

ADDENDUM-2

E - COMMERCE

There have been ongoing discussions on e-commerce at the WTO since the formulation of a Work Programme in 1998. With the fourth industrial revolution and technological advancement and expansion of cross-border business, the awareness for the necessity of international rules on e-commerce has been particularly heightened in recent years. Rules on e-commerce are also being discussed under various international frameworks other than the WTO, such as G7, G20, OECD, and APEC. It has also become a major trend to include regulations on e-commerce in EPAs/FTAs.

MAIN ISSUES ON E-COMMERCE

E-commerce has prompted WTO discussions regarding its relationship with existing WTO agreements because it is a new form of trade that frequently involves cross-border transactions. Specific areas being discussed with respect to e-commerce are as follows¹.

(1) DIGITAL CONTENT UNDER CURRENT WTO AGREEMENTS

E-commerce has brought substantial changes to the distribution structures for goods and services, but consensus has not been reached yet as to the concept of e-commerce and how to regulate this type of transaction within the context of the WTO.

The issue of classification of digital contents has been discussed for years. Depending on whether consideration for exchanged digital contents are classified, whether as goods prices, services fees, or fees relating intellectual property rights, the rules that apply regulating the digital contents differ. It also has been pointed out that trade distorting effects may occur if there is discriminatory treatment between physical distribution and network distribution.

The EU asserts that provision of digital contents is a service activity and should be disciplined only by the GATS. It also asserts that, from the standpoint of technical neutrality, digital contents should not be treated differently depending on whether they are provided through broadcasting services or through electronic commerce.

Japan's position is that where recording and cross-border transactions of digital contents through carrier media, fall within the coverage of GATT disciplines, it is appropriate that the same digital contents transmitted through the Internet should also be granted unconditional application of MFN and national treatment as under the GATT. The U.S. similarly argues that the discussion regarding digital contents should not be limited to discussions on whether digital contents should be regulated under the GATT or the GATS. Rather, it is essential to keep in mind that the discussion contributes to develop electronic commerce and that the disciplines on digital content should not reduce the level of market access currently enjoyed. Japan is wary of the EU's position that electronic commerce should be governed entirely by the GATS, because by making such argument, the EU may be trying to make the e-commerce field subject to the most-favored-nation exemptions and

¹ * See also the "electronic commerce" section in Part III, Chapter 7 for general rules on e-commerce (including chapters on e-commerce in EPAs).

reservations of market access and national treatment obligations that the EU has invoked for the 155 service sectors (particularly visual content and broadcasting), primarily for cultural reasons. Although the concepts of digital contents still need to be examined, it is essential to assure basic WTO principles, such as most-favored-nation and national treatment, to apply to digital contents in order to foster the growth of e-commerce.

(2) CUSTOM DUTIES ON ELECTRONIC TRANSMISSIONS

Digital content that used to be delivered physically, for example on floppy disks and CD-ROMs, is increasingly being delivered on-line. The main problem in attempting to tax these transactions is that it is almost impossible for customs agencies to capture them. If one attempts to tax electronic transmission of digital contents (for example, capturing the transmission log) as a substitute, one runs the risk of imposing taxes far in excess of or short of the value of the content because the value of digital content itself is not always proportionate to the transmission volume.

In addition to these technical difficulties in collecting customs duties on electronic transmissions, there is also the need to ensure a free trading environment to foster the growth of e-commerce. This has led many to support the establishment of an international agreement not to impose customs duties on on-line transactions.

At the Second WTO Ministerial Conference in 1998, Members agreed to a “Ministerial Declaration on Global Electronic Commerce” that promised to maintain the current practice of not imposing customs duties on electronic transmissions until the next Ministerial Conference (1999) (moratorium on payment of customs duties). However, when physical goods are moved along with e-commerce transactions, tariffs apply as with ordinary transactions.

The impasse at the Third Ministerial Conference in 1999 delayed agreement on the handling of the moratorium on payment of customs duties. The Fourth Ministerial Conference in Doha, Qatar in November 2001, however, officially announced that the moratorium would be extended until the Fifth Ministerial Conference. Although the September, 2003 Fifth Ministerial Conference in Cancun collapsed and the taxation moratorium was not extended, Members agreed in the General Council at the end of July 2004 that the moratorium would be extended until the Ministerial Conference in Hong Kong scheduled for the end of 2005. Afterward, Members agreed to extend the moratorium until the next Ministerial Conference, at the Sixth WTO Ministerial Conference in Hong Kong (December 2005), the Seventh Ministerial Conference (December 2009), the Eighth Ministerial Conference (December 2011), the Ninth Ministerial Conference (December 2013), the Tenth Ministerial Conference (December 2015) and the 11th Ministerial Conference (December 2017).

(Reference: Value Added Tax (VAT) on Electronically Distributed Services)

Where consumers receive digital contents and other services electronically, such as via the Internet from abroad, if no value added tax (VAT) is levied on such services whereas VAT is levied on similar services provided electronically by domestic companies, this could lead to distortion of competition between domestic and foreign companies. At the Ottawa Conference on Electronic Commerce in 1998, the OECD Committee on Fiscal Affairs presented a basic framework for making cross-border transactions of services subject to the levying of VAT in the countries where services were consumed. Recommendations based on this framework is published in 2003.

Under European Council Directive (2006/112/EC), for transactions of digital contents between non-EU businesses and EU consumers, non-EU businesses will be required to levy a VAT in the member state where the consumer of the service resides and pay it in the state where they register

for VAT. Non-EU businesses may register for VAT in all member states where they provide services and file VAT returns in these states, or may choose to register in only one member state and pay VAT via that state using the Mini One Stop Shop (MOSS) scheme.

In Japan, a consumption tax had been imposed on services provided electronically by domestic companies, whereas similar services provided by foreign companies had been exempt from taxation. However, under the amended Consumption Tax Act put into effect in October 2015, Japan imposes the consumption tax in the latter case as well. Accordingly, foreign companies that electronically provide services to consumers in Japan now are required to file consumption tax returns with Japanese tax offices.

(3) FISCAL IMPLICATIONS OF E-COMMERCE

It is difficult in electronic commerce to identify where production and consummation were undertaken. This raises the question of how to harmonize the traditional concept of state taxation and its practices. Developing countries have expressed concern that the expansion of e-commerce will lead to a reduction in state tax revenues. In order to convince developing countries otherwise, it is necessary to study the positive effects that the promotion of e-commerce will have on national economies as a whole and on the negative impacts that may be seen in state tax revenues.

HISTORY OF WTO DISCUSSION ON E-COMMERCE

The history of WTO discussions on e-commerce is as follows:

(1) DECISION OF A WORK PROGRAMME AT THE SECOND WTO MINISTERIAL CONFERENCE (MAY 1998)

At the second WTO Ministerial Conference (the Geneva Ministerial Conference) in May 1998, ministers adopted a “Ministerial Declaration on Global Electronic Commerce.” The Declaration paved the way for the formulation of a work programme for the consideration of all trade-related aspects of e-commerce and instituted a moratorium on payment of custom duties on electronic transmissions.

(2) CREATION OF WORK PROGRAMME AND DISCUSSION IN SUBSIDIARY BODIES (OCTOBER 1998 TO JULY 1999)

The electronic commerce work programme was created in October 1998 in response to the May 1998 declaration adopted at the Second WTO Ministerial Conference. Subsidiary bodies (the Council for Trade in Goods, Council for Trade in Services, Council for TRIPS, and Committee on Trade and Development) discussed these issues until July 1999 and reported their findings to the General Council.

(3) SUSPENSION AND RE-OPENING OF THE E-COMMERCE WORK PROGRAMME (DECEMBER 1999 TO DECEMBER 2000)

The E-Commerce Work Programme had been suspended since the collapse of the Seattle Ministerial Conference in October of 1999. However, strong demands for liberalization and rule formulation for rapidly developing e-commerce-related sectors spurred the General Council to announce the resumption of the Work Programme in July 2000, nearly six months after its

suspension at the Seattle Ministerial. While various WTO subsidiary bodies are addressed e-commerce issues, Japan and other WTO Members have come to recognize that many issues regarding the e-commerce and WTO disciplines require crosscutting consideration beyond individual agreements. As such, the WTO established a taskforce to study e-commerce issues in an inter-disciplinary manner so as to develop a broad understanding of the impact that it will have on WTO disciplines (the impact on trade in goods, services and intellectual property).

Subsequently, it was decided to hold a dedicated discussion on e-commerce in June 2001 as an arena for intensive discussion among experts on crosscutting issues.

(4) FOURTH WTO MINISTERIAL CONFERENCE IN DOHA (NOVEMBER 2001)

The Fourth WTO Ministerial Conference adopted a Ministerial Declaration in which it was agreed to continue the moratorium on payment of customs duties until the Fifth Ministerial Conference. Members also agreed to continue the Work Programme on e-commerce and instructed the General Council to consider the most appropriate institutional arrangements for handling the Work Programme, and to report on further progress to the Fifth Session of the Ministerial Conference.

(5) DISCUSSIONS AFTER THE DOHA MINISTERIAL CONFERENCE

After the Doha Ministerial Conference, e-commerce issues continued to be examined principally in the dedicated discussion under the General Council. At the second meeting (May 2002) and thereafter, discussions on classification issues and fiscal implications have continued. Along with other countries, Japan actively contributes and has submitted a paper outlining its cooperation in IT areas from the perspective of development. Since a seminar under the auspices of the Committee on Trade and Development was held in April 2002, developing countries were interested in these issues. As a result of Members' efforts and intensive discussions, developing countries gradually increasingly understand the importance of promoting electronic commerce.

The United States proposed that Members seek to reach an agreement on basic principles (assurance of free trading environment, expansion of market access, permanent moratorium on customs duties, etc.) for the further development of e-commerce. This idea was broadly supported by developed countries.

Moreover, parties agreed during the July 2004 General Council meeting that the moratorium on payment of customs duties, which was scheduled to be agreed on in the Fifth WTO Ministerial Conference, would be extended until the Sixth WTO Ministerial Conference.

(6) SIXTH WTO MINISTERIAL CONFERENCE IN HONG KONG (DECEMBER 2005)

The Sixth WTO Ministerial Conference declared that Members would maintain their current practice of not imposing customs duties on electronic transmissions until the next Session of the Ministerial Conference. Members took note that the examination of issues under the Work Programme on Electronic Commerce was not yet complete, and they agreed to reinvigorate that work, including development-related issues and discussions on the trade treatment of electronically delivered software.

(7) SEVENTH WTO MINISTERIAL CONFERENCE IN GENEVA (DECEMBER 2009)

Since no regular WTO Ministerial Conference was held between the Hong Kong Ministerial Conference and the December 2009 Conference in Geneva, the moratorium on payment of customs

duties had been ongoing. At the 2009 Ministerial Conference, however, Cuba, among others, said that developing nations were not experiencing sufficient benefits from Electronic Commerce, and opposed maintaining the moratorium. However, since there were some developing countries pressing for the extension of the moratorium, claiming they benefited from it, it was agreed to extend the moratorium until the next Ministerial Conference in 2011. Concerning the Work Programme on Electronic Commerce, it was agreed: a) to revitalize the work energetically; b) for the General Council to conduct regular reviews on the progress of the Work Programme; and c) for the Work Programme to include discussions on the fundamental WTO principles and the handling of software sent electronically during trade.

(8) EIGHTH WTO MINISTERIAL CONFERENCE IN GENEVA (DECEMBER 2011)

At the eighth WTO Ministerial Conference, WTO Members agreed to extend their current practice of not imposing customs duties on electronic transmissions until the ninth Ministerial Conference. Concerning the Work Programme on Electronic Commerce, from the perspective of enhancing access to public internet sites, it was agreed to: (a) continue the reinvigoration of the Work Programme, with special consideration toward developing countries, and particularly least developed country Members; (b) to examine access to e-commerce by micro-, small and medium-sized enterprises; and (c) for the General Council to hold periodic reviews (during sessions of the Work Programme in July and December 2012 and July 2013) to assess the progress of the Work Programme and consider any recommendations on possible measures related to electronic commerce to be adopted at the next Ministerial Conference.

(9) NINTH WTO MINISTERIAL CONFERENCE IN BALI (DECEMBER 2013)

At the ninth WTO Ministerial Conference, Members agreed to extend their current practice of not imposing customs duties on electronic transmissions until the next Ministerial Conference. Concerning the Work Programme on Electronic Commerce, it was agreed to continue active work, comply with the basic principles of the WTO (including non-discrimination, predictability, and transparency), expand application of e-commerce while giving special considerations to developing countries (in particular, least developed countries) and countries with limited access to e-commerce is not widely used, continue investigations of access to electronic commerce by micro-, small and medium-sized enterprises, and hold periodic reviews on the progress status of the Work Programme by the General Council.

(10) TENTH WTO MINISTERIAL CONFERENCE IN NAIROBI (DECEMBER 2015)

At the tenth WTO Ministerial Conference, Members agreed to extend their current practice of not imposing customs duties on electronic transmissions until the next Ministerial Conference. They also agreed to continue the Work Programme on Electronic Commerce and hold a periodic review on the progress status of the Work Programme in meetings of the General Council, etc. by the next Ministerial Conference.

Since the tenth WTO Ministerial Conference, e-commerce has gathered strong attention from WTO members. At the Workshop on Electronic Commerce held in July 2016, Members submitted various proposals. With an intent to actively participate in the formation of specific e-commerce rules at the WTO, Japan also submitted a proposal, which included provisions for free cross-border transfer of information by electronic means, for prohibition of requiring the establishment of computer-related facilities, and prohibition of obligating disclosure of source code. At the Workshop on Electronic Commerce held in October 2016, however, the content of these proposals

was not discussed, as some Members expressed concerns about discussing such rules at this Workshop. Discussions concerning e-commerce have been stalling since then.

(11) 11TH WTO MINISTERIAL CONFERENCE IN BUENOS AIRES (DECEMBER 2017)

Due to the above situation, at the 11th WTO Ministerial Conference, it was an important issue whether Ministers could agree on having cross-sectoral discussions in order to promote discussions on e-commerce at the WTO. Many countries, including both developed and developing countries, proposed the establishment of a new cross-sectoral platform beyond the sectors covered by the four affiliate bodies (the Council for Trade in Services, the Council for Trade in Goods, the Council for TRIPS, and the Committee on Trade and Development) or the institutionalization of the Workshop on Electronic Commerce. However, some developing countries strongly opposed the idea of changing the conventional approach to the discussion and insisted on continuing discussions by sector as is conventionally done. As a result, an agreement on the implementation of cross-sectoral discussion could not be reached. As with the tenth WTO Ministerial Conference, Members only agreed on periodic reviews on the progress status of the Work Programme held at the meetings of the General Council.

Amid such situation, Japan, Australia, and Singapore held a voluntary Ministerial meeting on e-commerce, which was participated in by Members hoping to actively promote discussions on e-commerce. After the completion of this meeting, the 70 participant countries issued a joint statement. This joint statement included that: [1] the countries share the goal of advancing electronic commerce work in the WTO; [2] the countries recognize the important role of the WTO in promoting open, transparent, non-discriminatory and predictable regulatory environments in facilitating electronic commerce; and [3] the countries will initiate exploratory work together toward future WTO negotiations on trade-related aspects of electronic commerce in the first quarter of 2018, and participation will be open to all WTO Members. The joint statement set the direction of future discussions on e-commerce at the WTO; the discussions will be led voluntarily by countries willing to do so.

REFERENCE

TRADE PRINCIPLES FOR INFORMATION AND COMMUNICATION TECHNOLOGY SERVICES

These principles provide the ideas obtained through the generalization of the commitment stipulated in the chapters on electronic commerce and telecommunication services of the EPAs/FTAs (for details, see the section on electronic commerce in Part III, Chapter 7). The contents agreed upon are not legally binding, but aim to spread the principles to third-party countries through international trade negotiations. Such principles were agreed among the US and the EU in 2011, followed by amongst the US and Japan.

The first set of Trade Principles for ICT Services was the "United States-EU Trade Principles for Information and Communication Technology Services" (announced on April 4, 2011; circulated to the Members of the Council for Trade in Services in July 2011), which was agreed to by the United States Trade Representative (USTR) and the European Commission. The principles support the global development of ICT networks and services in cooperation with other countries, and aim to enable competition in trade of the other country with service providers on equal grounds.

The Japan-United States Trade Principles for ICT Services (announced on January 27, 2012) was developed in the framework of the United States-Japan Economic Harmonization Initiative. The objective is to ensure transparency of regulations, share views on promoting trade in ICT services, and jointly disseminate the contents to other countries. Two items were added to the United States-EU principles; there are twelve all together.

Then the contents of both sets of principles are compared (refer to Figure II-Add2-1), the ten common items are almost the same. However, placing importance on cultural diversity is reflected strongly in the preamble of the United States-EU principles, which state that public funds and subsidies for the enhancement of cultural diversity is an exception to the principles. (For the relationship between the Japan-United States Trade Principles for ICT Services and personal information protection and privacy policies, see page 636 of the 2017 edition.)

Figure II-Add-2 Comparison of Trade Principles for ICT Services

		Japan - United States Trade Principles for ICT Services	United States - EU Trade Principles for ICT Services
Announced		January 27, 2012	April 4, 2011
Preamble	Intention	Same as United States - EU.	To promote the implementation of these principles within their bilateral economic relationship and in their trade negotiations with third countries.
	Exception	These principles are without prejudice to governments' rights and obligations under the WTO and to exceptions contained in the GATS. These principles are without prejudice to policy objectives and legislation in areas such as the protection of intellectual property and the protection of privacy, including of health information, and of the confidentiality of personal and commercial data. These principles are not intended to apply to financial services.	These principles are without prejudice to policy objectives and legislation in areas such as the protection of intellectual property and the protection of privacy and of the confidentiality of personal and commercial data, and the enhancement of cultural diversity (including through public funding and assistance). These principles are not intended to apply to financial services.
	Management	These principles are to be reviewed annually, with a view to discussing their implementation and use and to further refining and expanding them as appropriate.	These principles are to be reviewed biannually, with a view to discussing their implementation and use and to further refining and expanding them as appropriate.
Provisions	Transparency	Same as United States - EU. (Article 1)	Governments should ensure that all laws, regulations, procedures, and administrative rulings of general application affecting ICT and trade in ICT services are published or otherwise made available, and, to the extent practicable, are subject to public notice and comment procedures. (Article 1)
	Cross-border information flows	Same as United States - EU. (Article 2)	Governments should not prevent service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries. (Article 3)

Open Networks, Network Access and Use	In addition to the United States - EU, governments recognize that Internet access providers should strive to avoid unreasonable discrimination in transmitting lawful network traffic. (Article 3)	Governments should promote the ability of consumers legitimately to access and distribute information and run applications and services of their choice. Governments should not restrict the ability of suppliers to supply services over the Internet on a cross-border and technologically neutral basis. (Article 2)
Interconnection	Same as United States - EU. (Article 4)	Governments should ensure that public telecommunications service suppliers have the right and the obligation to negotiate and to provide interconnection on commercial terms with other providers. In addition, in accordance with the GATS Reference Paper, countries should ensure interconnection with major suppliers at cost-oriented, non-discriminatory rates. (Article 9)
Unbundling of Network Elements	Governments, through their regulators, should have the authority to require major suppliers in their respective territories to offer public telecommunications service suppliers access to network elements on an unbundled basis on terms and conditions, and at cost-oriented rates, that are reasonable, non-discriminatory and transparent. (Article 5)	No provision.
Local Infrastructure and Local Presence	Almost the same as United States - EU. (Article 6)	Governments should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services. (Article 4)
Foreign Ownership	Same as United States - EU. (Article 7)	Governments should allow full foreign participation in their ICT services sectors. (Article 5)
Use of Spectrum	Almost the same as United States - EU. (Article 8)	Governments should maximize the availability and use of spectrum by working to ensure that it is managed effectively and efficiently. Governments are encouraged to empower regulators with impartial, market-oriented means, including auctions, to assign terrestrial spectrum to commercial users. (Article 6)
Digital Products	Governments should provide treatment no less favorable to some digital products as compared to other like digital products based on place of creation or production, and nationality of author. (Article 9)	No provision.
Regulatory Authorities	Same as United States - EU. (Article 10)	Governments should ensure that the regulatory authorities that oversee ICT services sectors are legally distinct and functionally independent from all service providers, and regulatory decisions and procedures should be impartial. (Article 7)
Authorizations and Licenses	Same as United States - EU. (Article 11)	Governments should authorize the provision of competitive telecommunications services after simple notification, and should not require legal establishment as a condition of supplying a service.

			Licenses should be restricted in number for specified regulatory issues, such as the assignment of frequencies. (Article 8)
	International Cooperation	Same as United States - EU. (Article 12)	Governments should cooperate with each other to increase the level of digital literacy globally and reduce the "digital divide". Article 10)

COLUMN REGULATIONS CONCERNING DATA LOCALIZATION

1. Background

In recent years, the principle of free cross-border information transfer has been confirmed in various EPAs/FTAs and at various international forums to promote global economic growth.² On the other hand, some countries have introduced regulations to retain personal information and data important to the state within its territory (“data localization”) from the viewpoints of protection of individual human rights, protection of domestic industries, and national security. This Column compares and gives an overview of the cross-sectoral, general data regulations concerning data localization in the EU, China, Viet Nam, Indonesia, and Russia. Note that data localization regulations are also sometimes included in industry regulations, although these are not covered in this Column.

2. Comparison of Regulations

As stated above, this Column compares the following data protection regulations as major examples and gives an overview of their purpose and content: [1] Regulation (EU) of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as the General Data Protection Regulation or GDPR);³ [2] Cybersecurity Law of China; [3] Cybersecurity Law of Viet Nam;⁴ [4] Republic of Indonesia Minister of Communications and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System (hereinafter referred to as the “Personal Data Protection Regulation”); and [5] Russian Federal Law on Personal Data. These data protection regulations will be compared in terms of the following two aspects: [i] restrictions on cross-border transfers of data existing in the country’s territory; and [ii] obligation to retain data necessary to conduct business within the country’s territory (data localization obligation). Below, this Column summarizes the above regulations in terms of whether they impose restrictions on international data transfers and data localization obligations, and if applicable, the content of such restrictions.

(1) Regulation on Cross-Border Data Transfers

The EU, China,⁵ Viet Nam,⁶ Indonesia,⁷ and Russia⁸ all restrict the international transfer of personal information, etc. The differences among the regulations are summarized below. The

² For an overview of formation of rules on e-commerce, see the Column “New Trend in Rule-Making for E-Commerce” on page 633 of the 2017 Report on Compliance by Major Trading Partners with Trade Agreements - WTO, EPA/FTA and IIA -.

³ Scheduled to come into force on May 25, 2018.

⁴ Scheduled to be adopted in June 2018. In this Column, the 14th edition of the draft was referred to.

⁵ Article 37 of the Cybersecurity Law.

⁶ Article 48, paragraph 4 of the proposed Cybersecurity Law (14th edition).

⁷ Article 22 of the Regulation on Personal Data Protection.

⁸ Article 12 of the Russian Federal Law on Personal Data.

cybersecurity law in China and the similar law in Viet Nam regulate a wider scope for cybersecurity purposes.

A. Basic Content of Regulation

While the EU GDPR guarantees the freedom of the transfer of personal information within the EU territory,⁹ it restricts transfer of such information to a third country.¹⁰ However, the purpose of such restriction by the EU is to protect personal information vis-à-vis a third country; thus, the GDPR provides that personal information can be transferred to a third country if said third country fulfills certain criteria, such the protection level of personal information.

The Chinese Cybersecurity Law is aimed at ensuring national security. In addition to personal information, it protects data closely related to national security, economic development, and social public interests.¹¹ This law includes restrictive measures against the provision of personal information and important data to a foreign third party, such as compulsory security assessment on cross-border data transfers. The Vietnamese Cybersecurity Law also has a similar legal structure. These laws can be interpreted as restricting cross-border data transfers.

B. Scope of Information Subject to Regulation

The scope of regulation in the EU, Indonesia, and Russia is limited to personal information.

Meanwhile, China also regulates the transfer of “important data,” in addition to personal information. “Important data” subject to the regulation in China is defined as data closely related to national security, economic development, or social public interests.¹² Annex A of the Guidelines for Cross-Border Data Transfer Security Assessment (Draft) shows examples of important data in 27 sectors, including “oil and natural gas” and “communications.” These examples include an extensive range of items, from shipping slip data of post corporations to sampling information of mass-produced processed food products. Moreover, the law includes a bucket clause, which provides that important data is not limited to said 27 sectors but could also be data in other sectors. There is a concern that the transparency of the application of the law may not always be maintained.

The proposed Cybersecurity Law in Viet Nam regulates the transfer of “personal information and important data.” This law also requires caution as an extensive range of data and personal information are regulated as “important data” in the same manner as the Chinese law.

C. Regulated Entities

Under the regulations in the EU, Indonesia, and Russia, persons managing personal information are subject to regulation.

Meanwhile, China regulates a wide scope of entities from the viewpoint of national security. The Chinese Cybersecurity Law includes persons managing personal information as well as operators of critical information infrastructures, such as communications, financial, and medical institutions, in the scope of regulation. In addition, the draft Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data adds network operators in the scope as well. However, the definition of “network operator” is not clearly stated. Such ambiguity raises a concern as to what kind of business operators are included into the scope.

⁹ Article 1, paragraph 3 of the GDPR

¹⁰ Article 44 of the GDPR

¹¹ Article 1 of the Cybersecurity Law.

¹² Article 18 of the draft Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data. See also Article 3.5 of the Guidelines for Cross-Border Data Transfer Security Assessment (Draft) (draft for public comment dated August 25, 2017).

The proposed Cybersecurity Law of Viet Nam also includes persons managing personal information and managers, providers, and users of cyberspace in the scope of regulation. Attention needs to be paid to whether the transparency of the scope of regulated entities will be maintained.

D. Other Regulations

Generally, cross-border data transfer is allowed when one of the following grounds is met: [1] the individual concerned consents to the data transfer, or [2] the requirements of safety management measures are fulfilled. The latter case (requirements of safety management measures) is judged based on either the legal system of the transfer destination state or the attributes, etc. of the entity receiving the data. In addition to the above conditions, the Russian authority requires prior notification of cross-border data transfers scheduled, while the Indonesian authority imposes a reporting obligation. In addition to notification and reporting obligations, the Chinese Cybersecurity Law also imposes on network operators the obligation to provide technical support and cooperation for national security and crime investigations conducted by the national security authorities.

(2) Data Localization Obligation

The regulations in China,¹³ Viet Nam,¹⁴ Indonesia,¹⁵ and Russia¹⁶ include provisions concerning the obligation to store data within the territory of the nation (localization obligation), while the EU GDPR does not have such a provision. If a less advantageous treatment is accorded to foreign companies compared to domestic companies due to the localization requirement, it may constitute a violation against the principle of national treatment. In the course of formation of international rules on e-commerce, Japan has attached importance to securing the free transfer of information in principle and advocated for the observation of the non-discrimination principle, which is the fundamental principle of the WTO. In the context of data localization obligations, it is also necessary to pay close attention to avoid excessive localization obligations from being introduced.

A. Scope of Subject Information

As with cross-border data transfer, Russia limits the scope of data localization obligation to personal information. Meanwhile, China, Indonesia, and Viet Nam also include certain data that is important to the nation in the scope of the data localization obligation, in addition to personal information.

B. Regulated Entities

While Russia regulates persons managing personal information, China, Indonesia, and Viet Nam regulate system providers managing important data. However, the scope of such system providers differs among countries: such providers are referred to as “operators of important information infrastructures” (China), “cyberspace managers, etc.” (Viet Nam), and “electronic system providers for public services” (Indonesia). However, none of the scopes of these terms is clearly defined.

C. Other Regulations

China, Indonesia, and Russia impose data localization obligations on both domestic and foreign companies. On the other hand, the proposed Cybersecurity Law of Viet Nam limits the obligation to foreign companies. Attention should be paid to what the regulation under the final version of this

¹³ Article 37 of the Cybersecurity Law.

¹⁴ Article 34, paragraph 4, Article 48, paragraph 4, and Article 51, paragraph 2 of the Cybersecurity Law.

¹⁵ Article 17, paragraph 2 of the Government Regulation No. 82 of 2012 on the Electronic System and Transactions (Republic of Indonesia)

¹⁶ Article 18, paragraph 5 of the Russian Federal Law on Personal Data.

law will look like.