FEBRUARY 28, 2022

METI
Ministry of Economy, Trade and Industry

INTERIM REPORT OF THE EXPERT GROUP ON DATA FREE FLOW WITH TRUST

Table of Contents

Introduction

New forms of economy and society are developing based on the sharing of data generated by various actors such as individuals or companies. Data sharing produces new value and innovative solutions to both new and old challenges of our societies. Big data is an essential infrastructure in all sectors of the global economy as well as an essential resource that drives innovations including disruptive technologies such as artificial intelligence. In order to maximize the economic and social value that such data generates, it is vital to ensure the free flow of data across borders. As the use of data analytics is almost the conditions for the businesses to increase efficiency, streamline their business and participate international competition nowadays, data should be able to move freely while paying due attention to threats that use of data may generate. On the other hand, there is a growing practice to strengthen states' control over data generated in their territories, commonly referred to as data localization to impose the obligation to store and process data within the territory, , and other forms of restrictions on cross-border data transfers, government access. Some jurisdictions came to use the term ‘data sovereignty’ while leaving interpretative space for its precise scope and content.

Until now, the dominant perception around this situation has been that international competition for data as “merchant goods” was becoming fierce, much like the competition for "oil" in the 20th century due to the economic values that data produces. From this perspective, it was natural that the development of international mechanism on cross-border transfer of data first shaped as the rules for the “free trade” of data. On the other hand, there is a growing conception that emphasizes the public goods nature of data. And more fundamentally, data is different in nature from goods and services. Data can be classified into diverse and overlapping categories depending on the use and context in which it is handled, and can be structured, fragmented, or integrated over the life cycle of data - or, its value chain. Data are also non-rivalrous and easy to replicate while it is still possible to attach a certain degree of excludability by restricting access to data. In addition, even the concept of data "crossing borders" can assume various patterns, such as when data is replicated to a server in another region or when data is accessed across national borders. This pattern continues to increase with technological developments and new business models, and "cross-border transfer of data (international data flow)" is recognized as a concept that encompasses all of these.

With all these complexities surrounding the topic of data, we need to find the solution to remove the barriers to cross border free flow of data while paying appropriate attention to other interests such as privacy or security for which states regulate such flow of data.

Government of Japan, by returning to the origins of discussion – to seek what is needed to distribute the economic and social values internationally by sharing of data, and to promote healthy global economic and social development, proposed "Data Free Flow with Trust (DFFT)," a vision of international free flow of data based on "trust" as the foundation for establishing such flow. No matter how obvious the economic and social benefits of and efficacy of data sharing may be, data will not flow internationally without "trust", including the protection of personal data and security preservation. And to ensure this "trust," it is essential not only to share values and concepts, but also to create concrete mechanisms and systems to ensure the "trust" necessary for the cross-border transfer of data internationally.

So far, Government of Japan has worked to ensure "trust" in the cross-border transfer of data through the development of international trade rules and bilateral dialogue for personal data transfers. For example, bilateral agreements such as the Japan-U.S. Digital Trade Agreement and the Japan-UK Comprehensive Economic Partnership Agreement (EPA), and multilateral agreements such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership Agreement (RCEP) contain the rules relevant for the free cross-border transfer of data. It has also agreed on equivalence of standard of respective national regulations on personal data protection with the EU and the UK.

A trade agreement is an effective option to embody the DFFT by setting up the international rules for the free cross-border transfer of data while leaving a certain amount of policy space to each country. Mutual certification of regulation on personal data protections also enhances smooth personal data transfers.

Yet, in addition to trade agreements, we also shed the light to a variety of other initiatives to secure the trust that the DFFT aspires to. For example, the OECD has concluded the work towards trusted government access to personal data held by the private sector, and an inventory project[1]is underway to organize policy options such as national regulations and international frameworks for digital trade in each country. In addition, the G7 Digital and Technology Ministerial Meeting in 2021 has just formulated the DFFT Roadmap[2], which sets out action plans in four trans-disciplinary domains: (1) impact assessment of data localization, (2) comparative analysis of national policies on cross-border data transfer, (3) development of guidelines for reliable government access, and (4) promotion of mutual

[1] OECD Trade Policy Paper - Mapping commonalities in regulatory approaches to cross-border data transfers

[2] G7 Digital and Technology Ministerial Declaration, Annex2 - Roadmap for cooperation on data free flow with trust

data sharing.

Although various state, organizations and other international forums have been discussing the permissible scope of so-called data localization and government access, it will take a long time to reach a legitimate agreement on such scope, as each country has national circumstances to consider when taking measures for security, privacy and other justifiable interests. The report emphasizes, in addition to these regulatory restrictions on cross-border data flows , there are also many remaining challenges that hamper the cross-border transfer of data. The benefits of DFFT can be more strongly demonstrated if it is possible to establish an arrangement or a mechanism based first on a common understanding among countries that share the same basic values about the state of on each country's data-related regulations, and cross-cutting analysis on the lifecycle of data handled by companies.

Japan, as an advocate of DFFT, in a complementary manner with existing efforts on enhancing the cross-border free flow of data, and taking into account the unique circumstances of each country, will to promote the concrete measures to secure implementation of DFFT through proposals at international forums such as G7. To this end, the Ministry of Economy, Trade and Industry (METI) launched the Expert Group on Data Free Flow with Trust (hereinafter referred to as the "DFFT Expert Group") in November 2021, comprised both of experts and stakeholders. Through the three meetings held, the Expert Group studied the actual situations of international data flow, various actors in the data flow, the regulations which may set restrictive effect on the and recommendations on the data flow, as well as the various barriers that business and other data using entities face in their daily operations. The interim report provides the overview of outcomes of the three meetings and policy recommendations to set the direction for the embodiment of the DFFT towards Japan’s G7 presidency in 2023 and beyond.

The first challenge that the DFFT Expert Group tackled when working on the embodiment of DFFT was that, as a precondition for policy measures to promote the international flow of data , knowledge about the data “life-cycle,” i.e., "where" and "by whom" the data travels, was not well shared across industry sectors. Therefore, when discussing DFFT, there was little discussion that assumed a specific situation of "no data flow" in actual business settings.

Data goes through various processes (life-cycle) such as production, processing, replication, storage, aggregation, and analysis as it travels across physical devices and cyberspace. However, each of these processes involves various entities, and the management and decision-making of data in each process is defined by the conditions of the entities involved (management resources, knowledge, etc.)

and the conditions of the "place" where the entities are located (regulations, etc.). Cross-border transfer of data occurs as part of this life-cycle. From this vantage point, this report examines the life-cycles of data that companies want to disseminate, the various patterns of cross-border transfers that occur, and the impact of national regulations on data management and decision-making by the entities involved in data life-cycles. As a result, it became clear that there are many remaining challenges stemming out of differences in national legal systems, lack of clarity of provisions, and short of means to secure interoperability (e.g. granularity of 'adequacy'). Namely, there are still significant barriers that reduce the freedom of business in decision-making or have a considerable chilling effect on the cross-border transfer of data by companies. It also underscored the need to create a mechanism to ensure "trust" among different regulators, data users, and other stakeholders in order to ensure the free cross-border transfer of data among a multitude of countries.

- Companies are confronted with the problem of having to pay significant cost of coordination and compliance due to the lack of transparency of regulatory requirements regarding cross-border transfers of data, the lack of common standards regarding data governance and security regimes of third-country companies with whom they do business, in implementing the security standards required under national laws.
- Regulatory authority related to data is dispersed across multiple agencies within one country, and regulators in respective sectors do not necessarily have the holistic understanding of the regulations as well as the complex structure of the digital economy. There are scattered "siloing" issues where information is fragmented among authorities and industries. The result is regulatory duplication and extremely confusing requirements for data localization and statutory procedures across multiple laws.
- In terms of the relationship between individuals and companies, the idea that individuals should ensure "trust" in the collection and use of data pertaining to themselves is becoming more mainstream. The Japanese government is promoting a "human centric" approach to data in Society 5.0, which is consistent with the concept of securing "trust" in cross-border transfers.

In this report, Chapter 1 will first illustrate the patterns of cross-border transfers of data in the data life-cycle, and identify current or potential barriers that may arise. Chapter 2 outlines the laws and regulations that have restrictive effects on the cross-border transfer of data in each country. Chapter 3 discusses future directions and remaining challenges regarding mechanisms to ensure "trust" in order to embody the DFFT.

Chapter 1: The Data Life-cycle and Barriers to Cross-border Transfers

Chapter 1 summaries the outcome of the Expert Group on the DFFT to sketches out the representative types of data and of actions that constitute practices of "cross-border transfer of data," and also identify the barriers that companies and other entities that utilize data face in the dairy operations of data.

For this reason, in order to grasp the actual situation of cross-border transfers, this report is based on the concept of the "Data Management Framework (tentative)"[3] to understand i) the processes through which data is utilized by companies, etc., as a life-cycle starting from data production, ii) the entities involved in each process, iii) the location of data, and iv) transfers that could be considered to be cross-border transfers. In this report, interview surveys were conducted with companies whose business models are premised on the cross-border transfer of data, or which clearly will be so in the future. The collected cases are classified into six typologies. The companies interviewed were those involved in App services, those providing middleware such as Infrastructure as a Service (IaaS), those providing online platforms, those whose business models incorporate the use of IoT, and those handling information related to security and other network threats. These companies were selected because they cover the cross-border transfer of personal data, security-related data, and other non-personal data, and because they are representative models that the data analytics is a critical part of their business. In terms of typification, we have selected representative cases of business models that would involve different types of barriers and considerations in cross-border transfer of data (Types 1, 3, 4, and 5), cases that mainly handle security data not handled by representative business models (Type 6), and cases where cross-border transfers occur with a third party company (Type 2), which are discussed in this report. The "events" of the data life-cycle that are the focus of analysis in the survey can be broadly divided into generation, processing, use, storage, and disposal. Each of these may have overlapping characteristics, and the definition of an event may vary from case to case, as it is necessary to capture the "event" appropriately for each case and visualize the status of cross-border transfer of data. Depending on the existing regulations in each country, management choices regarding cross-border data transfers will change. However, this report collects cases that are difficult to deal with at the individual company level, especially with regard to the cost of compliance and the creation of business models that are adapted to the market situation.

This chapter is not intended to be a comprehensive guide to the barriers to cross-border transfer of

[3] A framework proposed by the Ministry of Economy, Trade and Industry for data management that takes data as its axis and considers the entire data life-cycle, from generation and acquisition to disposal.

data. It is only intended to clarify the snapshots of barriers with different natures through modeling data life-cycle in representative cases and to stimulate further discussion in the future.

1. Type 1: Utilization of data in product development for online App companies

(1) Summary

The customer's basic data and the use pattern of the Apps are analyzed, and sometimes combined with other externally obtained data in improving the Apps and develop new services. The data may be provided to third-party companies in third countries.

The data collected for product development can be broadly divided into i) the data provided at the time of registration for using the Apps (gender, age, region of residence, etc.), and ii) data generated from customer use of the apps (frequency of access, trends in information selected, etc.). With regard to the cross-border transfer of personal data, there were many respondent companies which answered that they would once store data in the commercial cloud in each market where the data was collected. After structuring and integrating the data to some extent within a “region” (a unit of area where a data center is located), they would transfer it to other clouds in the country where the R&D site is located. For the companies that are globally and internationally operating, the challenge is increasing diversity of regulations across the countries and conditions set by them. The ‘fragmentation’ makes the managing decisions more difficult in terms of handling of data. Many companies are also raising concerns about the cross-border “access" in terms of the laws of each country since they are hiring engineers and personnel of many different functions globally, and communicate one another online. In this setting, the access to the data which is stored in the server cloud of the headquarters or other function sites is a part of dairy operations for the people scattered around the world to fulfil their roles. Some companies raised concerns about uncertainty such as whether the internal meetings participated by the engineers located in the different regions constitute a cross-border transfer of data. On the other hand, there are cases where the companies would prefer to manage the data on a per-country basis where the data is used to improve the user experience locally.

With respect to data management, especially since many of the Apps providers are small businesses or start-ups, almost all of them indicated that it would be very difficult to set up servers/data centers in each country and process data locally while it is almost necessary due to the difference of regulatory conditions regarding the handling of data. Some also expressed concern that, although backups to mirror servers are essential from a security perspective, stricter regulatory conditions set on cross-border transfers of data will make routine backups more difficult. As regulations are being introduced

in various countries covering not only personal data but also various types of data from the perspective of security and others, the cost of legal compliance and of risk management for business, especially for those thinking to enter into new market is sharply increasing. Some companies responded that it is a critical barrier for building a new, innovative business model and even they had to completely block access from countries with extreme legal uncertainty.

(2) Status of cross-border transfers in the data life-cycle

i. Data production and acquisition

A) Data Status:

Data will be produced on customers' use of the App.

B) Company Request:

We would like to flexibly locate the data responding to the market environment, such as sending the data directly to the R&D site or headquarters from the users' Apps.'

- Each country has its own regulatory requirements for internationally transferring certain categories of data such as "personal data" and "critical information". Generally speaking, it is possible to incorporate the procedures such as prior individual consent or application of standard contractual clauses (hereafter referred to as "SCC") into the App itself. In reality, however, the requirements for consent differ in detail for each use case, and interpretative guidelines are established one after another, leaving a large room of development of the meaning of legal provisions. In addition, when third-party provision of data is involved, such as in the case of App integration, the partner company in a third country is often required to comply with the laws of the country from which the data is transferred (data origin).
- If laws start to differ greatly from country to country, the site to store and process data per country will be necessary, and the companies must process the data to make it non-personally identifiable before allowing it to cross the borders. This also creates the huge barriers for startups and SMEs with new ideas but limited resources to enter new markets.

ii. Data Processing[4]

A) Data Status:

[4]There are three main types of data processing

1) Structuring: While some data may be structured to some extent at the time of acquisition, information retrieval history, etc., should be structured according to parameters (e.g., gender, age, region of residence, occupation, etc.). Depending on the service, customer-related data may be combined with official data, but in Japan, since the format and assumptions vary from institution to institution, the data is treated as

- **Processing data.** Data is processed by engineers before the data is transferred beyond borders for checking regulatory compliance.

B) Challenges from the companies' perspectives:

We would like to flexibly locate the data responding to the market environment, such as sending the data directly to the R&D site or headquarters from the users' Apps.

- When processing data, the companies usually set the process to separate "personal data" from the collected set of data to ensure regulatory compliance. However, the definition and requirements under the regulations are often constructed in a way that cannot be understood without reading the laws together with other varied guidelines all together, making compliance more and more difficult.
- We are not sure how much abstraction is needed to make it no longer "personal data". As the amount of data collected and integrated increases, it becomes more unclear as to whether or not it constitutes "personal data", which critically changes the way companies set the operative resources about handling of the data.
- It is unclear whether the integration of data between multiple regions across borders or access to data across borders for product development or processing purposes could constitute a "cross-border transfer". Precautionary measures by taking safety precautions must be taken, but we are not sure how much precautions needed.
  - In relation to Japan's Personal Information Protection Act, some companies responded that they block access to data stored in Japan from Chinese subsidiaries as a precautionary measure while it is not explicitly required by law in both sides.

iii. Data Transfer

A) Data Status:

- **Consolidate data into R&D sites.** Move the data to the region where the development team is located (or, store the processed data in an environment available to the development team).

B) Challenges from the companies' perspectives:

- With respect to product and service improvement and development, it makes sense to

unstructured data at the time it is collected and then structured according to the parameters of each company (unless official data is standardized to some extent, which would be very costly to the user).

2) Integration: Structured data is combined and integrated depending on its use.

3) Separation: Depending on the laws of each country, the information will be separated and crossed over the border so that it does not become personal information (information with personal identifiability).

consolidate the data across borders. The forms of cross-border transfer of data (data movement) takes place depending on the location of R&D resources as well as the technologies that they choose to store and communicate the data Yet, this reality of the factors that determine the way that the data travel across the borders is not well considered by regulators. For example, accessing the data from a physically distant location is a cost of communication (speed of communication, security costs, etc.), thus we want to move the data flexibly according to the business needs.

- It is difficult to know what can be said to be free of "identifiability" in the personal data protection acts of each country. Even anonymized and integrated data may be subject to regulation. There are also other categories like “essential information” that are not allowed to be taken out of the border in some jurisdictions.
- When receiving data from third-country companies, various requirements for compliance with data origin laws may be contractually required. The responses to such requirement can be very complex. Furthermore, there are often limited texts and documents available in English to check local laws in these cases.
- Even if companies want to benefit from big data by integrating data across multiple regions, they currently do not have the resources to deal with the challenges due to differences in laws, uncertainty in interpretation of laws and regulations, and lack of information, and have not taken the plunge.
  - When the companies want to transfer data (e.g., information collected from Country A is to be further accessed by engineers in Country B or moved to the cloud in the Country C area), they need to understand the different conditions for cross-border transfer on all related countries – yet there are language barriers, lack of transparency in the articles, and other barriers such as contradictory conditions set by some regulations.

2. Type 2: Transfer of collected data to a company in third-party country for outsourcing of operations

(1) Summary

An example of companies in this category provides mobile payment services and online booking platform services. The company provides services using overseas cloud computing, but some operations are outsourced (including joint use) to other companies in a third-party country.

Among the data handled in this category, involvement of personal data requires particular attention in

relation to laws and regulations, including data provided at the time of registration for use (customer attributes, i.e., gender, age, residential area, etc.) and data generated from customer use of services. The main uses of the data are to improve the user experience, develop new services, and link with other companies' Apps and services such as linking the payment apps with other companies' services. The data cross the borders when their applications are linked to other applications or outsourcing, as both cases require handing collected data to overseas service providers in outsourced operations a cloud in another region.

(2) Status of cross-border transfers in the data life-cycle

i. Data production and acquisition

A) Data Status:

- **Data is produced on customer use of the App.**

B) Challenges from the companies' perspectives:

- Data related to user experience improvement will basically be stored in the region where the customers are and processed and analyzed in the same region. However, since the companies outsource many of their operations to overseas operators, they face the uncertainty regarding cross-border transfers (see below).

ii. Data Processing

A) Data Status:

- **Processing data.** The data will be processed by engineers within the region, but the team of engineers can consist of engineers sourced from other countries.

B) Challenges from the companies' perspectives:

- It is common to have a division of labor along the lines of specialization, and tasks, including analysis are increasingly outsourced internationally. In addition, the need for cross-border access to data is to perform the necessary operations is increasing as it becomes more and more difficult to find talented engineers. (Global competition of acquiring human resources)

iii. Data Transfer

A) Data Status:

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

B) Challenges from the companies' perspectives:

- The conditions for "cross-border transfers" are difficult to understand. There are many laws that do not tell us whether accessing data from outside the region is a "cross-border transfer. (For example, even if the personnel on a business trip from the company access the server of the company from the different region, is it a "cross-border transfer"? If so, this does not make much sense.) In addition, when a cloud exists across multiple countries, there is a possibility of "cross-border transfer" the moment data enters the cloud, so at least a prior consent must be obtained by the customer.

Even in cases where it is certain that the transfer is a "cross-border transfer to a third country" in light of the laws of each country, the following problems may exist:

- For transfers to third countries, the regulations on personal data protection from major countries require that the companies must make sure there is adequate level of data protection in the destination country, and also the companies that receive the data should also have the standard of data governance that is required at the data origin. This responsibility is placed on the company to investigate and confirm the adequacy, as well as the management standard of the counterparty company.
  - At present, there is no standard or even guidance for what one company should "base" and "how to confirm" that the level of protection that is adequate or equivalent between countries in a very concrete sense.
  - In fact, here is rarely room for individual contractual negotiations between one company and the cloud and other SaaS vendors used by its business partners while safety or protection standard of a company's data governance vastly defined by the services provided by the vendors.
- The definition of "contractor" that affects the scope of regulations is ambiguous under the laws of each country. An organization that is subjectively a "subsidiary" may become a "contractor" under the laws of the country in question. It is often as a matter of interpretation.

3. Type 3: Real-time data collection and analysis from the other countries via IoT (when personal data is clearly not included)

(1) Summary

For devices and other equipment sold globally, the IoT platform is used to collect and analyze data globally in real-time on operating conditions, associated operating environments, needs of repairs, etc., in order to predict the occurrence of failures and optimize maintenance plans etc based on such data.

This category of companies responded that the IoT devises they use do not contain personal devices, which collect the personal data. On the other hand, depending on the legal system, even information that does not contain personal data may be restricted from cross-border transfer such as security-related information.

Most companies in the interview still store data collected from equipments' sensors on the local operator's or distributor's servers (acquired and stored in the local region cloud or on-premise). In many cases, the local agencies manage the data, including customer data, and the data is not yet to be utilised in a way to benefit from the real-time monitoring. Yet, the potential of IoTs is considered to be fully unlocked when the analysis of data collected via IoT will be performed at the head office/R&D sites in real-time. The companies are reviewing the contractual relationship with the distributors and other details to optimise the data governance globally.

The raw data collected by IoT sensors can range from visuals, sounds to data related to failures of functions. Some data are needed to be processed to quantitative information such as weight, speed, and temperature.

(2) Status of cross-border transfers in the data life-cycle

i. Data production and transfer

A) Data status:

- **Data is obtained from sensors** installed in the equipment sold.
- **The data is aggregated and consolidated (desirably at the any places that the companies need to place it, but increasingly the companies feel pressure to do so locally)**

B) Challenges from the companies' perspectives:

- Since we are considering locating our analysis and other major operations to our headquarters, we would like to transfer the data (which are basically non-personal) obtained from the sensors directly to a server located at the headquarters location.
- Regulations concerning data other than "personal data" continue to increase, and some countries prohibit data from being taken out of the country even if it has absolutely no link to personal data (e.g., information on the flow of people at a particular station). However, if a process is included to separately scrutinize information that can cross borders and that cannot, the advantages of real-time monitoring, which is a characteristic of IoT, will be compromised.

- It is not yet common to analyze regional differences of data obtained from IoT devices for purposes other than marketing. Yet we would like to pursue this possibility, which require aggregation/consolidation of data in one place for analysis, product development, and prediction of the occurrence of failures and system construction.

4. Type 4: Real-time data collection and analysis from overseas via IoT (if personal data can be included)

(1) Summary

The cases of this category include IoT data acquired from personally owned devices, which means it may include data that leads to the identity of customers. The wide variety of data that can be collected (e.g., photos and videos of signs and infrastructure, location information, accident and near-miss information, road information, traffic congestion information, energy consumption, temperature, human flow, payment information) depending on the type of devices.

Increasingly, collection and cross-border transfer of data on the operating environments of devices are subject to the restriction in various jurisdictions. Since these sorts of data are necessary for product development and adoption to local environment, there is a risk that some services may have to be suspended if the regulations continue to grow rigid, change or are reinterpreted in an unpredictable way. If regulations continue to change in a short period of time and in an unpredictable manner, there will be pressure to place all the steps of data processing - gathering, analysis, and product development within a single country. However, as long as services are being developed globally, it is desirable, or even necessary that data be placed in multiple locations and always synchronized worldwide, so that analysis and development work and troubleshooting can be conducted 24 hours a day, 365 days a year.

(2) Status of cross-border transfers in the data life-cycle

i. Data transfer

A) Life-cycle status:

- **Data is obtained from sensors** installed in the equipment sold.
- **The data is aggregated and consolidated (desirably at the any places that the companies need to place it, but increasingly the companies feel pressure to do so locally)**

B) Challenges from the companies' perspectives:

- It is preferable that it be possible to send the collected data directly and automatically from the

customer's system to the any servers that companies have the need to send it.

- While some data is collected to adapt the product and service to the local environment, particularly, data concerning equipment and device operation in general (hardware and software errors, accidents and near-misses, payment information, energy consumption, etc.) is preferable to be placed in multiple sites and constantly synchronized worldwide. This way, analysis and development as well as trouble shooting can be conducted 24 hours a day, 365 days a year.
- New data categories under relevant regulations have emerged that include not only personal data but also non-personal data, such as "security data" and "essential data." However, the scope of the categories is extremely vague, and data types subject to the regulations are added increasingly through related documents such as interpretative guidelines and administrative agreements.
- In conducting real-time monitoring that takes advantage of the characteristics of the IoT, it is preferable that procedures for compliance with legal requirements for cross-border transfers can be standardized and formalized to some extent across countries.

5. Type 5: Provision of platform services and IaaS

(1) Summary

Various services and network resources are provided to customers who have created individual accounts on the platforms provided by the companies. In the provision of services, the process includes collecting and storing the data from customers and the Internet on the platform and analyzing and managing the data. The data analyzed here may also be used for advertising systems (e.g., targeted advertising).

In this business model, almost 100% of the companies responded that, in principle, customers themselves manage their own personal data and data held on the networks are provided by their customers in a manner that is compliant with the existing regulations including the perspective of ensuring data portability, etc., in light of the provisions of the GDPR, the regulation with most stringent personal data protection. These types of companies organize that the primary confirmation of legal compliance and sufficiency should be investigated and reviewed by the customers themselves. For each business purpose defined under the regulation, prior consent by individual customers is required, but the requirements, such as the authenticity of consent, have become stricter over the years. On the other hand, other data related to the provision of services include information on "service-related data (e.g., how often and at what time the provided services are used)," "security-related data (e.g.,

cybersecurity)," and "support service data (e.g., defect reports)," which are treated as "non-personal data" according to internal company policies. These non-personal data will be consolidated and analyzed either at the headquarters or in the region where the development sites are located and used to improve services. However, an increasing number of countries are tightening their control over non-personal data through new regulations other than privacy protection. Building business strategies involving determining service deployment policies and allocating resources, such as data centers, are becoming increasingly complex.

Regarding data management methods, many companies responded that distributed management (including mirroring) is used or is desirable from a security perspective. However, due to the high cost of legal compliance, some companies responded that they do not decentralize the data associated with customer accounts, nor do they convert it into big data.

(2) Status of cross-border transfers in the data life-cycle

i. Data generation and acquisition (customer data)

A) Data status:

- The customer creates an account. **Customer data is produced.**
- The varied types of data (e.g., customer information - past cookie information, past activity and browsing records, etc.) are collected on daily basis for analysis related to the provision of services.

B) Challenges from the companies' perspectives:

- From the standpoint of security and continuous service provision, it is best to have decentralized management (copying data for several locations synchronizing them).
- Simplicity of requirements is desirable for companies operating in multiple jurisdictions, and clear definitions and classifications (taxonomy) are also needed.
- Although there is a wide range of data for which cross-border transfer is restricted (e.g., "personal data," "critical data," "security data," etc.), general definitional or interpretative guidelines are vastly missing. The disadvantages resulting from the uncertainty are passed on to companies.
- Since the conditions for the transfer of personal and non-personal data as well as the definitions of the categories of data vary by laws and jurisdictions, the companies must also design the systems embedded to their services and other governance according to significantly detailed and varied purpose of use, conditions of use and other requirements for each territorial

jurisdiction.

- Various regulations are being introduced in each country and region every year, and it takes a considerable amount of time for a business to be able to respond to each of them, for not only by analyzing the laws of each country, but also by engineering the technology to reflect such laws and regulations into the systems and the interfaces.
- Some companies may have a policy of responding with a global risk-based approach based on the most stringent laws (GDPR or the California Consumer Privacy Act in the U.S.) rather than individual responses. While close cooperation between the local legal team and the headquarters is essential, the companies cannot afford to have the legal teams in all countries and regions.

- As the conditions for cross-border transfers are increasingly becoming complex, engineering costs of ensuring the customers' consent and other requirements is rising as the regulations get more complicated. This would also affect the customers of the platform. From the customer's point of view, they are constantly bothered by the large number of pop-ups that ask for permission to use the service for almost every time that they move the sites within the platform.
- Some new interpretations introduced by the courts could prohibit the companies to make the transfer of personal data a condition for the use of services for free – that the space of interpretation critically hit the companies' assumption on their business model.
- Laws in major countries impose on companies the obligation to confirm "safety" as well as " adequacy" in case of transferring the data to third country (and entity in the third country).
  - There are no concrete guidelines or definitions as to what conditions are "safe" or "sufficient". 'The vague concepts' do not help in the day-to-day business realities of companies.
  - If a global risk-based approach is taken, one option is to obtain U.S. government standards such as NIST 800-171 and NIST CSF, which are broadly related to security, global standards such as ISO, or regional or country-specific standards such as CS Mark or ISMAP, but obtaining such standards can be very expensive to obtain approval from an auditing firm, in addition to preparing in-house technical support for an audit. Furthermore, even for the expense, there is no guarantee that it is legal compliant to the specific jurisdiction of the regulation.

ii. **Data production and transfer (non-personal data))**

A) Data status:

- **Service-related data and support-related data are produced as customers access and use the service.** This data is considered as "non-personal data" under the internal standard of

the companies and is transferred across borders and consolidated at the headquarters or R&D sites.

B) Challenges from the companies' perspectives:

- From the standpoint of security and continuous service provision, it is best to have decentralized management (copying data for several locations synchronizing them).
- Simplicity of requirements is desirable for companies operating in multiple jurisdictions, and clear definitions and classifications (taxonomy) are also needed.
- Although there is a wide range of data for which cross-border transfer is restricted (e.g., "personal data," "critical data," "security data," etc.), general definitional or interpretative guidelines are vastly missing. The disadvantages resulting from the uncertainty are passed on to companies.
  - There are a wide range of cases where the boundary between "personal data" and "non-personal data" is ambiguous (especially when IDs are linked to support-related information, etc.). The scope of 'non-personal' data for which cross-border transfer is restricted from security and other perspectives can also be wide-ranging. When definitions are unclear, companies are forced to calculate the risk regarding the decisions on resource allocation (e.g. data centers and other facilities) and other decisions based on the strictest possible interpretation as a safety measure.

6. Category 6: Provision of cyber security services

(1) Summary

Services are provided to detect, respond to, and take preventive measures against cyberattacks by providing security software for hardware, smartphones, and other devices, as well as security maintenance for cloud environments. Since the same system is used to respond to cyberattacks for all customers using similar software around the world, the information necessary for threat analysis and updating software must be centrally collected and managed. Information determined to be a threat is stored in a database and analyzed. The outcome of analysis is eventually reflected to the software provided.

The information and data handled by the companies include information provided by both customers and external organizations as well as security-related information that the companies collect on its own. Information and data provided by customers can include personal data. In some cases, the data sent to the R&D sites sent directly from the software at customers' while in other cases, the data is first

analyzed in each region, then sent beyond borders when they determine a threat in the collected information. With respect to personal data, the respondents answered that to some extent there is a fixed operation within the companies, and for example, for e-mail, only engineers from the country where the region is located have access to the e-mail and analyze it locally (there is no cross-border access). Threat information sent after analysis is stripped of personal information. While there are countries (e.g., Japan, EU member countries, India, and Canada) where local regulations impose particularly strict or complex requirements for the handling of personal information, especially for third-country transfers, many respondents stated that for such countries, it is necessary to consolidate information on a server located in the region, process it so that it does not contain personal information, and then send threat information to a server in the country where the development site is based. In countries where regulations are less stringent, these companies transmit directly from the customer's system to the server in the country where the development site is located, generally with the customer's consent (checked in the system), regardless of national or regional laws.

When considering efficiency, it is always preferable to consolidate information in a single site. However, in case of a cyberattack or accident, it is also necessary to decentralize management to at least two sites and synchronize information at all times from the perspective of business continuity. On the other hand, it would be costly to invest in equipment and other resources to scrutinize and analyze the information for every region. At this time, we are holding reporting and update meetings on the status of each region and organizing the differences between the national systems into a matrix, which is updated each time. Server locations are also being constantly reviewed.

(2) Status of cross-border transfers in the data life-cycle

i. Data Transfer

A) Data status:

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

B) Challenges from the companies' perspectives:

- It would be preferable to be able to send threat-related information directly and automatically from the customer's system to the server at the R&D sites.
- Regulations regarding personal data vary widely from country to country, and the requirements

for transfer may be divided into detailed requirements for each purpose of use. To start with, the requirements are often difficult to interpret because they are structured in such a way that they cannot be understood without reading not only the regulations themselves, but also the guidelines and other administrative agreements together.

- Regarding the definition of "third party" in the transfer to a third party in a foreign country, even a subsidiary can be treated as an outsourcing entity and be subject to "safety management obligations."
- The standard of safety to be guaranteed in the "safety management obligations" is unclear, and this is to be interpreted at the risk of individual companies.
- The conditions for "easily verifiable" and "personal identifiability" in the definition of personal data are unclear, and ultimately it is difficult to know to what extent information is treated as easily verifiable or personally identifiable.

- For countries with strict or unclear legal requirements, we are consolidating information and data by each jurisdiction and sending threat- related data after removing personal data, but this adds costs such as investment on infrastructure and personnel expenses.
- After collecting and analyzing information and data on regulations concerning the handling of data globally, we have organized the differences between the system of each country, but there are many countries where the information on regulations is not available or fairly limited in English.
- Difference in governance that reflects the local legal culture, such as the custom that substantial content of obligation is actually falling under guidelines, or the requirement to obtain specific certifications issued by the country for the handling of security-related information. There is considerable overlap between certification standards and we wonder if it is possible to standardize internationally the common features of the local certificates.

Chapter 2: Current Status of Data-Related Regulations in Each Country

Chapter 2 outlines the current status of laws that have restrictive effects on cross-border transfers, which Japanese companies are relatively likely to need to deal with, while taking into account the background situation in each country as much as possible. Specifically, among the major laws, mainly data-related regulations, of each country, in addition to those that impose restrictions on cross-border transfers themselves, we will also introduce those that establish requirements to have data reside on local territory that affect the free cross-border transfer of data. The countries and regions introduced in this report were selected from those that had strong needs as "countries and regions that should be emphasized in responding to the system" in the corporate survey[5] conducted by the Ministry of Economy, Trade and Industry in 2021. In this chapter, overall, the information is organized as of the end of 2021.

1. EU

(1) Applicable Laws

For the EU as a whole, the General Data Protection Regulation (GDPR)[6], which entered into force on May 25, 2018, Articles 44-50 set forth regulations for cross-border transfers.

This discipline has been inherited from the EU Data Protection Directive 95[7], the predecessor of the GDPR, which states that while the flow of personal data within and outside the EU is necessary for the expansion of international trade and cooperation, it should not threaten the level of protection of natural persons ensured by the GDPR and that data transfer may be carried out in full compliance with the GDPR (GDPR Preamble, paragraph (101)).

(2) Cross-border transfer regulations

i. **Regulated conduct**

Article 44 of the GDPR provides that (i) transfers of personal data to third countries or international organizations outside the EEA and (ii) transfers of personal data from such third countries or international organizations to another third countries or international organizations (Onward Transfer) are subject to the regulations under Article 44.

[5] Ministry of Economy, Trade and Industry "Survey on the Current State of Companies' Data-related Management and Contracts for the Promotion of Data Utilization"

[6] https://eur-lex.europa.eu/eli/reg/2016/679/oj

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

With respect to (i), even if the transfer of personal data occurs within the same country, while the country locates outside the EEA (e.g., from US entity A to US entity B to which the GDPR applies), the transfer is subject to the cross-border transfer regulation. With respect to (ii), this includes, for example, the case where a company in the EEA transfers personal data to a vendor in the U.S., who in turn transfers the personal data to a subcontractor located outside the EEA.

ii. **Types of data subject to regulations**

Personal data subject to the cross-border transfer regulation in the relevant provisions of the GDPR means information about an identified or identifiable natural person (data subject), and an identifiable natural person is defined as one who can be identified directly or indirectly in particular by reference to an identifier, such as a name, identification number, location data or online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, (Article 4(1) of the Law).

iii. **Definition and scope of persons subject to regulations**

Under the GDPR, controller (a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, Article 4(7) of the Law) and processors (a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, Article 4(8) of the Law) are subject to cross-border transfer regulations (Article 44 of the Law). Persons who process personal data on behalf of the controller are processors, which may include, for example, cloud service providers or payroll processing companies used by the controller.

iv. **Content of regulations**

Under the GDPR, the transfer of personal data outside the EEA is prohibited in principle (Article 44 of the Law), but it is possible to transfer personal data outside the EEA on an exceptional basis if one of the following conditions is met

A) First, it is permissible to transfer personal data outside the EEA without additional special measures for data transfers to countries, regions or international organizations[8] that have been certified by the European Commission as ensuring an adequate level of data protection (adequacy decision) (Article 45(1) of the GDPR).

B) If the destination country has not obtained a adequacy decision, personal data can be

[8] In addition to Japan, other countries that have received adequacy decision are Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, United Kingdom and South Korea.

transferred outside the EEA in compliance with the following safeguards as specified in Article 46 of the GDPR

1) Legally binding and enforceable instruments between public authorities or bodies
2) Binding Corporate Rules (BCR)[9]
3) SCC adopted by the European Commission[10]
4) SCC adopted by supervisory authority and approved by the Commission
5) GDPR Article 40 prescribed code of conduct (voluntary rules established by industry associations of controllers and processors)
6) Approved certification that the data protection measures of the controller or processor comply with the GDPR[11]
7) Contract clauses or arrangements are authorized on an specified basis by a supervisory authority

C) If an adequacy decision under (a) above has not been obtained and the appropriate safeguards under (b) above cannot be put in place, personal data may be transferred outside the EEA only if the Derogations[12] specified in Article 49 of the GDPR are met.

[9] THIS REFERS TO PERSONAL DATA PROTECTION POLICIES WHICH ARE ADHERED TO BY A CONTROLLER OR PROCESSOR ESTABLISHED ON THE TERRITORY OF A MEMBER STATE FOR TRANSFERS OR A SET OF TRANSFERS OF PERSONAL DATA TO A CONTROLLER OR PROCESSOR IN ONE OR MORE THIRD COUNTRIES WITHIN A GROUP OF UNDERTAKINGS, OR GROUP OF ENTERPRISES ENGAGED IN A JOINT ECONOMIC ACTIVITY (ARTICLE 4(20) OF THE GDPR). THE MATTERS PRESCRIBED IN ARTICLE 47(2) OF THE LAW ARE REQUIRED TO BE SET FORTH IN THE RELEVANT BYLAWS.

[10] IT IS A TEMPLATE FOR A CONTRACT FOR THE TRANSFER OF PERSONAL DATA OUTSIDE THE EEA AND IS LISTED AS AN ANNEX TO https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN THE SCC IS UNABLE TO MAKE CHANGES TO THE CONTENT OF THE CLAUSES AND WILL SELECT A VARIATION BASED ON THE TYPE OF DATA TRANSFER AND FILL OUT THE REQUIRED INFORMATION TO BE USED.

[11] IT IS A CERTIFICATION AS DEFINED IN ARTICLE 42 OF THE GDPR AND GRANTED BY A COMPETENT SUPERVISORY AUTHORITY OR A BODY DULY AUTHORIZED TO PERFORM THE CERTIFICATION.

[12] THE FOLLOWING EXCEPTIONS ARE SPECIFIED.

1) WHERE THE DATA SUBJECT HAS EXPLICITLY CONSENTED TO THE PROPOSED TRANSFER, AFTER HAVING BEEN INFORMED OF THE POSSIBLE RISKS OF SUCH TRANSFERS FOR THE DATA SUBJECT DUE TO THE ABSENCE OF AN ADEQUACY DECISION AND APPROPRIATE SAFEGUARDS
2) WHEN THE TRANSFER IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT BETWEEN THE DATA SUBJECT AND THE CONTROLLER OR THE IMPLEMENTATION OF PRE-CONTRACTUAL MEASURES TAKEN AT THE DATA SUBJECT'S REQUEST
3) WHEN THE TRANSFER IS NECESSARY FOR THE CONCLUSION OR PERFORMANCE OF A CONTRACT CONCLUDED IN THE INTEREST OF THE DATA SUBJECT BETWEEN THE CONTROLLER AND ANOTHER NATURAL OR LEGAL PERSON
4) WHEN THE TRANSFER IS NECESSARY FOR IMPORTANT REASONS OF PUBLIC INTEREST
5) WHEN THE TRANSFER IS NECESSARY FOR THE ESTABLISHMENT, EXERCISE OR DEFENSE OF LEGAL CLAIMS
6) WHEN THE TRANSFER IS NECESSARY IN ORDER TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR OF OTHER PERSONS, WHERE THE DATA SUBJECT IS PHYSICALLY OR LEGALLY INCAPABLE OF GIVING CONSENT
7) WHEN THE TRANSFER IS MADE FROM A REGISTER WHICH ACCORDING TO UNION OR MEMBER STATE LAW IS INTENDED TO PROVIDE INFORMATION TO THE PUBLIC AND WHICH IS OPEN TO CONSULTATION EITHER BY THE PUBLIC IN GENERAL OR BY ANY PERSON WHO CAN DEMONSTRATE A LEGITIMATE INTEREST, BUT ONLY TO THE EXTENT THAT THE CONDITIONS LAID DOWN BY UNION OR MEMBER STATE LAW FOR CONSULTATION ARE FULFILLED IN THE PARTICULAR CASE

2. United States of America

(1) Applicable Laws

In the U.S., there is no comprehensive federal law on the protection of personal information.

1) Electronic Communications Privacy Act of 1986 (ECPA) [13,14]
2) Gramm Leach Bliley Act (GLBA) [15,16]
3) Health Insurance Portability and Accounting Act (HIPAA) [17,18]

As for state laws, California (California Consumer Privacy Act of 2018 (CCPA)[19])[20], Virginia (Consumer Data Protection Act[21]) and Colorado (Colorado Privacy Act[22]) have comprehensive laws regarding the protection of personal information. In addition, there are individual laws and regulations that establish rules related to personal information protection, such as the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act[23] and the New York Department of Financial Services Cybersecurity Regulation[24] in New York State, and the Illinois Biometric Information Privacy Act[25] and Personal Information Privacy Act[26] in Illinois.

However, for these federal and state laws, there exist no provisions that establish regulations specific to cross-border transfers or mandate intra-regional or intra-regional storage of data.

3. Canada

(1) Applicable Laws

In Canada, there are two comprehensive federal laws regarding the protection of personal information: (i) the Personal Information Protection and Electronic Documents Act (PIPEDA)[27], a federal law

---

[13] https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

[14] OF THESE, Title II, the Stored Communications ACT (SCA) and its amendment, the Clarifying Lawful Overseas Use of Data Act. 18 U.S.C. §§ 2510, 2701-2713. (CLOUD Act) are privacy-related regulations.

[15] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

[16] OF THESE, the Privacy Rule and the Safeguards Rule. 15 U.S.C. §§ 6801-6809, 6821-6827 are privacy-related regulations.

[17] https://www.cdc.gov/phlp/publications/topic/hipaa.html

[18] OF THESE, the Privacy Rule and the Safeguards Rule. 41 U.S.C. §§ 1320D is a privacy-related regulation.

[19] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[20] IN CALIFORNIA, THE California Privacy Rights Act, which is more restrictive than the Californian Consumer Privacy Act Of 2018, IS SCHEDULED TO TAKE EFFECT ON JANUARY 1, 2023.

[21] https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392

[22] https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf

[23] https://www.nysenate.gov/legislation/bills/2019/s5575

[24] https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)&bhcp=1

[25] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

[26] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67

[27] https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

applicable to the private sector that was enacted in stages from 2001 to 2004, and (ii) the Privacy Act[28], a federal law applicable to the public sector that came into force on July 1, 1983.

However, there are no provisions in any of these laws that establish regulations specific to cross-border transfers or mandate domestic preservation or domestic storage of data.

However, the Office of the Privacy Commissioner of Canada has published Processing Personal Data Across Borders Guidelines[29], which require the same level of protection at the destination as at the source, as is required for data transfers within Canada.

In addition, some individual state laws provide for regulation of cross-border transfers, including examples requiring a privacy notice (Alberta[30]) and reasonable measures (Quebec[31]).

4. China

(1) Applicable Laws

In China, there is a comprehensive law on the protection of personal data, the Personal Information Protection Law (PIPL) [32], which came into effect on November 1, 2021, with provisions that establish regulations specific to cross-border transfers and mandate domestic preservation and domestic storage of data.

Other laws with relevant provisions are the Cybersecurity Law (also known as the Network Security Law)[33], a basic law on security in the Internet domain that came into force on June 1, 2017 and the Data Security Law[34] that came into force on September 1, 2021 that establishes measures for the supervision and management of data and its security and utilization[35].

However, since the interpretation of each requirement subject to regulations under these laws is not always clear, there are reports that some companies are moving to avoid cross-border transfers of data from China.

The purpose of the provisions establishing regulations specific to cross-border transfers and requiring domestic preservation and domestic storage of data is considered to be national security.

---

[28] https://laws-lois.justice.gc.ca/eng/acts/P-21/

[29] https://www.priv.gc.ca/media/1992/gl_dab_090127_e.pdf

[30] Personal Information Protection Act (SA 2003 C P-6.5) section 6(2))

[31] Act Respecting the Protection of Personal Information in the Private Sector (CQLR c P-39.1) section 17

[32] http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[33] https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf

[34] http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml

[35] In addition, there are some automotive industry-specific cross-border transfer regulations and domestic storage obligations in some provisions of the Automobile Data Security Management, which have been in effect on a pilot basis since October 1, 2021.

(2) Cross-border transfer regulations

i. Regulated conduct

A) Although the content has not been finalized[36], Article 17 of the Draft Measures for Security Assessment of Personal Information and Important Data to be Transmitted Abroad (hereinafter referred to as "2017 Bill"), promulgated on April 11, 2017, which is positioned as a subordinate law of the Cybersecurity Law, provides that network operators shall be regulated in providing personal information and important data [37] collected and generated in their domestic operations[38] to organizations, organizations or individuals located outside China.

B) In addition, although the content has not also yet been finalized, Article3.7 of the Draft Measures on Security Assessment of Cross-Border Data Transfer[39] regulates one-time or continuous activities in which network operators provide personal information and important data collected and generated in their domestic operations to organizations, organizations or individuals located

[36] In China, even laws whose contents have not yet been finalized may serve as a reference for interpretation, and are therefore presented in this report as reference information.

[37] Under the Draft Measures on Security Assessment of Cross-Border Data Transfer, a foreign company is considered to be "operating" in China if it conducts any management activities or provides products or services in China, regardless of whether or not it is registered in China (Article 3(2) of the Draft Guidelines). Determining factors for the applicability of this operation in China include (i) whether or not the Chinese language is used in the transaction, (ii) whether or not the renminbi is used as the settlement currency, and (iii) whether or not the delivery and distribution of goods to or within China are involved.

[38] According to Article 17 of the 2017 Bill, important data is data closely related to national security, economic development, and social and public interests, the specific scope of which refers to relevant national standards and important data identification guidelines. In addition, according to Appendix A of the Draft Measures on Security Assessment of Cross-Border Data Transfer, important data is data (including original and derived data) collected or generated in China by governments, organizations, or individuals that is closely related to national security, economic development, or public interest and does not constitute state secrets, and that is disclosed, lost, abused, altered, or destroyed without consent, or analyzed, etc., if such data: (i) harms national security or defense interests or destroys international relations; (ii) harms state property, public interests, or legitimate personal interests; (iii) affects state prevention or control of industrial espionage, military espionage, or organized crime; (iv) affects investigations by administrative agencies into illegal or corrupt activities; (v) obstructs government administrative activities; (vi) causes damage to national critical infrastructure, critical information infrastructure, or government system information systems; (vii) causes damage to the economic and financial order; (viii) allows access to national secrets or sensitive data; (ix) other matters that may cause damage to national security matters. The guidelines specify the scope of important data in 27 categories, including telecommunications, steel, finance, e-commerce, and food and drug products, for each industry sector.
In addition, Article 38 of the Measures on Data Security Management (draft for soliciting opinions) published on May 28, 2019, which is also premised on the Cybersecurity Law, states that important data is data that could directly affect national security, economic security, social stability, public health and safety if leaked, specifically including non-public government information, broad population, genetic health, geography, and mineral resources.
It has not yet been determined whether the content of any of these valve in 2017 bill and 2019 bill will be finalized.
Furthermore, the Data Security Law establishes a data classification system for important data and specifies that the national government shall establish a important data inventory based on the importance of data in economic and social development and the level of harm to national security, public interest, or the legitimate rights and interests of individuals or organizations once they are altered, destroyed, leaked, or illegally acquired and used (Article 21 of the Law).

[39] https://www.tc260.org.cn/file/20170830203000000004.docx

outside China directly or through business development, provision of services or products, etc., through network or other means, and the following situations are also considered to be subject to cross-border transfer regulations.

1) Providing personal information and important data to institutions, organizations or individuals (i.e., foreign companies or foreigners from the perspective of China) that are not subject to Chinese jurisdiction or registered in China[40], but that are located in China
2) Where data is not transferred or stored in areas outside of China but can be accessed and viewed by mechanisms, organizations, or individuals outside of China (excluding public information and website access)
3) Data transfers within the corporate group, even if they involve personal information and important data collected and generated in operations in China

On the other hand, the regulations of the Article do not extend to the following situations

1) Personal information and important data that has not been collected or originated in our domestic operations in China and is transferred outside of China through China without being changed or processed
2) Personal information and important data that were not collected and generated in our domestic operations in China are stored and processed in China before being transferred outside China, but are not related to personal information and important data collected and generated in our domestic operations in China.

ii. **Types of data subject to regulations**

A) Personal information subject to the cross-border transfer restrictions of the Personal Information Protection Law is defined as all kinds of information recorded by electronical or other means related to identified or identifiable natural persons, not including information after anonymization (Article 4 of the PIPL).

B) Personal information and important data are subject to regulation with respect to the cross-border transfer regulations of the Cybersecurity Law. Among these, personal information refers to various types of information, including but not limited to a natural person's name, date of birth, identification number, personal biometric information, address, telephone number, etc., that can identify the identity of a natural person (individual) alone or in combination with other information recorded in electronic or other formats (Article 76(5) of the Cybersecurity Law).

C) Under the Data Security Law, data falling under controlled items[41] related to the maintenance

[40] REFERS TO MAINLAND CHINA, NOT INCLUDING HONG KONG, MACAU, AND TAIWAN. THE OPPOSITE IS TRUE FOR "OUTSIDE THE COUNTRY."

[41] GOODS, TECHNOLOGIES, SERVICES, AND OTHER ITEMS RELATED TO THE FULFILLMENT OF INTERNATIONAL OBLIGATIONS, INCLUDING DUAL-USE

of national security and interests and the maintenance of the fulfillment of international obligations (Article 25 of the Data Security Law) and important data (Article 31 of the Data Security Law) are subject to cross-border transfer regulations.

iii. **Definition and scope of persons subject to regulations**

A) Under the relevant provisions of the Personal Information Protection Law, personal information controllers are subject to cross-border transfer regulations. A personal information controller is defined as an organization or individual who voluntarily determines the purpose and method of handling personal information in its handling activities (Article 73(1) of the PIPL).

B) Under the relevant provisions of the Cybersecurity Law, critical information infrastructure[42] operators[43] are subject to cross-border transfer regulations.

C) Under the relevant provisions of the Data Security Law, data processors (under Article 27 of the Law) are subject to cross-border transfer regulations.

iv. **Content of regulations**

A) With respect to the Personal Information Protection Law, a case in which a personal information controller is certain to need to provide personal information outside of China due to business or other needs is allowed only if one of the following conditions is met (Article 38 of the PIPL). However, personal information controllers who are critical information infrastructure operators or personal information controllers who reach the quantity specified by the Cyberspace

---

ITEMS, MUNITIONS, NUCLEAR WEAPONS, AND OTHER ITEMS RELATED TO THE MAINTENANCE AND PROTECTION OF NATIONAL SECURITY AND INTERESTS AND THE PREVENTION OF PROLIFERATION, INCLUDING DATA SUCH AS ITEM-RELATED TECHNICAL DATA (ARTICLE 2 AND 4 OF THE EXPORT CONTROL LAW).

[42] THE TERM IS DEFINED AS CRITICAL INDUSTRIES AND SECTORS SUCH AS PUBLIC TELECOMMUNICATIONS AND INFORMATION SERVICES, ENERGY, TRANSPORTATION, WATER CONSERVANCY, FINANCE, PUBLIC SERVICES, E-POLITICAL AFFAIRS, AND OTHER CRITICAL INFORMATION INFRASTRUCTURES THAT, ONCE DESTROYED, LOSE THEIR FUNCTIONALITY, OR HAVE THEIR DATA COMPROMISED, COULD SERIOUSLY HARM NATIONAL SECURITY, THE NATIONAL ECONOMY AND PEOPLE'S LIVELIHOOD, AND PUBLIC INTERESTS (ARTICLE 31, CYBERSECURITY LAW). THE MORE SPECIFIC DETAILS ARE SET FORTH IN ARTICLE 18 OF THE CRITICAL INFORMATION INFRASTRUCTURE SECURITY PROTECTION ORDINANCE, WHICH STIPULATES THAT (I) GOVERNMENT AGENCIES AND ORGANIZATIONS IN INDUSTRIES AND AREAS SUCH AS ENERGY, FINANCE, TRANSPORTATION, WATER CONSERVANCY, SANITATION, EDUCATION, SOCIAL INSURANCE, ENVIRONMENTAL PROTECTION, AND PUBLIC WORKS; (II) ORGANIZATIONS IN TELECOMMUNICATION NETWORKS, RADIO AND TELEVISION BROADCASTING NETWORKS, INFORMATION NETWORKS SUCH AS THE INTERNET, AND CLOUD COMPUTING, BIG DATA AND OTHER LARGE PUBLIC INFORMATION NETWORK SERVICES; (III) ORGANIZATIONS IN INDUSTRIES AND AREAS SUCH AS NATIONAL DEFENSE, SCIENCE AND TECHNOLOGY INDUSTRY, LARGE EQUIPMENT, CHEMICAL INDUSTRY, AND FOOD AND MEDICINE IN SCIENTIFIC RESEARCH AND PRODUCTION; (IV) MASS MEDIA SUCH AS RADIO STATIONS, TV STATIONS, NEWS AGENCIES; AND (V) NETWORK FACILITIES AND INFORMATION SYSTEMS OPERATED AND MANAGED BY OTHER IMPORTANT ORGANIZATIONS THAT, ONCE DESTROYED, LOSE THEIR FUNCTIONS OR LEAK DATA, MAY CAUSE SERIOUS DAMAGE TO NATIONAL SECURITY, NATIONAL ECONOMY, PEOPLE'S LIVELIHOOD AND PUBLIC INTERESTS.

[43] THE 2017 BILL EXPANDS THE PERSONS SUBJECT TO THE CROSS-BORDER TRANSFER REGULATION FROM OPERATORS OF CRITICAL INFORMATION INFRASTRUCTURE TO ALL NETWORK OPERATORS (WHICH, UNDER ARTICLE 76(3) OF THE CYBERSECURITY LAW, IS DEFINED AS NETWORK OWNERS, CONTROLLERS AND INTERNET SERVICE PROVIDERS). IF SUCH PROVISIONS ARE IMPLEMENTED, OPERATORS USING NETWORKS IN CHINA WILL BE SUBJECT TO WIDESPREAD REGULATION.

Administration of China[44] cannot rely on the following grounds (ii) to (iv), and must pass a security assessment by the Cyberspace Administration of China in advance, unless an exemption is granted by law, administrative regulations or the Cyberspace Administration of China when a cross-border transfer is necessary (the second sentence of Article 40 of the PIPL).

1) Pass a security assessment by the Cyberspace Administration of China in accordance with the provisions of Article 40 of the Law.
2) Obtain certification of personal information protection by a professional organization in accordance with the rules of the Cyberspace Administration of China.
3) Conclude a contract with the transferee outside of China in accordance with the standard contract established by the Cyberspace Administration of China, and to stipulate the rights and obligations of both parties.
4) Laws, administrative regulations or other conditions stipulated by the Cyberspace Administration of China

In addition to this, when providing personal information outside of China, personal information controllers must notify the subject of personal information of the name or names of recipients outside of China, the method of contact, the purpose of handling, the method of handling, the type of personal information, and the method and procedures for exercising the rights prescribed in the Personal Information Protection Law from the subject of personal information to recipients outside of China, and must obtain individual consent (Article 39 of the PIPL).

B) According to the Cybersecurity Law, critical information infrastructure operators must store personal information and important data collected and generated in the course of their operations within China, and if there is a definite need to provide such data outside China due to business needs, they must conduct a security assessment in accordance with regulations established by the China Internet Network Information Center, together with relevant departments of the State Council, or if there are separate provisions in laws and administrative regulations, they must follow such provisions (Article 37 of the Cybersecurity Law).

C) With respect to the Data Security Law, data falling under controlled items related to the maintenance of national security and interests and the maintenance of the fulfillment of

[44] ALTHOUGH THERE ARE NO CLEAR STANDARDS UNDER THE CURRENT LAW, THE FOLLOWING INFORMATION SET FORTH IN ARTICLE 4(1) OF THE DRAFT VERSION OF THE MEASURES FOR DATA EXPORT SECURITY ASSESSMENT (DRAFT FOR SOLICITING OPINIONS) PUBLISHED BY THE CYBERSPACE ADMINISTRATION OF CHINA ON OCTOBER 29, 2021 (SPECIFYING THE CASES IN WHICH A SAFETY EVALUATION BY THE CYBERSPACE ADMINISTRATION OF CHINA IS REQUIRED WHEN A DATA CONTROLLER PROVIDES DATA OUTSIDE CHINA) IS HELPFUL.
(I) CASES IN WHICH PERSONAL INFORMATION CONTROLLERS WHO HANDLE PERSONAL INFORMATION OF MORE THAN 1 MILLION PEOPLE TRANSFER PERSONAL INFORMATION OUTSIDE OF CHINA
(II) WHEN TRANSFERRING PERSONAL INFORMATION OF 100,000 OR MORE INDIVIDUALS OR SENSITIVE PERSONAL INFORMATION OF 10,000 OR MORE INDIVIDUALS OUT OF CHINA ON A CUMULATIVE BASIS

international obligations are subject to export control in accordance with the law (Article 25 of the Law). In addition, among important data, (i) the provisions of the Cybersecurity Law apply to the security management of important data collected and generated by critical information infrastructure operators in their operations in China during cross-border transfers, and (ii) for important data collected and generated by other data processors in their operations in China, the Data Security Law stipulates that the China Internet Network Information Center, in cooperation with relevant departments under the State Council, shall enact regulations on security management during cross-border transfers (Article 31 of the Data Security Law).

(3) Regulations that establish requirements to have data reside on local territory

i. Definition and scope of persons subject to regulations

A) Under the Personal Information Protection Law, (i) state agencies (Article 36 of the Law), (ii) critical information infrastructure operators (Article 40 of the PIPL), (iii) personal information controllers whose personal information handled reaches the quantity specified by the Cyberspace Administration of China (Article 40 of the PIPL), and (iv) personal information controllers who provide personal information stored in China to foreign judicial or law enforcement agencies (Article 41 of the PIPL) are subject to regulations that establish data requirements to have data reside on local territory.

B) Under the Cybersecurity Law, operators of critical information infrastructures[45] are subject to regulations that establish requirements to have data reside on local territory for data (first sentence of Article 37 of the Cybersecurity Law).

C) Under the Data Security Law, (i) critical information infrastructure operators and other data processors (Article 31 of the Data Security Law) and (ii) organizations or individuals in China (Article 36 of the Data Security Law) are subject to regulations that establish requirements to have data reside on local territory for data.

ii. Content of regulations

A) Under the Personal Information Protection Law, personal data processed by state agencies must be stored in China, and if there is a definite need to provide it outside the country, it must pass a security evaluation (Article 36 of the PIPL). Article 40 of the Law as described in (2) iv.(a), i.e., critical information infrastructure operators and personal information controllers whose

[45] THE 2017 BILL EXPANDED THE PERSONS SUBJECT TO THE CROSS-BORDER TRANSFER REGULATIONS FROM OPERATORS OF CRITICAL INFORMATION INFRASTRUCTURE TO ALL NETWORK OPERATORS (WHICH, UNDER ARTICLE 76(3) OF THE CYBERSECURITY LAW, IS DEFINED AS NETWORK OWNERS, CONTROLLERS AND INTERNET SERVICE PROVIDERS). IF SUCH PROVISIONS ARE IMPLEMENTED, OPERATORS USING NETWORKS IN CHINA WILL BE SUBJECT TO WIDESPREAD REGULATION.

personal information handled reaches the quantity specified by the Cyberspace Administration of China must store personal information collected and generated in China domestically, unless exempted by law, administrative regulations, or the Cyberspace Administration of China. The stipulation that the personal information generated must be stored domestically, and if there is a definite need to provide it outside China, it must pass a security assessment organized by the Cyberspace Administration of China, can be seen as a regulation on cross-border transfers as well as a regulation on the obligation to store and keep data domestically. In addition, the competent authorities are to process requests for the provision of domestically stored personal information by foreign judicial or law enforcement agencies in accordance with relevant laws and international treaties or agreements that China has signed or is a member, or in accordance with the principle of reciprocity, and no personal information controller shall provide personal information stored in China to foreign judicial or law enforcement agencies without the approval of the competent authority (Article 41 of the PIPL).

B) The discipline in Article 37 of the Cybersecurity Law described in (2) iv. (b) can be taken as regulations on cross-border transfers as well as regulations that establishes requirements to have data reside on local territory for data.

C) The Data Security Law stipulates that the provisions of the Cybersecurity Law shall apply to the secure management of important data collected and generated by critical information infrastructure operators in their operations in China (resulting in the need for security assessments as described above), and that the China Internet Network Information Center, together with relevant departments of the State Council, shall enact regulations for the secure management of important data collected and generated by other data processors in their operations in China (Article 31 of the Data Security Law). In addition, the competent authorities are to controller requests by foreign judicial or law enforcement agencies for the provision of data in accordance with relevant laws and international treaties or agreements that China has concluded or joined, or in accordance with the principle of reciprocity, and no organization or individual in China shall provide data stored in China to foreign judicial or law enforcement agencies without the approval of the competent authorities (Article 36 of the Data Security Law).

5. India

(1) Applicable Laws

In India, there is no comprehensive law on the protection of personal data in force, but there are two

individual laws: the Information Technology Act, 2000[46], which came into force on June 9, 2000 and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (Security Rules)[47], which came into force on April 11, 2011. However, in these laws, there are no provisions that establish regulations specific to cross-border transfers or mandate domestic preservation and domestic storage of data.

On the other hand, for certain industries, there are provisions requiring domestic storage and domestic custody of data, and for the Central Bank of India, there is a Decree on the Storage of Payment System Data (DL Directive)[48] and FAQs on the DL Directive[49] (together with the DL Directive, referred to as the "DL Regulation"). In addition, for telecommunications service providers, there is the Uniform Licensing Act in the field of telecommunications[50].

In addition, there exists[51] a report related to the Bill[52], submitted on December 16, 2021, which proposes to partially amend the Bill No. 373 of 2019 (Bill No. 373 of 2019)[53] submitted to the National Assembly on December 11, 2019, as a comprehensive law on the protection of personal data, although the details are not finalized.

With respect to the provisions in the draft bill of the Personal Information Protection Law that provide for the obligation to store and keep data in the country, there is information available at[54] that it is drafted for the purpose of ensuring security and contributing to criminal investigations, and that the authorities (The Joint Parliamentary Committee) consider it an essential element of data protection.

(2) Regulations that establish requirements to have data reside on local territory

i. Definition and scope of persons subject to regulations

With respect to the DL Regulations, payment system providers (including intermediaries, payment gateway providers, third-party vendors, etc.) subject to approval by the Central Bank of India are subject to regulations that establish requirements to have data reside on local territory for data.

With respect to the Uniform Licensing Act, telecommunications service providers licensed by the Department of Telecommunications under the Act are subject to the regulations governing

[46] https://www.meity.gov.in/writereaddata/files/itbill2000.pdf

[47] https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf

[48] https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244

[49] https://m.rbi.org.in/scripts/FAQView.aspx?Id=130#:%7E:text=The%20entire%20payment%20data%20shall,except%20in%20cases%20clarified%20herein.&text=The%20data%20should%20include%20end,of%20a%20payment%20message%20%2F%20instruction

[50] https://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf

[51] SINCE IT IS UNCLEAR AT THE END OF 2021 WHETHER OR NOT THE PROPOSALS IN THIS REPORT WILL BE ADOPTED AS A BILL, WE WILL NOT INTRODUCE THE CONTENTS OF THE BILL IN THIS REPORT, BUT WE MUST CONTINUE TO MONITOR RELATED TRENDS CLOSELY

[52] http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

[53] http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[54] https://sflc.in/summary-jpc-recommendations-personal-data-protection-bill-2019

requirements to have data reside on local territory.

ii. **Content of regulations**

A) With respect to DL Regulation, it aims to monitor and supervise payment data in order to ensure the healthy development of digital payments and reduce risks from data breaches. All payment system providers (including intermediaries, payment gateway providers, third-party vendors, etc.) subject to approval by the Central Bank of India are required to store information related to their payment systems only in India.

B) Regulated payment system information should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction (Article 2(i) of the DL Directive), and the data should include Customer data (Name, Mobile Number, email, Aadhaar Number, PAN number, etc. as applicable); Payment sensitive data (customer and beneficiary account details); Payment Credentials (OTP, PIN, Passwords, etc.); and, Transaction data (originating & destination system information, transaction reference, timestamp, amount, etc.). (Article 3 of DL FAQ).

C) The DL Directive, in principle, requires that end-to-end information be stored in India, but this does not apply to transactions with certain foreign elements as specified in the DL FAQs (Article 2(i) of the DL Directive). In other words, with respect to information on international transactions that involves handling information from both sides of the transaction, it is permissible to keep a copy of the information from the Indian side outside India, if necessary.

D) The Agreement for unified license prohibits telecommunications service providers licensed by the Department of Telecommunications under the Act from transferring accounting information of service users (excluding international roaming and tariff information) and user information (excluding information pertaining to subscribers outside India who use the network of an Indian operator for roaming) outside India (Article 39(23) (viii) of the Act).

6. Vietnam

(1) Applicable Laws

There is no comprehensive law on the protection of personal information in Vietnam that has come into force, and there are individual laws such as the Cybersecurity Law[55], which came into effect on January 1, 2019 and Decree No. 72 on Management, Provision and Use of Internet Services and

[55] https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx

Online Information, which came into effect on September 1, 2013[56] (hereinafter referred to as "Decree No. 72").

In addition to this, there is a Draft Decree on Personal Data Protection[57] issued in February 2021 that comprehensively defines detailed provisions for the protection of personal data. In the Draft Decree, there are some details that are yet to be finalized, but there are provisions that establish regulations specific to cross-border transfers and that require domestic preservation and domestic storage of data.

(2) Cross-border transfer regulations

i. Regulated conduct

Article 21 of the Draft Decree on Personal Data Protection provides that the act of transfer outside the borders and territory of Vietnam shall be regulated.

ii. Types of data subject to regulations

In the relevant provisions of the Draft Decree on Personal Data Protection, personal data subject to the cross-border transfer regulation is defined as information about individuals or information that identifies or can identify a specific individual[58] (Article 2(1) of the Draft Decree).

iii. Definition and scope of persons subject to regulations

The Draft Decree on the Protection of Personal Data applies to institutions, organizations and individuals concerned with personal data (Article 1(2) of the draft Decree) and provides that all domestic and foreign organizations, enterprises and individuals doing business in Vietnam are liable for violating the Decree (Article 4(2) of the Draft Decree).

iv. Content of regulations

The Draft Decree on Personal Data Protection provides that personal data of Vietnamese citizens may be transferred outside the borders and territory of Vietnam if all of the following requirements (i) through (iv) are met (Article 21(1) of the Draft Decree).

1) Data entity consents to the transfer
2) Original information is preserved in Vietnam.
3) Documentation is provided to prove that the country or territory receiving the information, or a

---

[56] https://thuvienphapluat.vn/van-ban/cong-nghe-thong-tin/nghi-dinh-72-2013-nd-cp-quan-ly-cung-cap-su-dung-dich-vu-internet-va-thong-tin-tren-mang-201110.aspx

[57] http://www.bocongan.gov.vn/van-ban/van-ban-du-thao/du-thao-nghi-dinh-quy-dinh-ve-bao-ve-du-lieu-ca-nhan-240.html#parentHorizontalTab4

[58] "PERSONAL INFORMATION" IS FURTHER CLASSIFIED INTO "BASIC PERSONAL INFORMATION" AND "SENSITIVE PERSONAL INFORMATION" (ARTICLE 2(2) OF THE DRAFT DECREE).

specific region within that country or territory, has a level of personal data protection regulation equal to or higher than the level set forth in this Decree.

4) Obtain written approval from the Personal Information Protection Committee
   In addition to this, the Draft Decree also provides that personal information may be transferred outside of Vietnam in the following cases, even if the requirements (i) through (iv) above are not met (Article 3(3).
5) Data entity consents to the transfer
6) Obtain written approval from the Personal Information Protection Committee
7) There exists a commitment by the data processor to protect personal information.
8) There exists a commitment for the personal information processor to implement privacy measures

Although the above two types of regulations have much in common in terms of their wording, the wording of the proposed Decree is currently unclear in terms of its purpose, and the interpretation of the relationship between the application of Article 21(1) and (3) above and the details of each requirement is unclear.

The above rules can also be viewed as regulations that establish requirements to have data reside on local territory for data.

(3) Regulations that establish requirements to have data reside on local territory

i. Definition and scope of persons subject to regulations

A) The regulations that establish requirements to have data reside on local territory for data under the Cybersecurity Law shall apply to domestic and foreign operators[59] that provide services on telecommunications networks or the Internet or other value-added services in cyberspace in Vietnam (Article 26(3) of the Law).

B) In addition, the rules governing establish domestic preservation and domestic storage regulations for data in Japan under Decree No. 72 apply to the following online service providers (Article 24(2), Article 25(8), Article 28(2), and Article 34(2) of Decree No. 72).
   1) Organizations and companies that have general websites[60] (so-called news distribution services are considered to fall under this category)
   2) Organizations and companies providing social networking services

[59] ALTHOUGH THE WORDING OF THE LAW ALONE COULD BE READ AS IF ALL ONLINE SERVICE PROVIDERS ARE INCLUDED, THE OBLIGATION IS TO BE STIPULATED BY A CABINET ORDER WITH DETAILED ENFORCEMENT REGULATIONS (ARTICLE 26(4) OF THE LAW), SO CLOSE ATTENTION SHOULD BE PAID TO THE DETAILS TO BE STIPULATED BY THE SAID DECREE.

[60] UNDER DECREE NO. 72, A "GENERAL WEBSITE" IS DEFINED AS "A WEBSITE OF AN INSTITUTION, ORGANIZATION OR COMPANY THAT PROVIDES GENERAL INFORMATION, ACCURATELY CITING OFFICIAL SOURCES AND CLEARLY INDICATING THE NAME OF THE AUTHOR OR THE INSTITUTION OF THE OFFICIAL SOURCE AND THE TIME OF PUBLICATION OR BROADCAST" (ARTICLE 20(2) OF DECREE NO. 72).

3) Organizations and companies that provide information content services on mobile telecommunications networks (services that distribute information by SMS, etc. using cell phone networks are considered to fall under this category)
4) Online electronic game service providers

ii. **Content of regulations**

A) Cybersecurity Law stipulates that service providers described in i.(a) are obligated to keep data related to personal information, data related to service users' relationships or data created by service users in Vietnam for a certain period of time determined by the Vietnamese government when collecting, using, analyzing or processing such data (Article 26(3) of the Law). In addition, companies outside of Vietnam that meet such requirements are obliged to establish a branch or representative office in Vietnam (the same Article).
B) Under Decree No. 72, online service providers described in i.(b) are required to install at least one server system in Vietnam that is capable of responding to requests by competent administrative authorities to inspect, verify, store, and provide information in order to respond to customer complaints regarding service provision as determined by the Ministry of Information and Communications (Article 24(2), 25(8), 28(2) and 34(2) of Decree No. 72).
C) As mentioned above, the regulations in the Draft Decree on Personal Data Protection, which are introduced as regulations on cross-border transfers in (2) above, can be regarded as regulations on cross-border transfers as well as regulations that establish requirements to have data reside on local territory for data.

7. Indonesia

(1) Applicable Laws

There is no comprehensive law on the protection of personal data that has come into force in Indonesia, and there are two individual laws: (i) Government Regulation No. 71 of 2019 on the Administration of Electronic Systems and Transactions[61], which came into effect on October 10, 2019 (hereinafter referred to as "2019 Regulation") and (ii) Minister of Communications and Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in an Electronic System[62], which came into effect on December 1, 2016 (hereinafter referred to as "2016 Ministry Regulation").

[61] https://jdih.kominfo.go.id/produk_hukum/unduh/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019+tanggal+10+oktober+2019
[62] https://jdih.kominfo.go.id/produk_hukum/unduh/id/553/t/peraturan+menteri+komunikasi+dan+informatika+nomor+20+tahun+2016+tanggal+1+desember+2016

There is also the Personal Data Protection Bill[63], which was submitted to the National Assembly on January 24, 2020, as a unified decree on personal data protection. The bill also contains a number of provisions that are similar to those in the GDPR and, while not yet finalized, establish regulations specific to cross-border transfers.

The provisions in question have a GDPR-like intent to ensure that the level of protection of individuals is not compromised by the cross-border transfer of data.

(2) Cross-border transfer regulations

i. Regulated conduct

The 2016 Ministry Regulation regulates the transfer of personal data outside of Indonesia.

ii. Types of data subject to regulations

Under the relevant provisions of the 2019 Decree, personal information subject to the cross-border transfer regulation is defined as information that, alone or in conjunction with other information, directly or indirectly identifies an individual, whether through electronic systems or not (Article 1 of the Decree).

In addition, personal data subject to the cross-border transfer regulation is defined in the relevant provisions of the 2016 Provincial Regulation as certain personal data stored and controlled and information whose confidentiality must be protected (Article 1(1) of the Regulation).

iii. Definition and scope of persons subject to regulations

A) Both the 2019 Decree and the 2016 Ministry Regulation apply to electronic system providers (Article 1(4) of the 2019 Decree, etc.).

B) Under the Personal Data Protection Bill, the cross-border transfer regulation applies to the controller of personal data (Article 49 of the Bill).

iv. Content of regulations

A) In the 2016 Ministry Regulation, this is to be carried out in collaboration with the Ministry of Information and Communications (Article 22(1)(a) of the Regulation). In such collaboration, it is stipulated to (i) implement a report that includes, at a minimum, the destination country, the recipient of the transfer, the date of the transfer, and the reason for the transfer, (ii) request assistance as needed, and (iii) implement a report on the results of the transfer (Article 22(2).

B) In addition, the Personal Data Protection Bill states that cross-border transfers shall be subject

[63] https://web.kominfo.go.id/sites/default/files/users/4752/Rancangan%20UU%20PDP%20Final%20%28Setneg%20061219%29.pdf

to one of the following conditions (Article 49 of the Bill)

1) The destination country must have personal data protection rules equivalent or superior to those of Indonesia
2) There must be a international agreement between Indonesia and the destination country
3) There is an agreement between the personal data controller at the source and the personal data controller at the destination regarding the processing of personal data
4) The consent of the data subject has been obtained

(3) Regulations that establish requirements to have data reside on local territory

i. Definition and scope of persons subject to regulations

Regulations governing requirements to have data reside on local territory for data under the 2019 Decree shall apply to electronic system providers appointed by public authorities (Article 20(2) of the Decree).

On the other hand, private sector electronic system providers may manage, process, or store electronic systems and electronic data outside of Indonesia (Article 2(1) of the same Decree). Under the same Decree, the public sector is defined as central and local government agencies (excluding the Financial Services Agency) and persons appointed by government agencies (Article 2(3) and (4) of the same Decree), while the private sector is defined as electronic system providers regulated or supervised by government agencies who have web portals, websites or apps used for specific purposes[64] (Article 2(5) of the same Decree).

ii. Content of regulations

A) Under the 2019 Decree, public sector electronic system providers are required to manage, process or store electronic systems and electronic data in Indonesia (Article 20(2) of the Decree). However, as an exception to such obligation, public electronic system operators may store data outside of Indonesia if the storage technology is not available in Indonesia (Article 20(3) of the same Decree). The criteria for determining whether a case falls under this

[64] THE FOLLOWING PURPOSES ARE DEFINED (ARTICLE 2(5) OF THE SAME DECREE).

1) PROVISION, MANAGEMENT, OR OPERATION OF OFFERS FOR GOODS OR SERVICES OR TRANSACTIONS
2) PROVISION, MANAGEMENT OR OPERATION OF FINANCIAL TRANSACTION SERVICES
3) DISTRIBUTION OF MATERIALS OR PAID CONTENT BY DOWNLOADING THEM TO YOUR DEVICE THROUGH A WEB PORTAL, WEBSITE, EMAIL, OR OTHER APP
4) PROVISION, MANAGEMENT, OR OPERATION OF COMMUNICATION SERVICES SUCH AS SHORT MAIL, VOICE COMMUNICATIONS, VIDEO TELEPHONY, E-MAIL, CHAT ROOMS, NETWORKING SERVICES, AND SOCIAL MEDIA
5) PROVISION OF SEARCH ENGINE SERVICES OR ELECTRONIC INFORMATION IN THE FORM OF TEXT, SOUND, IMAGES, ANIMATION, MUSIC, VIDEO, MOVIES, GAMES, OR ANY COMBINATION THEREOF
6) PROCESSING OF PERSONAL DATA FOR ACTIVITIES IN THE PUBLIC INTEREST RELATED TO ELECTRONIC TRADING ACTIVITIES

"unavailability" category are to be determined by a committee composed of relevant ministries, such as the Minister of Communications and Informatics, but such criteria have not been made public.

B) In addition, in the financial sector, Indonesian non-bank financial institutions, commercial banks, etc. are obligated to store and retain data domestically according to regulations established by the Indonesian Financial Services Agency (OJK Regulation No.4/POJK.05/2021 on Application of Risk Management During the Use of Information Technology by Non-bank Financial Service Institutions, OJK Regulation No. 38/POJK.03/2016 on the Application of Risk Management in the Use of Information Technology by Commercial Banks (amended by OJK Regulation No. 13/POJK.03/2020), etc.).

8. Overview

Table 1: Data-related regulations under the laws of each country

	Cross-border transfer regulations		Requirements to have data reside on local territory	
EU	General Data Protection Regulation (GDPR) [Text footnote 6]			
	Information subject to regulation	Information about an identified or identifiable natural person (personal data)		
	Those who are subject to regulation	controller or processor		
	Content of Regulations	Cross-border transfers are possible only when one of the following conditions is met: (i) If the country to which the transfer is to be made has received an adequacy decision (ii) In case of compliance with the safeguards in Article 46 of the GDPR (Binding Corporate Rules, Standard Contractual Clauses, certification by authorities, etc.) (iii) In cases where the exceptional grounds of Article 49 of the GDPR are met (e.g., consent of the data subject, necessary for a contract in the data subject's interest, necessary for the vital interests of the public, etc.)	Not applicable under personal data protection legislation	
U.S.	Not applicable under personal data protection legislation		Not applicable under personal data protection legislation	
Canada	Not applicable under personal data protection legislation		Not applicable under personal data protection legislation	
China	Personal Information Protection Law [Text footnote 32]		Personal Information Protection Law [Text footnote 32]	
	Information subject to regulation	Non-anonymized information related to identified or identifiable natural persons (personal information)	Information subject to regulation	Non-anonymized information related to identified or identifiable natural persons (personal information)
	Those who are subject to regulation	Personal information controller	Those who are subject to regulation	(i) National Agencies (ii) Critical information infrastructure operators (iii) Personal information controllerswho handles a certain number specified by the Cyberspace Administration of China (iv) Personal information controllers who provide personal information to government agencies
	Content of Regulations	Cross-border transfer of data is possible only if the following conditions are met: (a) Obtaining consent from the data subject + (b) (i) Critical information infrastructure operators, or (ii) Personal information controllers who handles a certain number specified by the Cyberspace Administration of China: Conduct security assessments (iii) Other personal information controllers: (i) security assessment, (ii) certification by the authorities, (iii) execution of a prescribed standard contract, or (iv) other conditions as prescribed by law.	Content of Regulations	(i) (ii) (iii) Requirements to store data domestically and security assessment (iv) Approval from the competent authorities is required to provide the information to government agencies outside of China
	Cybersecurity Law [Text footnote 33]		Cybersecurity Law [Text footnote 33]	
	Information subject to regulation	Data collected and generated domestically (i) names and other information that can identify natural persons (personal information) and (ii) data closely related to national security, economic development, etc. (important data)	Information subject to regulation	Information collected and generated domestically, including (i) names and other information that can identify natural persons (personal information) and (ii) important data
	Those who are subject to regulation	Critical information infrastructure operators	Those who are subject to regulation	Critical information infrastructure operators
	Content of Regulations	Security assessment	Content of Regulations	Requirements to store data domestically and security assessment
	Data Security Law [Text footnote 34]		Data Security Law [Text footnote 34]	
	Information subject to regulation	Data related to (i) the maintenance of national security and interests and the maintenance of the fulfillment of international obligations; and (ii) important data collected and generated domestically	Information subject to regulation	(i) and (ii) below: important data collected and generated domestically (no limitation for (iii))
	Those who are subject to regulation	Regarding (ii) (i) Critical information infrastructure operators (ii) Other data processors	Those who are subject to regulation	(i) Critical information infrastructure operators (ii) Other data processors (iii) Domestic organizations or individuals
	Content of Regulations	Regarding (i) Implementation of export control Regarding (ii) (i): Same as the Cybersecurity Act (ii): In compliance with regulations established by the Cyberspace administration of China together with the relevant departments of the State Council	Content of Regulations	(i): Same as the Cybersecurity Law (ii): In compliance with regulations established by the the Cyberspace administration of China together with the relevant departments of the State Council (iii): Approval from the competent authorities is required to provide the information to government agencies outside of China

	Cross-border transfer regulations		Requirements to have data reside on local territory	
India	Not applicable under personal data protection legislation		The text [Text footnotes 48, 49] of the Decree on the storage of payment system information [Financial sector]	
			Information subject to regulation	End-to-end transaction details and information (payment system information) collected / carried / processed as part of the message / payment instruction
			Those who are subject to regulation	Providers of payment systems subject to central bank authorization
			Content of Regulations	Obligation to store only in India
			Agreement for Unified License [Text footnote 50] [Electronic Communications Sector]	
			Information subject to regulation	Accounting information and user information of service users
			Those who are subject to regulation	Licensed telecommunications service providers
			Content of Regulations	Prohibition of transfer outside India
Vietnam	Decree on Personal Information (Draft) [Text footnote 57]		Cybersecurity Act [Text footnote 55]	
	Information subject to regulation	Information about an individual or information that identifies or can identify a specific individual (personal information)	Information subject to regulation	Data concerning personal information, data concerning service users' relationships or data created by service users
	Those who are subject to regulation	Agencies, organizations and individuals concerned with personal information	Those who are subject to regulation	Businesses that provide services, etc. on domestic information and telecommunications networks or the Internet
	Content of Regulations	Cross-border transfers are possible only when all of the following (i) through (iv) are met (even if (i) through (iv) are not met, it is possible if certain conditions are met) (i) Consent of the data subject (ii) Domestic preservation of original data (iii) Proof of existence of personal data protection regulations in the destination country (iv) Written approval from the Personal Information Protection Committee	Content of Regulations	Obligation to store data related to personal information and data related to the use of services in Vietnam for a certain period of time and to establish a domestic site when collecting, using, analyzing, or processing such data.
			Decree Article 72 [Text footnote 56]	
			Those who are subject to regulation	Online service providers
			Content of Regulations	Obligation to install one or more domestic servers
Indonesia	Regulation No.71 of 2019 [Text footnote 61] and Regulation No.20 of 2016 [Text footnote 62]		Regulation No.71 of 2019 [Text footnote 61]	
	Information subject to regulation	(i) Information that directly or indirectly identifies an individual (personal information) (ii) Information that must be stored and controlled and whose confidentiality must be protected (personal data)	Those who are subject to regulation	Electronic system providers appointed by public agencies
	Those who are subject to regulation	Electronic system providers	Content of Regulations	Obligation to manage, process and store electronic systems and electronic data in the
	Content of Regulations	Requires collaboration with the Minister of Communication and Information Technology of the destination country, the party to which the transfer is to be made, the date of the transfer, the reason for the transfer, and the obligation to report the results of the transfer		
	Personal Data Protection Bill [Text footnote 63]		FSA Regulations [Financial Sector]	
	Information subject to regulation	Personal data	Those who are subject to regulation	Non-bank financial institutions, commercial banks, etc.
	Those who are subject to regulation	Personal data controller		
	Content of Regulations	Cross-border transfers are possible only if one of the following conditions is met: (i) Personal data protection regulations in the destination country must be at least equivalent to those in Indonesia (ii) Existence of international agreement with the destination country (iii) Existence of a contract for the processing of personal data between the source and the transferee (iv) Consent of the data subject	Content of Regulations	Requirements to store data domestically

Chapter 3: Conclusion

Since its first meeting on November 2, 2021, the Expert Group on DFFT has held three meetings to deepen discussions on an interoperable framework for the cross-border transfer of data. In order to discuss concrete measures, mechanisms and systems to ensure the necessary "trust" under "Data Free Flow with Trust (DFFT)," the Expert Group on DFFT aims to identify the practical barriers and propose specific policy options to eliminate them, rather than to discuss the list of abstract norms. In so doing, the Expert Group is working backward from the goal of "ensuring necessary data to be transferred across borders in order to sustain economic growth and social prosperity to reach the policy measures that are necessary, and the norms and rules to be established to enable them."

In order to embody the vision of DFFT as a concrete set of policy measures and implementing mechanism, it is important for countries that share basic values to establish interoperable mechanisms across the different approaches of data governances stemming out of different regulatory needs to mitigate threats posed by the use of data, such as privacy, security, and intellectual property protection. In order to smoothly facilitate international data distribution, "trust" must exist not only between governments, but also among all stakeholders involved in the data life-cycle. The data life-cycle relies on a vast network that extends into both physical and cyberspace, where various actors are involved, including companies (including data users, data processors (cloud providers), network providers, etc.), natural persons, regulatory authorities, and international organizations. Therefore, the international mechanism that the embodiment of the DFFT should aim at identification and minimization of the barriers to data flow between governments, but also, from a bottom-up perspective, those that currently exist between the various actors.

This report summarizes the results of company interviews and surveys of laws and regulations in each country, focusing on the following three issues from the perspective of identifying barriers to the cross-border transfer of data by entities that utilize data, such as companies.

- 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)?
- Also, what barriers do companies face in transferring data across borders?
- What are the main perspectives regarding data-related regulations in each country?

First, Chapter 1 sought to "visualize" the barriers to cross-border transfer of data by identifying a part of data's life-cycle through examining information gathered from company interviews and other sources in a comparable form. In each step of the life-cycle i.e. data production,

processing, analysis, and integration, different stakeholders are involved and various patterns of "cross-border transfer" occur.

And during this data life-cycle, companies' business options diverge by the existence of barriers to the cross-border transfer of data. This divergence is summarised in this report as "company requests" and "challenges from the company's perspective". Having some common understanding among all actors involved in this data life-cycle of how data is handled across sectors, what stakeholders are involved in cross-border transfers, and to whom and how the costs of regulation can be passed on is a necessary foundation for the DFFT vision to take a concrete form. Of course, such "barriers" from the perspective of the entities utilizing the data could also be systems to ensure the legitimate legal interests of the respective countries, such as privacy protection and security. Therefore, this report also focuses on the nature of the barriers themselves, from the perspective of balancing the wide variety of regulatory needs with the economic and social value created by the international sharing of data.

By identifying specific situations of cross-border transfers of data, a number of cases have emerged in which the cost of business operations can be significantly reduced by international cooperation on policies, capacity building, and also by simply clarifying the situations that cause the rise of cost for cross-border transfer of data: for example, over-regulation that seems to result from digital silos among domestic regulators; lack of legal transparency resulting from the fact that the substance of regulatory requirements rely on interpretative rules and other related rules and guidelines; legal stability and related research costs on the part of companies due to frequent changes in these rules; regulations that are seemingly resulting from a lack of understanding of the business reality regarding data transfer to third countries; lack of common parameters of "security" "adequate level of protection"; complicated and expensive requirements for obtaining certification and standards for data handling for specific countries or regions. Others voiced a lack of clarity regarding the various activities that could be encompassed by the term "cross-border transfer" of data. During the company interviews, various situations were identified that are difficult to conceptualize as an analogy to trade of goods and services between territories. Tackling the barriers to the cross-border free flow of data could take various forms depending on the business models, the regulatory approaches, the customs of business in the field, and other technical conditions.

Next, based on the fact that the specific definition of "cross-border transfer" at this point in time comes down to a matter of interpretation of regulations in each country, Chapter 2 summarizes relevant information on regulatory systems, mainly data protection laws in each country. In some cases, it is difficult to compare the regulatory systems of different countries because

different laws, such as privacy protection and security laws, have different purposes and restrictions on cross-border transfers of data. The regulatory systems that are gradually being introduced in various countries differ not only in terms of the information subject to cross-border transfer regulations and the requirements for cross-border transfers to be permitted, but also in terms of the addressees of requirements to have data reside on local territory and in terms of the requirements set, etc. In recent years, the cost for global companies that perform cross-border data transfer to comply with the laws of each country has become increasingly significant.

In light of this situation, many companies called for a simple, internationally accepted common definition and classification (taxonomy). However, as mentioned in the Introduction, while data itself is multifaceted in nature and can be classified in various ways depending on purpose and context, there is always a problem of interpretation at its boundaries. Although there are laws and regulations in various countries that define data as "personal information" in their regulatory systems, for example, in classifying personal information and non-personal information, even anonymized information may have personal identifiability under certain conditions, or it may be possible to identify an individual's behavioral patterns by combining it with other data. In some countries/regions, encrypted personal information (e.g., hashes) might also be treated as personal information by definition. Other typical classifications, such as the distinction between public and private data, are fraught with similar problems. Although the nature of such data makes it difficult to establish common international definitions and classifications in a simple and easily implementable form, efforts to clarify each country's respective definitions and classifications should continue, and it is important that studies be conducted to ensure harmonization at the operational level from the perspective of reducing corporate burden.

Based on the above considerations, the DFFT Expert Group identified the following five elements as core areas for DFFT embodiment and proposed elements to be considered in each area.

1) Transparency

The analysis of the needs of companies conducted in this report revealed that there are overlapping laws and regulations that have a restraining effect on cross-border transfers of data by companies, such as general laws and business jurisdiction laws, that the specific requirements of these regulations depend on numerous implementation rules and interpretation rules, and that frequent revisions are reported. Since ensuring transparency contributes to all governments and stakeholders involved in the data life-cycle, it may be necessary to share perceptions and issues related to ensuring transparency with countries that share basic values, and to consider the contents of encouragement and international

cooperation for improvement (information sharing, reporting systems, sharing guidelines and best practices, etc.).

2) Technology and Standardization

Along with the lack of transparency, another situation that emerged regarding the cross-border transfer of data is the challenges to enhancing the interoperability. In particular, many companies point out the lack of clarity for them regarding the privacy and security protections required to ensure when transferring data to third countries, in light of their specific business circumstances. The businesses often have limited clue what would be the parameters of "being sufficiently compliant" with the standards required under the terms such as "adequate", "safe" of provisions and would like to have the common understanding across the countries where the data frequently travel each other. It may also be necessary to stimulate international understanding and discussion on specific technologies for data storage, analysis, and other data processing that can be used as a guide for ensuring privacy, security, etc., as well as on how to implement technologies to lower regulatory compliance costs. Other policy options should also be studied and compared such as the need for standards for the implementation of such technologies. Seeking enhanced coordination and involvement among multi-stakeholders, particularly industry is also necessary.

3) Interoperability

Along with issues that need to be addressed immediately, such as ensuring transparency and improving operations through technology and standards, many companies have highlighted the lack of clarity regarding the equivalence and differences in protection standards required by various regulations in different countries as barriers to the cross-border transfer of data. While this mutuality can be ensured by standardized technology, there have been various attempts at mutuality, such as mutual authentication of adequacy of personal data protection between two countries or certification schemes between multiple countries by third-party certification authorities. Given the different national systems in each country regarding cross-border transfer of data, it would be necessary to investigate various policy options other than in the pillar of technology and standardisation to ensure "interoperability". In doing so, from the perspective of ensuring security and privacy, there may already be certifications required to be obtained by country or region, and the possibility of ensuring mutuality of those standards should also be included in the scope of consideration

4) Complementarity with related systems

From the perspective of making policy proposals at international forums such as the G7, it is necessary to enhance them in a complementary and harmonized manner with existing efforts

to develop digital trade principles and rules (such as the G7 Digital Trade Principles), as well as with discussions and regulatory cooperation in the privacy fields. The DFFT is an approach that seeks to find as harmonious a solution as possible to the various interests surrounding the cross-border transfer of data. In so doing, establishing a forum where the cross-cutting discussion focusing on the topic of cross-border free flow of data takes place would be useful, proceeding under the common premises.

5) Implementation of the DFFT embodiment implementation framework (Implementation)

It is necessary to embody an institutional arrangement to implement the policy proposals to be developed around the four pillars above, first among countries that can agree on the DFFT vision and promote policies that are DFFT friendly. (e.g., reporting systems and reviews of each country's efforts to amend its laws in order to ensure transparency).

The interim report is a summary of outcome from the three meetings held by the Expert Group on DFFT, which was concluded in February 2022. The Expert Group on DFFT for the next term will focus on in-depth discussion on the possible policy options around the five pillars prioritized above to materialize the framework of DFFT while ensuring and enhancing the cross border free flow of data on a concrete and pragmatic basis.