the Comprehensive and Progressive Agreement on Trans-Pacific Partnership (CPTPP) includes a provision (Article 14.17) that prohibits disclosure or access to source code of software owned by parties from other country as a condition for importing or selling source code.
- In addition, technical safeguards could be introduced. For example, data could be encrypted or anonymized in advance of a government access request.

Figure 18

Measures to Address the Anticipated Risks

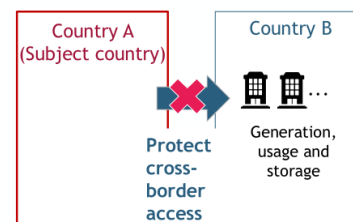
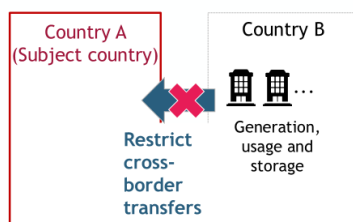
~ Forced access to data (government access) ~

Restrict data transfers to avoid government access within the subject country

- Control/restrict data transfer and storage for data may be subject to government access within the country
 - Select storage locations/services with presumed lower risk levels
 - Restrict transfers to the country and transactions with companies in that country
- Properly identify that is both valuable to the company and exposed to risks within the processed data, and take measures

Prepare for cross-border government access from other countries

- Take actions against data that may be subject to cross-border government access from other countries
 - Identify/apply restrictions on data submission to other governments within own country (e.g., international trade agreements, national laws)
 - Introduce technical safeguards



5.3 Mandatory Data Sharing and Disclosure

- In visualizing risks in “c. Mandatory data sharing and disclosure,” identify concerns that data sharing and disclosure is mandatory for corporate activities based on relevant regulations.
 - For example, the EU Data Act allows access to generated and processed data of connected products and services by users of such products and services in the EU, and mandates data provision to users upon their request or to third parties. Product manufacturers are concerned about increased costs due to product development and specification changes, and leakage of product know-how, depending on the scope of data provided and disclosed.
 - The EU Battery Regulation requires disclosure of information such as carbon footprint (CO₂ emissions), corporate due diligence and audits (risks of environmental pollution and human rights violations) throughout the entire product life cycle, from acquisition of raw materials to final disposal and recycling. OEMs (finished product manufacturers) and suppliers are concerned about increased costs for data collection and visualization, and sales injunctions in the region in the event of failure to comply. It also stipulates that certification will be performed by certification bodies based in the EU, and risks must be appropriately assessed in the institutions and countries and regions where supply chain data and battery composition (design data) are stored.
 - Various ESG and sustainability-related regulations will be adopted and will start to apply in the future. For example, the EU Corporate Sustainability Due Diligence Directive (CSDDD), applicable in 2027, requires companies to implement measures to control, identify, and mitigate adverse human rights and environment-related impacts in value chains and to disclose the status of activities, which may require extensive data disclosure.
 - Such regulations for ESG and sustainability require companies to collect data not only on themselves and their business partners (with business contracts), but also on companies not directly trading with them throughout the supply chain. In addition, there is a risk that data needed for legal compliance cannot be disclosed if restrictions on data transfer and business activities (data localization) in 5.1 make it difficult to obtain data from business partners in specific regions or countries.
- In risk assessment, it is recommended to identify data and legal application processes and determine the impact to the company and the priority to respond.
 - Regarding the data subject to regulation, discussions are currently underway within the EU expert group on the scope and definition of such data in the context of the EU Data Act, particularly concerning provision of connected products, related services and data processing services. For manufacturers of related products, the impact on them may vary depending on whether the data is currently collected exclusively for maintenance or equipment operating data that is intended to be disclosed and used by users. As the regulations become more concrete, it will be necessary to closely monitor the definition of data subject to regulations.
 - For legal application processes, it is recommended to identify and confirm to whom and to what extent data will be disclosed, and how disclosed data will be used by the recipients.

- In cases where data is disclosed in response to a business partner's request, it is considered effective to make an appropriate contract or arrangement with them in advance on the scope of disclosure, notification and response to disclosure, etc. The proposed items to be basically agreed upon in the contract for data sharing and utilization are as follows (Figure 19). As described in 3.5 “Organizing Risks and Actions,” the following appropriate contracts and arrangements with business partners are effective for “risks from private companies' actions” as well.
 - The basic items should be agreed upon can be categorized into: “Provisions for the data provided and its use,” “Validity scope/duration & response in case of non-performance/dispute,” and “Other and general matters.”
 - For the above, it is also considered effective to examine and agree on arrangements among the parties by contents and requirements of the regulation. Under the EU Data Act, for example, it is considered useful for product manufacturers and distributors to agree in advance with users on the scope of third-party sharing and its conditions when disclosing data to third parties upon request by the user or the user's agent. In addition, when the EU Battery Regulation requires suppliers to disclose and provide data to OEMs (finished goods manufacturers) on carbon footprint (CO2 emissions) and corporate due diligence and audits (violation risks of environmental pollution and human rights), it is considered effective for suppliers to agree with OEMs on the content and calculation logic, provision method, and format for efficient data sharing and collaboration.
 - With regard to the EU Data Act, Model Contractual Terms (MCT) are being developed for three contractual relationships: between users and data holders, between data holders and data recipients, and between users and data recipients. These are scheduled to be published before the Act takes effect in September 2025. However, they are not to be used as they are, like SCCs for complying with the GDPR's cross-border transfer regulations, rather, they are intended to be used as a basis for operators to create contractual clauses based on them.
 - For data sharing and usage agreements between companies, METI's “Contract Guidance on Utilization of AI and Data²⁶” and “Data Linkage Infrastructure Agreement Ver. 1.0²⁷” provide details and model terms as templates for the basic items to be agreed upon in the manual, please refer to them for details.

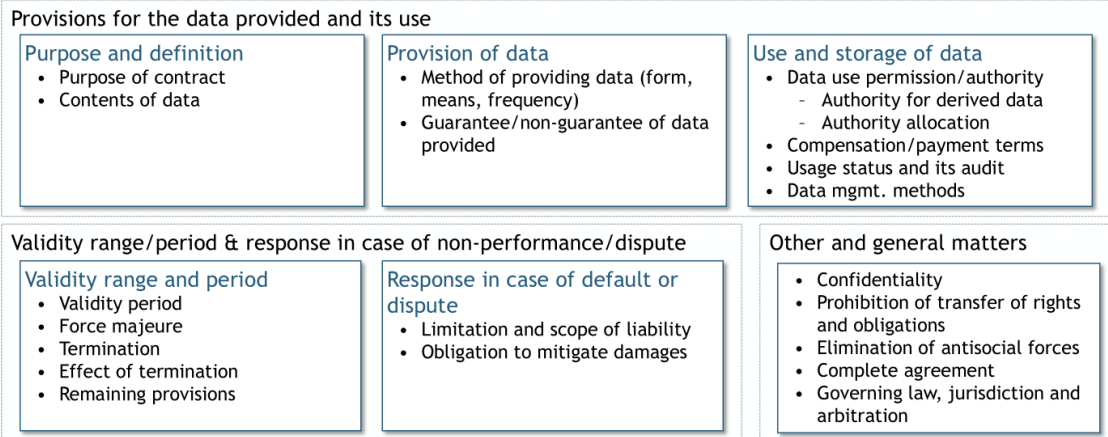
²⁶ https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20200619002.pdf

²⁷ https://www.meti.go.jp/policy/mono_info_service/digital_architecture/model_kiyaku.pdf

Figure 19

Measures to Address the Anticipated Risks ~ Mandatory data sharing and disclosure¹~

E.g. of data sharing/utilization contract items



1. This could be effective actions to address not only “mandatory data sharing/disclosure” for risks associated with government actions, but also risks associated with private enterprise actions in general

(Supplemental) Conflict of laws, policy index on cross-border data

- As companies expand their business to multiple countries, there are more situations where they need to comply with laws and regulations in different countries and regions.
- With different laws and regulations in countries and regions, it is becoming increasingly important to recognize and evaluate whether there is a conflict of laws where multiple laws with different contents are applied.
- The Global Data Alliance, a cross-industry business alliance dedicated to digital economic growth and innovation through international, trusted, and free data distribution and transfer, has released “the Cross-Border Data Policy Index²⁸” in 2023, which evaluates cross-border data policies in 100 economies. Please refer to this index for an overview and characteristics of policies by region.

²⁸ <https://globaldataalliance.org/resource/cross-border-data-policy-index/>

6 Conclusion

- Regulations concerning data across different countries and the state of international data sharing and utilization among companies are rapidly evolving, encompassing a wide range of related themes. The “Industrial Data Sub-Working Group” in FY2024 determined major themes and issues to be explored in depth in the future as follows: updating and expansion of information on related laws and regulations (cloud computing regulations, laws and regulations in Asia and the Global South, etc.), collection and dissemination of best practices (collection of best practices and dissemination of information through seminars, panel discussions by experts, etc.), the ideal organizational structure including roles and responsibilities for industrial data, and the direction of support for companies with limited personnel and resources such as SMEs. Based on the content and progress of relevant international and domestic discussions, updates will be made as needed in the future.

Industry Data Sub Working Group Member List

(Members)

Chair	Naoto Ikegai	Professor, Graduate School of Law, Hitotsubashi University
	Hiroyuki Ishii	GM, Industry Data PF Group, IT Management Division, Toyota Motor Corporation
	Osamu Ishihara	Senior Chief Engineer, Managed & Platform Services Business Division, Cloud Service Platform Business Unit, Hitachi Ltd. Japan
	Kyoko Izumi	Vice President, Japan Intellectual Property Association
	Koji Kono	General Manager for research and analysis, General Affairs Planning Department, Information-technology Promotion Agency, Japan
	Toshihiro Suzuki	Senior Director, Standards Strategy & Architecture/Government Affairs, Oracle Corporation Japan
	Tomoko Naoe	Director - Policy, Japan, Global Data Alliance/Business Software Alliance
	Kazuo Nakashima	General Manager, Industrial IoT, Robot Revolution & Industrial IoT Initiative
	Rie Hamada	Group Manager, Strategic Planning Department, DX Innovation Center, Intellectual Property Licensing Group 4, Legal and External Relations Department, Mitsubishi Electric Corporation
	Kenta Hiram	Associate Professor, Faculty of Social Sciences, University of Nagasaki
	Kojiro Fujii	Partner, Nishimura & Asahi (Gaikokuho Kyodo Jigyo)
	Mitsuo Wakameda	Director, Data Society Alliance
	Mariko Watanabe	Professor, Department of Management, Faculty of Economics, Gakushuin University

(Gojuon order without honorifics)

(Observers)

International Strategy, Group of Service for Citizens, Digital Agency
Global Strategy Bureau, Ministry of Internal Affairs and Communications
Personal Information Protection Commission Secretariat

(Project management office)

Office of International Affairs, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
Boston Consulting Group