Newsletter

ATSUMI & SAKAI
TOKYO | NEW YORK | LONDON | FRANKFURT
www.aplawjapan.com/en

October 2021
No.VTM_031

Explanation of the key points regarding handling of personal information between Japan and Vietnam

- Dealing with cross-border transfer of personal information after the amendment of Japan's Act on the Protection of Personal Information and Vietnam's data localization regulations -

TABLE OF CONTENTS

Key Points of this Article

- With Japan's amended Act on the Protection of Personal Information scheduled to come into effect, it will be necessary to ensure the provision of information related to relevant laws and that a “System Conforming to Standards” (defined below) is in place when transferring personal information to Vietnam.
- In Vietnam, a decree that sets general rules for the protection of personal information is scheduled to come into effect before end of 2021.
- It is anticipated that laws and regulations, as well as standard practices, will continue to be established with regard to data localization and cross-border transfers of data going forward.

1 How Japan’s amended Act on the Protection of Personal Information applies to the transfer of personal information to Vietnam

Japan’s amended Act on the Protection of Personal Information (hereinafter referred to as the "amended Act") is scheduled to go into effect on April 1, 2022. While the revisions to the Act are wide-ranging, it is necessary to take measures for the improvement of information provided to the data subject when transferring data from Japan to a country which is not recognized by the Personal Information Protection Commission (PPC) of Japan as having a system for the protection of personal information considered to be at a level equivalent to that of Japan for the protection of the rights and interests of individuals. The intention behind these regulations is to ensure the protection of personal data by requiring measures stricter than those in Japan. This is because, while it is sufficient to utilize “opt-out provisions” when transferring personal data to third parties who are also in Japan, in the case of foreign countries, there is no guarantee that personal data will be protected at the same standard as in Japan.

As Vietnam does not fall under the exception described above, below we explain the key points to keep in mind when transferring personal data from Japan to Vietnam under the amended Act.

(1) When the cross-border transfer of data to Vietnam is permitted

Under the amended Act, the provision of personal data to a third party in a foreign country by a business operator handling personal information is permitted when either (1) the consent of the data subject is obtained in advance, approving the provision of personal data to a third party in a foreign country; or (2) the recipient of the personal data has developed a system conforming to the standards provided in the revised Personal Information Protection Commission Regulations which will come into effect at the same time as the amended Act (hereinafter referred to as the "Revised Regulations") (hereinafter “System Conforming to Standards”), and necessary measures have been taken to ensure the continued implementation of appropriate measures by the recipient (Article 24, paragraph 1 of the amended Act).

“Third party in a foreign country” referred to here means a person other than a business operator handling personal information who provides personal data, and the data subject who can be identified by such personal data, and includes not only business partners but also foreign governments and current subsidiaries, etc.

Below we discuss a number of scenarios, the applicable laws, and the way to handle them.

(2) When transferring data from Japan to Vietnam based upon consent of the data subject

Under the amended Act, when a company causes personal data to be transferred from Japan to Vietnam based upon the consent of the data subject, it is required to provide the relevant data subject, in advance, with information on the system for protection of personal information in the relevant foreign country, the measures taken for the protection of personal information by such third party, and any other information that may be helpful to such data subject (Article 24, paragraph 2 of the amended Act). The specific details are set forth in the Revised Regulations. It will be necessary to provide (a) the name of the relevant foreign country, (b) information obtained in a reasonable and appropriate manner on the system for protection of personal information in the relevant foreign country, and (c) information on measures taken by such third party for the protection of personal information, etc. (Article 11-3, paragraph 2 of the Revised Regulations).

(a) Name of the relevant foreign country

It is sufficient to indicate the name of the foreign country in which the personal data recipient is located, and it is not necessarily required to state the official name of such country. However, the name provided must be one from which the data subject can reasonably be expected to recognize the location to which his or her own personal data has been transferred.

(b) Information regarding the personal information protection system in the relevant foreign country

Under the guidelines to the amended Act, it is necessary to consider points (i) through (iv) below.

(i) Existence of a system for the protection of personal information in the destination foreign country
(ii) Existence of information that can serve as an indicator of the system for the protection of personal information in the destination foreign country
(iii) Absence of operator's obligations or rights of the data subject corresponding to those in the eight principles of the OECD Privacy Guidelines[1]
(iv) Existence of other systems that may have a material impact on the rights of the data subject

With regard to (i) above, as discussed below in "Overview of Vietnam's legislation relating to protection of personal information and relevant trends," a general law relating to the protection of personal information has yet to be established in Vietnam. Also, with regard to (ii) above, as Vietnam is not a member of APEC's CBPR (Cross-Border Privacy Rules) system, it is expected that transfers of data will be carried out on the assumption that no information exists which may serve as an indicator of the system for the protection of personal information in Vietnam. With regard to (iii) above, please see the explanations in 2.(2)(a). With regard to (iv) above, it should be noted that there are laws and regulations that have provisions related to government access and data localization which fall under "systems that may have a material impact on the rights of the data subject."

(c) Information regarding measures for the protection of personal information taken by a third party

This information must be information which enables the data subject to be reasonably aware of the essential differences between the measures taken by a third party in a foreign country for the protection of personal information and the measures under the laws of Japan (specifically, the Act on the Protection of Personal Information) which are required for business operators obtaining personal information regarding the handling of personal data. In the case of Vietnam, this is understood to mean that information must be provided to the data subject so that the data subject can reasonably recognize which of the measures corresponding to the eight principles of the OECD Privacy Guidelines have not been sufficiently carried out.

(3) When personal data is transferred to Vietnam without obtaining the consent of the data subject, but based upon establishment of a System Conforming to Standards

Even in cases where the consent of the data subject has not been obtained, personal data may be transferred if (a) the recipient of the personal data has established a System Conforming to Standards as set forth in the Revised Regulations, and (b) necessary measures have been taken to ensure the continuous implementation of appropriate measures by the recipient.

(a) System Conforming to Standards

The requirements for the establishment of a System Conforming to Standards are as follows (Article 11-2 of the Revised Regulations).

[1] The eight principles defined in the Guidelines for the Protection of Privacy and the International Distribution of Personal Data adopted in 1980 by the Organization for Economic Co-operation and Development (OECD)

(i)	The implementation of measures consistent with the purpose of the provisions in Chapter 4, Section 1 of the amended Act is ensured between the business operator handling personal information and the recipient to whom personal data is provided, in an appropriate and reasonable manner, with respect to the handling of such personal data by the recipient of such data.
(ii)	The person receiving the personal data has been certified based on an international framework concerning the handling of personal information.

With regard to (i), this might be, for example, a service agreement concluded with a business partner which includes provisions covering the handling of personal information. Another example would be, in the case of a corporate group, creating internal rules or a privacy policy for such group. With regard to (ii), certification under APEC's CBPR system could be considered an applicable event.

(b) "Measures necessary to ensure the continuous implementation of appropriate measures by the third party in a foreign country"

Details are as follows (Article 11-4, paragraph 1 of the Revised Regulations).

(i)	Regularly checking, in an appropriate and reasonable manner, the status of implementation of the appropriate measures by the relevant third party as well as whether there exists any system in the relevant foreign country which may affect the implementation of such appropriate measures, and the details of said foreign country's system.
(ii)	In the event of any hindrance to the implementation of appropriate measures by the third party, in addition to the party providing the personal data taking necessary and appropriate measures, if the third party has difficulty in ensuring the continuous implementation of the appropriate measures, provider shall suspend the provision of the personal data to such third party.

The law requires that if the data subject requests, the above information must be provided to the data subject (Article 24, paragraph 3 of the amended Act).

In light of the foregoing, in the case of transferring personal data to Vietnam based upon establishment of a System Conforming to Standards, it is necessary to develop and manage regulations that comply with updates to the Vietnamese legal system and that satisfy the requirements of Japan's laws and regulations relating to protection of personal data set forth in agreements with the recipients of personal data transfers.

2 Overview of Vietnam's legislation relating to protection of personal information and relevant trends

(1) Overview of the legislation relating to protection of personal information

In Vietnam, there are no laws or regulations equivalent to the Personal Information Protection Act of Japan, which comprehensively provides for the protection of personal information. Instead, what protection there is comes from the Civil Code, as well as the many laws and regulations which have been established for each individual sector, and as a consequence, the relevant definitions and regulations are not unified.

It was under these circumstances that the draft Decree on Personal Data Protection was published in February 2021. As it was the first regulation to provide comprehensive provisions relating to the protection of personal data, it has been the subject of much attention. Originally, the Draft Decree on Personal Data Protection was scheduled to be promulgated and entered into force in 2021, but at present, it has not yet been promulgated.

Further, as a recent trend in Vietnam, in a movement similar to movements in other countries, draft decrees to revise the regulations concerning data localization of personal information and regulations on cross-border transfer have been proposed, with the goal of protecting the personal information of the citizens of Vietnam. These regulations are also included in the information provided to the information subject at the time of information transfer from Japan, as described in 1 above. The key points are discussed below.

(2) Overview of the Draft Decree on Personal Data Protection

(a) Relationship with the eight principles of the OECD

As mentioned above, when transferring personal data from Japan to Vietnam based on the data subject's consent, it is necessary to provide information on the absence of the operator's obligations or rights of the data subject corresponding to the eight principles of the OECD.

As Vietnam is not an OECD member, it is not required to reflect the eight principles of the OECD in its domestic laws and regulations. However, although the Draft Decree on Personal Data Protection does provide for principles equivalent to the eight principles of the OECD, provisions surrounding the (1) collection limitation principle, (6) openness principle, and (8) accountability principle seems to be insufficient.

Eight principles of the OECD	
① Collection Limitation Principle	⑤ Security Safeguards Principle
② Data Quality Principle	⑥ Openness Principle
③ Purpose Specification Principle	⑦ Individual Participation Principle
④ Use Limitation Principle	⑧ Accountability Principle

(b) Definition and classifications of personal data

"Personal data" is defined as "data concerning an individual or data relating to the identification or possible identification of an individual" (Article 2, paragraph 1 of the Draft Decree on Personal Data Protection). As the following table shows, personal data is divided into basic personal data and sensitive personal data (Article 2, paragraphs 2 and 3 of the Draft Decree on Personal Data Protection).

In principle, registration with the Personal Data Protection Committee of Vietnam is required in order to process information falling under sensitive personal data (Article 20, paragraph 1 of the Draft Decree on Personal Data Protection).

Basic personal data (Article 2, paragraph 2 of the Draft Decree on Personal Data Protection)	**Sensitive personal data (Article 2, paragraph 3 of the Draft Decree on Personal Data Protection)**
(i) Family name, middle name, first name, alias (if any) (ii) Date of birth, date of death, date of disappearance (iii) Blood type, gender (iv) Place of birth, place of registration of place of birth, registered address, current address, hometown, contact details, email address (v) Academic background (vi) Ethnicity (vii) Nationality (viii) Telephone number (ix) ID number, passport number, identification card number, driver's license number, license plate number, individual taxpayer number, social insurance number (x) Marital status (xi) Data reflecting activities or history of activities in cyberspace	(i) Political and religious views (ii) Health condition (physical and mental) (iii) Hereditary or genetic characteristics (iv) Biometric data (v) Sexual status (vi) Sexual life and orientation (vii) Criminal history and criminal conduct (viii) Personal financial data (bank accounts, credit cards, payment methods, financial status, credit history, income level, etc.) (ix) Location information (x) Social relationships (xi) Other individual personal data that require legal safeguards

(c) Obtaining consent when processing personal data

When "processing" personal data, unless such processing falls under grounds for exclusion stipulated by law, it is necessary in principle to obtain the data subject's voluntary consent after clearly indicating the type of data to be processed, the purpose of the processing, and the rights of the data subject, etc. (Article 8, paragraph 1 of the Draft Decree on Personal Data Protection). "Processing" includes any act that has an impact on the data, including collection, recording, analysis, retention, modification, disclosure, permitting access thereto, acquisition, retrieval, encryption, decryption, copying, forwarding, deletion, and removal (Article 2, paragraph 6 of the Draft Decree on Personal Data Protection).

A data subject's consent must be in a written form that can be printed or copied, and silence or non-response from the data subject is not considered consent. Further, a data subject is permitted to attach conditions to his or her consent or provide only partial consent. Additionally, the data subject may withdraw his or her consent at any time (Article 8, paragraphs 2, 3, 4, and 7 of the Draft Decree on Personal Data Protection).

(d) Penalties for violations

Violations of the regulations concerning personal data protection apply to all domestic and foreign organizations, corporations, and individuals conducting business in Vietnam (Article 4, paragraph 2 of the Draft Decree on Personal Data Protection), and, in the event of a violation, an administrative penalty corresponding to the severity of the violation will apply.

Specifically, violations and penalties are divided into three levels as follows (Article 22, paragraphs 1, 2, 3, and 4 of the Draft Decree on Personal Data Protection). The Director of the Department of Cyber Security and Hi-tech Crime Prevention, which falls under the Ministry of Public Security, has the authority to impose penalties (Article 22, paragraph 6 of the Draft Decree on Personal Data Protection).

	Level 1	**Level 2**	**Level 3**
Major penalties	Fines of between VND 50,000,000 and VND 80,000,000	Fines of between VND 80,000,000 and VND 100,000,000 Additional penalties: Suspension of the processing of personal data from one to three months, or revocation of approval for cross-border transfer of sensitive personal data or personal data	Fine of no more than 5% of total revenue in Vietnam
Violations	• Violations concerning data disclosure • Violations concerning consent of data subject • Violations concerning access rights of data subject • Violations concerning data subject's right to receive notifications • Violations concerning processing of personal data without data subject's consent • Violations concerning data accuracy • Violations concerning retention and deletion of data	• Violations concerning the technical operations for data retention and the establishment of regulations • Violations concerning registration for processing sensitive data • Cross-border transfer of data • Two occurrences of a level 1 violation	Two occurrences of a level 2 violation

(3) **Regulatory trends in data localization and cross-border transfer of data**

The Cybersecurity Law is one of the current laws and regulations that provides for data localization. However, the law has yet to be put into practice due to delays in the promulgation of a decree that will provide the detailed regulations for its enforcement. Further, a draft decree (hereinafter "Draft Decree on Internet Services") to amend Decree No. 72/2013/ND-CP, amended by Decree No. 27/2018/ND-CP, on the management, provision, and use of internet services and online information mandates data localization by referring to the Cybersecurity Law.

The Draft Decree on Personal Data Protection provides for cross-border transfer of data. Each draft decree is discussed below.

(a) Draft Decree on Enforcement of the Cybersecurity Law

The Cybersecurity Law, which came into force in 2019, regulates activities to ensure social order and safety in cyberspace and to protect national security, and provides for the responsibilities of agencies, organizations, and individuals involved therein (Article 1 of the Cybersecurity Law).

According to the Cybersecurity Law, domestic and foreign corporations that provide services or value-added services on communication networks, the Internet, and cyberspace in Vietnam are subject to application of the regulations on data localization, and must, when collecting, utilizing, analyzing, or processing any of (1) data concerning the personal information of service users, (2) data concerning service users' relationships, or (3) data generated by service users in Vietnam, retain such data in Vietnam (Article 26, paragraph 3 of the Cybersecurity Law). Furthermore, the Cybersecurity Law provides that a foreign company that satisfies all of the above conditions bears an obligation to have a representative office or branch in Vietnam.

In addition to these kinds of regulations, the Cybersecurity Law also provides for the provision of information in response to written requests from authorities for the purpose of investigating violations of laws and regulations concerning cybersecurity (Article 26, paragraph 2, item (a) of the Cybersecurity Law; so-called "government access"). Due to these provisions, deep concerns were expressed both domestically and internationally before and after the law's establishment.

The draft decree, announced in 2019, which provides detailed regulations for the enforcement of the Cybersecurity Law, limits the scope of application even more than the Cybersecurity Law by restricting the obligations concerning data localization and the establishment of representative offices or branches to the following cases (Article 26, paragraph 1, item (c) of the Draft Decree Detailing the Cybersecurity Law).

(i) Failure to establish preventative or response measures despite having received a warning that the service violates laws and measures to correct the violation have not been taken;
(ii) Resistance to, interference with, or disregarding written requests from the Ministry of Public Security's Department of Cyber Security and Hi-tech Crime Prevention to cooperate in investigation of, and response to, violations of the law; or
(iii) Disabling of cybersecurity safeguards implemented by the cybersecurity protection task force.

(b) Draft Decree on Internet Services

The Ministry of Information and Communications published the Draft Decree on Internet Services for public comment in July 2021. Under the Draft Decree on Internet Services, amendments are planned in order to harmonize the provisions of the Cybersecurity Law with those on cross-border provision of information stipulated in Circular No. 38/2016/TT-BTTTT which is currently in effect.

According to the Draft Decree on Internet Services, "cross-border provision of information" refers to the provision of information by foreign organizations or individuals to users in Vietnam who use, access, or utilize websites, social networking, online applications, search services, or other similar forms of media (Article 1, paragraph 2 of the Draft Decree on Internet Services).

Also, if an entity that engages in cross-border provision of information leases a data server, etc. in Vietnam or has at least 100,000 monthly regular visitors to its website in Vietnam, that entity will be obligated to do the following. (Article 1, paragraph 17 of the Draft Decree on Internet Services).

(i) Notify the Ministry of Information and Communications of Vietnam (hereafter "MIC") of its contact information;
(ii) Prevent or remove any illegal information in accordance with the instructions of the MIC;
(iii) Implement a cooperation agreement with the Vietnamese media when citing information from the Vietnamese media as the information source;
(iv) Retain data and establish a representative office or branch in Vietnam in accordance with the provisions of the Cybersecurity Law and the detailed regulations for enforcement thereof;
(v) Establish a department in charge of handling any instructions or requests from competent authorities or users in Vietnam;
(vi) Respond to any requests from users in Vietnam within 24 hours of receiving such request;
(vii) Social networking providers must only allow accounts for which contact details have been submitted to the MIC to perform live streaming or participate in revenue-generating services of any kind;
(viii) Publish policies and procedures for user support; and
(ix) Comply with systems for regular and rush reporting.

As (iv) in the above list states, if an entity that engages in cross-border provision of information is subject to obligations relating to data localization and establishment of branches, etc. in accordance with the Cybersecurity Law and the detailed regulations for the enforcement thereof, that entity is required to comply with the obligations of the Cybersecurity Law.

If an entity that engages in cross-border provision of information from abroad breaches any of the above obligations, the MIC will not impose normal administrative penalties, such as a fine, on the entity that engages in the cross-border provision of information, but will instead employ preventative measures such as notifying such entity of the illegal content and instructing such entity to remove such content (Article 1, paragraph 17 of the Draft Decree on Internet Services). Specifically, an entity that engages in cross-border provision of information is required to respond to requests such as the following:

- In the case of live streaming, prevent or delete illegal content within 3 hours of receiving instructions from the MIC.
- In the case of social networks and websites, etc., for accounts or pages that have published illegal content five times or more in one month, lock such accounts, etc. for a period of 7-30 days within 24 hours of receiving instructions from the Ministry of Information and Communications.
- In the case of online applications, exclude or remove such applications from app stores within 24 hours of receiving instructions from the MIC.

If a cross-border information provider fails to employ response measures within the above time frames after receiving instructions from the MIC, the MIC can take measures against the illegal content and service, but specific details regarding what such measures entail have not been found.

(c) Draft Decree on Personal Data Protection

Under the Draft Decree on Personal Data Protection, in principle, the cross-border transfer of personal data of Vietnamese nationals is allowed if all of the following four requirements are satisfied (Article 21, paragraph 1 of the Draft Decree on Personal Data Protection).

(i) Consent of the data subject has been obtained;
(ii) The original data is retained in Vietnam;
(iii) There is documented evidence that the country, region, or specific area of such country or region to which the data will be transferred has regulations equivalent to or stricter than the Draft Decree on Personal Data Protection; and
(iv) Written consent has been obtained from the Personal Data Protection Committee of Vietnam

In particular, it is necessary to keep in mind that one of the requirements for cross-border transfer is the obligation to retain the original data in Vietnam.

3 Conclusion

In the field of personal information protection, legislation is rapidly developing around the world, and the protection of the data of a country's own citizens in the case of cross-border transfers of personal information is an important issue.

It is anticipated that it will take some time for practices in Vietnam to be established, due to the fact that, as explained above, the laws are still in the process of being developed. Therefore, when developing your business in Vietnam, it is important to get expert advice and pay attention to the legal and regulatory trends when establishing and operating an appropriate protection system for personal information.

Authors

Yumiko Fujikawa
Associate
E: yumiko.fujikawa@aplaw.jp

Yuri Suzuki
Partner
E: yuri.suzuki@aplaw.jp

Yuko Nihonmatsu
Partner
E: yuko.nihonmatsu@aplaw.jp

Yasuharu Miura
Of Counsel
E: yasuharu.miura@aplaw.jp

Natsuko Tomatsu
Associate
E: natsuko.tomatsu@aplaw.jp

Wataru Kamihigashi
Associate
E: wataru.kamihigashi@aplaw.jp

Minh Chau Dang*
Associate
*Not Registered as a Foreign Lawyer in Japan
E: minhchau.dang@aplaw.jp

Ciaran Rose*
Associate
*Not Registered as a Foreign Lawyer in Japan
E: ciaran.rose@aplaw.jp

Contacts

E-mail: aandsvietnam@aplaw.jp

If you would like to sign up for A&S Newsletters, please fill out the sign-up form.
Back issues of our newsletters are available here.

Atsumi & Sakai

www.aplawjapan.com/en/

Tokyo Office: Fukoku Seimei Bldg., 2-2-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011, Japan

New York Office: *Attorneys associated with the New York office will telework from Tokyo while observing the progress of the Novel Coronavirus infection. We will provide services for the time being by working from home and using web conferencing systems.*

London Office: 4th Floor, 50 Mark Lane, London EC3R 7QR, United Kingdom

Frankfurt Affiliate Office: OpernTurm (13F) Bockenheimer Landstraße 2-4, 60306 Frankfurt am Main, Germany