METI
Ministry of Economy, Trade and Industry

Summary

Interim Report

Expert Group on Data Free Flow with Trust

February 28, 2022

- Table of Contents -

1. Key Points of the Report

- In order to embody the vision of "Data Free Flow with Trust (DFFT)", it is essential for **countries that share basic values to seek interoperable solutions across different forms of data governance while respecting the regulatory demands such as privacy, security, and intellectual property.**
- In addition, to facilitate cross-border transfer of data, **"trust"** must **exist** not only between governments, but also **between all stakeholders in data life-cycle**, including companies, natural persons, regulators, and international organisations.
- Therefore, the discussion on operational instruments and mechanisms to embody the DFFT should include in its scope the **identification of and solution to the barriers that currently exist in the relationships among all of these stakeholders** beyond previous G2G-focused approaches.

➢ This report focuses on the following three issues in company interviews and surveys of regulations in each country.

① How are cross-border data transfers taking place in dairy business operations of companies (identification of the data life-cycle, stakeholders involved in the lifecycle, and patterns of cross-border transfers)?

② Alos, what barriers do companies face in transferring data across borders?

③ What are the main perspectives regarding data-related regulations in each country?

2. The Data Life-cycle and Barriers to Cross-border Transfers

Type 1 Online Apps Providers and Developpers

■Outline

The analysed data of customer's basic information (name, gender, region..) and the patters of Apps usage are combined with other data such as data provided by public sectors to improve and develop the applications and services.

■Data Management Methods

Data collected from customers is firstly stored in the cloud in each region, structured and integrated to some extent there, and then transferred to the cloud in the country where the R&D headquarter is located. Since engineers and other personnel are hired globally, the companies consider that internal "cross-border access" also occurs even during online-meetings, in addition to data-analysis, development of applications, etc.

The data life-cycle

Production of Data

A) Data Status

- Data is generated through customers' use of Apps. The two main types of data are customers' information and customer usage data.

(B) Company requests

- It is preferable if we can flexibly choose to consolidate data in the region where R&D headquarter is located or to manage in a cloud in each region, depending on the market environment.

(C) Challenges from the company's perspective

- The requirements for extraterrestrial transfer of data differ from country to country, and the requirements for consent for personal data also vary depending on the purpose of use, so it is difficult to take a standardized approach internationally. In the case of third-country provision of data, compliance with the laws of the destination country is also required, which adds high compiance cost.
- If laws differ from country to country, the barriers of market entry are too high for startups and SMEs, as they need to have one storage site per country for conducting pre-cross-border processing.

Process

A) Data Status

- From the viewpoint of work efficiency and compliance with laws, the engineers must perform processes such as separation of personal data before the data 'crosses' the border.

(B) Company request

- It is preferable if we can flexibly choose to consolidate data in the region where R&D headquarter is located or to manage in a cloud in each region, depending on the market environment.

(C) Challenges from the company's perspective

- The definition and requirements for "personal data" are difficult to interpret because the substance of regulation extends not only to the regulations themselves, but also to guidelines and related administartive agreements.
- As more data collected and consolidated, what constitutes "personal data" becomes more difficult to define.
- We are often not sure if a concrete case of data integration or "access" to the data between multiple regions constitutes a "cross-border transfer" even in processing. This uncertainity causes considerable chilling effects.

Transfer

A) Data Status

- Data is consolidated at R&D sites. Transfer the data to the cloud in the region where the R&D team is located or store the processed data in an environment that the R&D team can use.

(B) Company request

- Due to telecommunication of cross-border data access costs a lot, we would like to consolidate data where R&D resources are available.

(C) Challenges from the company's perspective

- The definition of "personal identifiability" is not always clear in actual cases under the laws of each country.
- Even if the data is anonymized, etc, it may be subject to regulation as 'critical information' which can be designated within governments' descretion.
- It is difficult to comply with the requirements of laws when receiving information from third countries.
- Even if they want to develop big data across multiple regions, we are unable to take the plunge due to differing laws of each country and uncertainties in their interpretation.

Type 2: Transfer of collected data to an overseas third-country company for outsourcing of operations

■Outline

Providers of mobile payment services and online booking platform services uses clouds to provide its services, and outsources some of its operations to an overseas company.

■Data Management Methods

Data generated by customer App usage is used to improve the user experience, to improve and develop services, and to link payment apps with other companies' apps and services. Data used to improve the user experience, etc., is collected and stored in each region, where it is used and processed, but cross-border access or cross-border transfers occur due to the outsourcing of some operations to overseas providers.

The data life-cycle

Production of Data

A) Data Status

- Data is generated on customers use of Apps. The two main types of data are customers' information and customer usage data.

(B) Company requests

- Data related to user experience improvement will basically be stored within each region and processed and analyzed locally. However, since the relevant companies outsource many of their operations to overseas service providers, they face the uncertainty of the system of laws regarding cross-border transfers.

Process

A) Data Status

- Engineers hired from overseas access and process data located within each region.

(B) Company requests

- In the relevant industry, the division of labor along the lines of expertise is increasing. Outsourcing analysis and other work overseas is basic assumption of business while keeping data stored in the region from the perspective of user experience. Thus the uncertainity regarding cross-border access is getting serious.

(C) Challenges from the company's perspective

- The conditions for "cross-border transfer" are unclear. Does this also apply to data access from outside the region or when employees physically move outside the region to access the data?
- The definition of "cross-border transfers to a third country" is also unclear.

Transfer

A) Data Status

- Cross-border transfer of data to a third country.

(C) Challeges from the company's perspective

- Regulations regarding personal data protection in major countries require the business that they ensure that their counterparts provide the 'adequate' level of data protection of the data management system and operation as the data-origin country. This responsibility of the company to check and confirm the adequacy of the protection in the destination country despite the difference of regulatory approaches impose the disproportionate burden on the business.
- The definition of "contractor"(the third party) that affects the scope of obligation is ambiguous under the laws of each country. (An organization's "subsidiary" may become a "contractor" under the laws of the relevant countries.)

Type 3: Real-time data collection and analysis from overseas via IoT

(when personal information is not included)

■Outline

By utilizing an IoT platform to collect and analyze real-time data on utilities' operating conditions, operating environments, repairs, etc., for devices sold globally, the companies will be able to predict the occurrence of failures and make maintenance plans optimized based on such data.

■Data Management Methods

Up to the present, the data is still stored at the acquisition site most of the times. In the future, it is desirable that the data is automatically sent via IoT to cloud servers in the region of the headquarter and other relevant locations for data use and analysis. Since data acquired from sensors in this category is collected from IoT devices that are usually not for individual/house-hold use, personal data is not supposed to be included, but as data pertainig to security can be included, and hence, cross-border transfer of data may be restricted.

The data life-cycle

Production, Transfer and Process

A) Data status and life-cycle

- Data is obtained from sensors installed in the sold devices such as air-co, lights, etc
- Consolidate information acquired from sensors. (At this time, the data is stored individually at the acquisition site, but we would like to make use of it in the future.)

(B) Company request

- There is little analysis of regional differences in information obtained from IoT devices for purposes other than marketing of specific regions. We would like to consolidate our analysis in one place for product development, failure prediction and system construction.
- We would like to transfer the information obtained from the sensors directly to a server located at the headquarters location.

(C) Challenges from the company's perspective

- Regulations regarding data other than "personal data" continue to increase, and in some countries, even information that has absolutely no link to personal information (e.g., information on the flow of people at a particular station) may be prohibited from being taken out of the country. However, if the process of human intervention must be added to separately scrutinize collected information whether it can and cannot be crossed borders due to the regulatory uncertainty, the characteristics of IoT, such as the advantages of real-time monitoring, will be undermined.

Type 4: Real-time data collection and analysis from overseas via IoT
(when personal information is included)

■Outline

For devices and other products sold globally, the IoT platform will be used to collect and analyze data related to equipment operations and associated operating environments, energy consumption, etc. from overseas in real time to provide product systems based on customer needs, predict the occurrence of failures, and adapt to local environments.

■Data Management Methods

Information is collected from personally owned devices, which may include personal data such as the customer's own ID. In addition, cross-border transfer of information on the operating environment of devices might be subject to restriction under relevant regulations as IoT devices can collect a wide variety of data including 'critical' 'essential' information for the government. Yet, a part of data, which is and can be restricted is also essential to the operation of the devices. Thus, a sudden change in the regulation or its interpretation could lead to a partial service outage.

The data life-cycle

Production and Transfer

A) Data status and life-cycle

- Data is obtained from sensors installed in the devices sold.
- Consolidate information acquired from sensors. Due to the nature of the IoT, data is sent directly to the headquarters or development sites.

(B) Company request

- It is preferable that it be possible to send the collected information directly and automatically from the customer's system to the site's server.
- While some information is collected to adapt to the local environment, particularly important information in relation to the business model is information on equipment operation in general (equipment and software errors, accidents and near-misses, payment information, energy consumption, etc.), it is preferable that data should be placed in multiple sites and constantly synchronized worldwide so that analysis and development work and trouble shooting can be conducted 24 hours a day, 365 days a year.

(C) Challenges from the company's perspective

- New data categories have emerged for regulations on cross-border transfer of data, including not only personal data but also non-personal data such as "security information" and "critical information." However, the scope of the regulations is extremely vague, and the scope and of information subject to the regulations is increasingly expandiong by interpretative guidance and other documents.
- In conducting real-time monitoring that takes advantage of the characteristics of the IoT, it is preferable that procedures for complying with legal requirements can be standardized and formalized to some extent.

2. The Data Life-cycle and Barriers to Cross-border Transfers

Type 5: Provision of platform services and IaaS

■Outline

Customers(business, concumers) provide user data to the platform to access a variety of services. Collected data is stored, analyzed, and processed (it can also be combined with data from other relevant sources e.g. open data from public sectors), and it can be used for advertising and promotion systems.

■Data Management Methods

All companies responded that they need to take the advatnage of big data. Some companies also responded that they adopt or should adopt decentralized approaches to data management from a security perspective, and it is essential that data can cross the border flexibly for taking back-ups. Yet, some companies responded that they are forced to manage data tied to customer accounts locally due to the high compliance costs with local regulations. They also said that the data, which is necessary for improving the user experience is normally mamaged locally.

The data life-cycle

Production of Data
(Customer data)

A) Data Status
- Customer creates an account. (Customer data, past cookie information, and browsing records, etc are collected).
- Some data will be managed and analyzed locally, while others will be transferred to and consolidated at the headquarters or R&D sites.

(B) Company request
- Decentralized management is optimal from the standpoint of security and seamless provision of services (maintenance etc).
- It is preferable to have an interoperable soluition that is simple for companies to deal with regulations in major jurisdictions. Or at least, regulations should have clear definitions, classifications, etc. for key privisions.

(C) Challenges from the company's perspective
- The definition of data restricted to transfer across borders is unclear, and the disadvantages of uncertainty is passed on to companies.
- The conditions for cross-border transfers are so complex that a wide variety of consents must be sought from customers. Not sure if the regulators understand the business reality.
- Laws in major countries impose obligations on companies to "check safety" and "check sufficiency" in third-country transfers. But we are not sure what we are asked to do in a concrete sense.

Production and transfer
(Data on customer use of services)

A) Data Status
- Service-related data and support-related data are generated by customers' use of services.
- These data are considered "non-personal data" and are transferred across borders and consolidated at the headquarters or R&D sites.

(B) Company request
- Decentralized management is optimal from the standpoint of security and seamless provision of services.
- It is preferable to have an interoperable soluition that is simple for companies to deal with major jurisdictions and regulations should have clear definitions, classifications, etc. for key privisions.

(C) Challenges from the company's perspective
- The definitions of data restricted to transfer across borders are unclear, and the disadvantages of uncertainty is passed on to companies.

Production and transfer
(Security-related data)

A) Data Status
- Service-generated data is generated by customer use of the service.
- These data are considered "non-personal data" and are transferred across borders and consolidated at the headquarters or R&D sites.

(B) Company request
- It would be preferable to be able to send security risk/threats-related information directly and automatically to the server at R&D sites.

(C) Challenges from the company's perspective
- The definition of data restricted to transfer across borders is unclear, and the disadvantages of uncertainty is passed on to companies.

Type 6: Providing cyber security services

■Outline

Providing customers security software for devices and security maintenance service for cloud environments. Collected data necessary for analysis and development of service is consolidated and centrally managed. Information determined to be a threat is also stored in a database on-premises.

■Data Management Methods

There is data provided by customers and external organizations, as well as security-related information that the company collects on its own. Data provided by customers may include personal data. In some cases, the data is sent to the R&D sites directly from the systems provided to customers, while in other cases, the data is stored and analyzed in each region. For the latter case, if a threat is determined to exist, personal data is removed before being sent to the headquarter. From the standpoint of efficiency, information should be consolidated in a single location, but from the standpoint of security and seamless service provision, it should be distributed to at least two locations so that data is always synchronized. On the other hand, it would be costly to invest in equipment and other resources to scrutinize and analyze the information for every region before cross-border transfer.

The data life-cycle

Production, Transfer and Process

A) Data status and life-cycle

- Threat-related information is sent directly from the customer's system to a server at the R&D sites.
- Collect, analyze, and process information in each region in some cases.

(B) Company request

- It would be preferable to be able to send threat-related information directly and automatically from the customer's system to the server at R&D sites.

(C) Challenges from the company's perspective

- Laws regarding personal data protection vary from country to country, and the requirements for transfer are provided as detailed requirements for each purpose of use. In addition, the laws are constructed in such a way that they cannot be understood without reading the guidelines and other administrative documents together, which is often difficult to interpret. In addition, many countries have limited information available in English.
- For countries with strict or unclear legal requirements, information must be, technically, aggregated per region and threat information is sent after removing personal information as appropriate, but this involves costs such as capital investment and personnel expenses to set up local facilities and personel.
- With respect to handling security-related information, companies are sometimes required to obtain not only global standards and certificates but also regional or country-specific certifications, and the costs involved in obtaining such certifications are significant.

2. The Data Life-cycle and Barriers to Cross-border Transfer Barriers (conclusion)

- Barriers that companies face in the situations involving cross border transfer of data include: **overlaping regulations within a country** that may be caused by digital silos among domestic regulators, **legal transparency issues** resulting from the multi-layered nature of regulatory requirements; **legal stability issues** due to frequent changes in these requirements and related **research costs on** the part of companies, **challenges resulting from regulators' lack of understanding of the business realities of data transfers to third countries; significant costs associated with obtaining certification for data handling**, and **lack of a clear definition of "cross-border transfers", "personal data" etc**.

Issues from the company's perspective (excerpts)

- The definition and provisions on the requirements for cross border transfer of "personal data" extend not only to the main body text of the regulations, but also to guidelines and adminsitrative agreements and are difficult to interpret. In addition, many countries have limited information available in English. (Type 1, Type 6)
- Not sure if data integration and cross-border data access between multiple/several regions across borders constitutes a "cross-border transfer". (Type 1, Type 2)
- New data categories including "non-personal data" such as "security information" and "critical information" are emerging, but the scope of regulatory coverage is extremely vague, and abrupt changes are increasing. (Type 4, Type 5)
- Regulations regarding "sensitive" "important" data continue to increase and in some cases the regulators prohibit taking out such data from the country. Including a process of individual scrutiny for each data set would undermine the characteristics of the IoT, such as the benefits of real-time monitoring. (Type 3)

→ **Ensuring Transparency**

- When data is transferred across borders to a third country, the business are asked to ensure that their counterparts provide the same protection level in their data management system and operation as the data-origin country while their counterparts are located in different reguatory jurisdiction. This puts a disproportionate amount of burden and responsibility to abide by on the side of the business (Type 1, Type 2).
- In the light of real-time monitoring that takes advantage of the characteristics of the IoT, can compliance to legal requirements for cross-border transfers be standardized? (Type 4)
- With respect to handling security-related information, companies are sometimes required to acquire not only international standards and certificates but also regional or country-specific certifications, and the costs involved in obtaining such certifications are significant. (Type 6)

→ **Technology and Standardization**

3. Current Status of Data-Related Regulations in Each Country (i)

- Regarding data-related regulations that have been introduced incrementally in various countries, the provisions related to cross-border transfer regulations and domestic preservation and requirements to have data reside on local territory have been organized. The **information subject to cross-border transfer regulations, the requirements for permissible cross-border transfers, and the existence and content of domestic preservation and storage obligations differ greatly from country to country, and** the **cost of complying with the legislations of each country for companies** doing business **globally** has become **increasingly significant in recent years**.
- On the other hand, the existence of "data" itself is multifaceted in nature, and while it can be classified in various ways depending on purpose and context, there are always problems of interpretation at its boundaries, making it difficult to generalize a taxonomy (definition and classification) in a simple and easily performable form.

	Cross-border transfer regulations							Requirements to have data reside on local territory			
	Name of the Law	information that is subject of regulation .	Regulation target	Requirements for permissible cross-border transfers				Name of the Law	Regulated data	Regulation target	Obligation Details
				Authorities Certification, etc.	Prescribed contract	Consent of the person in question	Other				
EU	GDPR	Personal data (information about an identified or identifiable natural person)	Controller or processor	Possible (adequacy decision)	Possible (SCC, ad hoc contracts)	Possible	Binding cooperate rules, certification by public authorities, ensuring the performance of contracts, inportant reasons of public interests, etc.	N/A under personal data protection legislation			
U.S.	N/A under personal data protection legislation							N/A under personal data protection legislation			
Canada	N/A under personal data protection legislation							N/A under personal data protection legislation			

3. Current Status of Data-Related Regulations in Each Country (ii)

	Cross-border transfer regulations							Requirements to have data reside on local territory			
	Name of the Law	Information subject to regulation	Regulation target	Requirements for permissible cross-border transfers				Name of the Law	Regulated data	Subject of regulation	Details of Obligations
				Authorities Certification, etc.	Prescribed contract	The person in question consent	Other				
China	Personal Information Protection Law	Personal information (non-anonymized information related to an identified or identifiable natural persons)	Personal information controller	Possible in combination with other procedures (Consent of the data subject) (*)	Possible in combination with other procedures (Consent of the data subject) (*)	Possible in combination with other procedures (e.g. security assessment)	Security assessment, other conditions as required by law (*)	Personal Information Protection Law	Personal information	(i) National agencies, (ii) Operators of critical information infrastructure, (iii) Controllers of personal information who reach a certain number	Duty to store data on local territory and security assessment
										Personal information controller	Approval of competent authorities for provision to foreign government agencies
	Cybersecurity law	(i) Personal information (information that can identify natural persons) and (ii) Important data (data closely related to national security, economic development, etc.)	Critical Information Infrastructure Operator	(Unregulated)	(Unregulated)	(Unregulated)	Security assessment	Cybersecurity law	Personal Information and Important Data	Critical Information Infrastructure Operator	Duty to store data on local territory and security assessment
	Data Security Law	Data related to the maintenance of national security and the international obligations, etc.	(Unregulated)	(Unregulated)	(Unregulated)	(Unregulated)	Export controls	Data Security Law	Important data	Critical Information Infrastructure Operator	Duty to store data on local territory and security assessment
										Other data processors	Separately prescribed by laws
		Important data	Critical Information Infrastructure Operator	(Unregulated)	(Unregulated)	(Unregulated)	Security assessment		(Unregulated)	Organizations or individuals within China	Approval of competent authorities for provision to foreign government agencies
			Other data processors	(Unregulated)	(Unregulated)	(Unregulated)	Separately prescribed by laws				

*Not applicable with the case of an operator of critical information infrastructure or a personal information controller who handles a certain number of personal information.

3. Current Status of Data-Related Regulations in Each Country (iii)

	Cross-border transfer regulations							Requirements to have data reside on local territory			
	Name of the Law	information that is subject of regulation	Regulation target	Requirements for permissible cross-border transfers				Name of the Law	Regulated data	Subject of regulation	Obligation Details
				Authorities Certification, etc.	Prescribed contract	The person in question consent	Other				
India	N/A under personal data protection legislation							Decree on the Storage of Payment System Data	Payment system data (end-to-end transaction details and information)	Payment system providers subject to authorization	Duty to store only in India
								Unified License Agreement	Accounting information and user information	Telecommunications service provider	Prohibition of transfers outside India
Vietnam	Draft Decree on Personal Data Protection	Personal information (information that can identify a specific individual)	Agencies, organizations and individuals concerned with personal information	Possible in combination with other procedures (consent, storage data on local territory, etc.)	(Unregulated)	Possible in combination with other procedures (storage data on local territory, approval by authorities, etc.)	(Unregulated)	Cybersecurity law	Data concerning personal information, or data created by service users,etc.	Network service providers	Duty to store data on local territory and to establish a domestic site
								Decree No. 72	(Unregulated)	Online service provider	Duty to install domestic servers
Indonesia	Regulation No.71 of 2019 and Regulation No.20 of 2016	Personal information (information that identifies an individual) and confidential personal data	Electronic System Providers	(Unregulated)	(Unregulated)	(Unregulated)	Collaboration with the Minister of Communication and Information Technology	Regulation No.71 of 2019	(Unregulated)	Electronic system providers appointed by public authorities	Duty to manage, process, and store data on local territory
	Personal Data Protection Bill	Confidential Personal Data	Controller	(Unregulated)	Possible	Possible	Regulatory equivalence or, international agreement	FSA regulations	(Unregulated)	Non-bank financial institutions, commercial banks, etc.	Duty to store data on local territory

Note: The light blue portion is about the bill legislations

4. Conclusion

- In the report, the following **five core areas have been identified for future policy development to achieve DFFT embodiment.**

Ensuring Transparency

With regard to regulations on cross-border transfers of data, identifying the options of international cooperation to improve transparency of regulations (e.g., information sharing, reporting systems, sharing guidelines and best practices, etc.).

Technology and Standardization

Stimulating international understanding and discussion on technologies that can serve as a guide for ensuring privacy and security when transferring data to third countries, as well as standards for the implementation of such technologies, and seek collaboration and involvement from industry and other stakeholders.

Interoperability

Research and study on policy options to ensure "interoperability", including existing certification systems based on the premise that national domestic systems relevant to cross-border transfer of data may differ considerably.

Complementarity with related systems

Development of policy initiatives on DFFT embodiment should be conducted in a complementary and harmonised manner with related tracks on international cooperation on privacy and security in addition to existing trade rules and principles related to cross-border data transfer.

Implementation of the DFFT embodiment

With countries that support the vision of DFFT, we will consider the modalities of a cooperative international framework/arrangement to promote DFFT-friendly policies, for example, a reporting system on legal reforms in each country to ensure transparency and a review on related efforts.