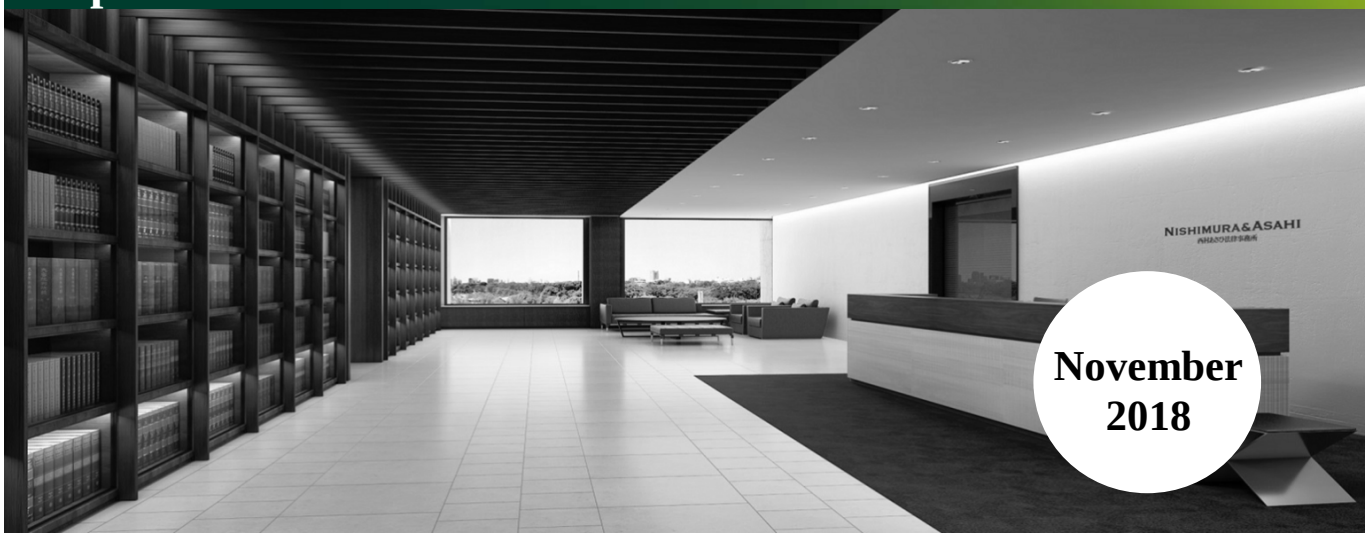
西村あさひ法律事務所

NISHIMURA & ASAHI

Corporate Newsletter



Announcement of Supplementary Rules Concerning the Handling of Personal Data Transferred from the EEA Based on an Adequacy Decision; and Practical Implementation at an Establishment in Japan

Noriya Ishikawa, Yuko Kawai, Yujin Suga, Yui Sugiyama

On August 24 of this year, the Personal Information Protection Commission (the "**PPC**") announced the "Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU Based on an Adequacy Decision" (the **"Supplementary Rules"**).[1] After the European Commission decides that Japan ensures an adequate level of protection of personal data (a so-called "adequacy decision") pursuant to Article 45 of the EU General Data Protection Regulation (the **"GDPR"**), these supplementary rules will be required to be complied with when a Japanese business operator handling personal information receives personal data transferred from the European Economic Area (EEA)[2] based on the adequacy decision.

In this newsletter, we provide an outline of the Supplementary Rules and briefly explain what should be implemented at an establishment in Japan going forward. The "results of public comments regarding the 'Guidelines on the Act on the Protection of Personal Information (volume on handling of personal data transferred from the EU based on an adequacy decision) (proposal)' "[3] that were announced on the same day as the Supplementary Rules are simply hereinafter referred

---

1 "Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU Based on an Adequacy Decision" by the Personal Information Protection Commission https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf.

2 Member States of the EU as well as Iceland, Liechtenstein, and Norway.

3 "Requests for public comments" by the Personal Information Protection Commission https://www.ppc.go.jp/news/public-comment/.

to as the **"Public Comment Results"**.

I. Outline of the Supplementary Rules

1. Position of the Supplementary Rules

The Supplementary Rules are binding on business operators handling personal information that receive personal data transferred from the EEA based on the adequacy decision and thus must be complied with. As these rules are legally binding, any rights and obligations under these rules are enforceable by the PPC in the same way as the provisions of the Act on the Protection of Personal Information (the **"APPI"**). In case of infringement of the rights and obligations provided under these rules, data subjects can also obtain redress at courts in the same way as with respect to the provisions of the APPI.

As regards enforcement by the PPC as mentioned above, in case a business operator handling personal information does not comply with one or more obligations under the Supplementary Rules, the PPC has the authority to take measures pursuant to Article 42 of the APPI.[4] Failure by a business operator handling personal information to take measures in line with a recommendation received pursuant to Article 42, paragraph (1) of the APPI, without legitimate grounds, is considered a "serious infringement of an imminent nature of an individual's rights and interests" within the meaning of Article 42, paragraph (2) of the APPI.

2. Issues concerning the applicable scope of the Supplementary Rules

The Supplementary Rules apply to the handling of personal data transferred from the EEA based on the adequacy decision. The Public Comment Results clarify the following points:

(i) Even after Japan receives the adequacy decision, personal data can still be transferred from the EEA based on standard contractual clauses (SCCs), binding corporate rules (BCRs), or any derogation pursuant to 49 (1) of the GDPR, such as explicit consent;[5]

(ii) The Supplementary Rules do not apply to personal data transferred based on SCCs, BCRs, or such derogation;[6] and

(iii) Personal data duly transferred in other way before receiving the adequacy decision will not be subject to the

---

4 Article 42 of the APPI provides that the PPC may, when recognizing that there is a need to protect an individual's rights and interests in cases where a personal information handling business operator has violated some provisions of the APPI, recommend that the personal information handling business operator, etc. suspend the act of violating or take other necessary action to rectify the violation. The same Article further provides that the PPC may, when recognizing that a serious infringement of an individual's rights and interests is imminent in cases where a personal information handling business operator having received a recommendation did not take action in line with the recommendation without legitimate grounds, order the personal information handling business operator to take action in line with that recommendation.

5 Public Comment Results No. 45 and others.

6 Public Comment Results No. 11, No. 52, and others.

Supplementary Rules.[7]

Therefore, we understand that a company in Japan that already implemented its own method for receiving personal data transferred from the EEA, such as SCCs, BCRs, or others, may keep that method without taking any new measures for the Supplementary Rules.

3. Timing of the adequacy decision and the enforcement date of the Supplementary Rules

The enforcement date of the Supplementary Rules is the day on which the adequacy decision from the European Commission comes into effect. The specific timing is uncertain.

4. Outline of the Supplementary Rules

The Supplementary Rules are rules for Japanese business operators handling personal information to handle personal data transferred from the EEA based on the adequacy decision, which they need to comply with in addition to the APPI and the guidelines thereof. The details of the Supplementary Rules are described below (5 items):

(1) Special care-required personal information

"Special care-required personal information" in the APPI is defined as information containing descriptions, etc. requiring special care when being handled. "Special care-required personal information" is a notion comparable to "sensitive data" or "special categories of personal data" under the GDPR. It is personal information comprising a data subject's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions, etc. prescribed by a cabinet order as that which requires special care in its handling so as not to cause unfair discrimination, prejudice, or other disadvantages to the data subject (Article 2, paragraph (3) of the APPI).

The GDPR provides that the processing of special categories of personal data should be limited to the cases where a data subject has given explicit consent (Article 9, paragraph (2) of the GDPR). Specifically, the special categories cover personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

If comparing special care-required personal information under the APPI with special categories of personal data under the GDPR, the latter covers a wider range; accordingly, to fill a gap between the two and protect personal data transferred from the EEA, the Supplementary Rules require that "information concerning sex life, sexual orientation, or trade union" shall be handled in the same way as special care-required personal information under the APPI. To be more specific, a business operator handling personal information shall not acquire this

[7] Public Comment Results No. 17.

information, in principle, without the prior consent of the data subject (Article 17, paragraph (2) of the APPI) and shall not provide it to a third party by an opt-out procedure (Article 23, paragraph (2) of the same act).[8]

(2) Retained personal data

"Retained personal data" is defined as personal data that a business operator handling personal information has the authority to disclose, to correct, add to or delete, to discontinue its utilization, to erase, and to discontinue its provision to a third party, excluding data that is harmful to the public or other interests if its presence or absence is known and data that will be erased within a period of no longer than six months (Article 2, paragraph (7) of the APPI and Article 5 of the Cabinet Order to Enforce the Act on the Protection of Personal Information). Practically speaking, "retained personal data" under the APPI means personal data that is subject to an individual's request for disclosure, correction, addition, deletion, discontinuance of utilization, etc. According to the definition, "retained personal data" does not cover personal data that will be erased within a period of less than six months.

Meanwhile, under the GDPR, a right of access to (Article 15 of the GDPR), a right to rectification of (Article 16 of the same), a right to erasure of (Article 17 of the same), and a right to restriction of processing of (Article 18 of the same) personal data and other rights of a data subject are granted regardless of the retention period of personal data.

Therefore, under the Supplementary Rules, personal data that a business operator handling personal information receives from the EEA based on the adequacy decision shall be handled as "retained personal data" under Article 2, paragraph (7) of the APPI regardless of the period within which the data will be erased.

(3) Specifying a utilization purpose; restrictions due to a utilization purpose

If business operators handling personal information handle personal information beyond the necessary scope to achieve a utilization purpose specified pursuant to Article 15, paragraph (1) of the APPI, they must obtain the relevant data subject's consent in advance (Article 16, paragraph (1) of the same act). Further, when receiving personal data from a third party, business operators handling personal information must confirm matters such as the circumstances under which the said personal data was acquired by the third party, and record these matters pursuant to the rules of the PPC (Article 26, paragraphs (1) and (3) of the APPI).

Meanwhile, the GDPR provides that personal data shall not be further processed in a manner that is incompatible with the utilization purposes specified when acquiring the personal data, with limited exceptions such as the case where the processing is based on the relevant data subject's consent (Article 5, paragraph 1(b) and Article 6, paragraph (4) of the GDPR).

Consequently, the Supplementary Rules provide that in the case where a business operator handling personal

[8] Public Comment Results No. 76 and No. 78.

information receives personal data transferred from the EEA based on the adequacy decision, the circumstances regarding the acquisition of the said personal data, including the utilization purposes specified when the said personal data was transferred from the EEA, should be confirmed and recorded as prescribed by Article 26, paragraphs (1) and (3) of the APPI. Similarly, in the case where a business operator handling personal information receives from another business operator handling personal information personal data previously transferred from the EEA based on the adequacy decision, the circumstances regarding the acquisition of the said personal data, including the utilization purposes specified when the said personal data was transferred, should be confirmed and recorded as prescribed by Article 26, paragraphs (1) and (3) of the APPI. In any of the above-mentioned cases, the business operator handling personal information is required to specify the utilization purpose of the personal data, which was confirmed and recorded pursuant to Article 26, paragraphs (1) and (3) of the APPI, within the scope of the utilization purpose specified when the personal data was originally or subsequently received, and utilize that personal data within the said scope (Article 15, paragraph (1) and Article 16, paragraph (1) of the APPI). This will serve to protect the scope of the original utilization purpose specified when the personal data was acquired in the EEA.

However, it is important to note that the utilization purpose of personal data transferred from the EEA based on the adequacy decision can still be changed. According to the Public Comment Results, Article 15, paragraph (2) of the APPI (which specifies that the utilization purpose can be changed to the extent that the utilization purpose after the change is reasonably related to the original purpose) could apply if the utilization purpose is changed within the scope of the expected utilization purpose of personal information transferred based on the adequacy decision.[9]

What requires attention in practice is that it is construed that even in cases where obligations of confirmation or recording of the circumstances under which the personal data was acquired are not imposed under the APPI in Japan, it is necessary to specify and restrict the utilization purpose.[10] To be more specific, although confirmation or recording obligations are not imposed in the following cases, when personal data is transferred from the EEA, a utilization purpose must be specified, and that personal data is required to be utilized within the specified scope, which means that intragroup transfer of personal data will be affected.

(i) if personal data is transferred from a headquarters in the EEA to a branch or local office in Japan (confirmation or recording is not obligated under the laws of Japan if a transfer occurs within a single legal entity);[11]

(ii) if personal data is transferred from a business operator in the EEA to a business operator in Japan based on entrustment, business succession, or joint utilization (confirmation or recording is not obligated under

---

9 Public Comment Results No. 111, No. 112, and No. 113. The GDPR also provides that personal data can be utilized for another purpose if a "compatibility" test that ascertains whether the processing for another purpose is compatible with the purpose for which the personal data was initially collected is satisfied (Article 6, paragraph (4) of the GDPR).

10 Public Comment Results No. 95.

11 Public Comment Results No. 96 and No. 99.

the laws of Japan if a transfer is made based on these events).[12]

(4) Restriction on provision to a third party in a foreign country

According to Article 24 of the APPI, when providing personal data to a third party located outside Japan, a business operator handling personal information should obtain in advance a data subject's consent to the effect that the data subject approves the provision of the personal data to the third party in a foreign country except: (i) when the third party is in a country listed by the rules of the PPC as a foreign country possessing a personal information protection system recognized to have equivalent standards to those in Japan in regard to the protection of an individual's rights and interests, (ii) when the third party establishes a system conforming to the standards prescribed by Article 11-2 of the rules of the PPC as necessary for continuously taking measures equivalent to those that a business operator handling personal information must take, or (iii) in those cases set forth in each item of Article 23, paragraph (1) of the APPI.[13]

Meanwhile, according to Article 44 and the following provisions of the GDPR, personal data can only be transferred to a third country in the following situations: (i) transfer to a country that has received an adequacy decision, (ii) transfer in accordance with appropriate security measures, including BCRs and SCCs, or (iii) derogations in the specific circumstances, including if a data subject gives explicit consent to the transfer and if the transfer is necessary for the performance of a contract between a data subject and a controller. When obtaining the data subject's explicit consent, information on risks that might arise as a result of the transfer to a third country must be provided.

Based on these two regulations, the Supplementary Rules provide that when providing personal data transferred from the EU to outside Japan, a business operator handling personal information should obtain in advance a data subject's consent to the effect that the data subject approves the provision of the personal data to the third party in a foreign country after having provided information on the circumstances surrounding the transfer necessary for the data subject to make a decision on consent. It should be noted however that this rule does not apply to cases falling under (i) through (iii) above (as for (ii), only if a system is established based on a contract, other forms of binding agreements, or binding arrangements within a corporate group).

---

12 Public Comment Results No. 97, No. 98, No. 100, and No. 101.

13 Article 23, paragraph (1) of the APPI specifies that a personal information handling business operator may exceptionally provide personal data to a third party without obtaining a data subject's prior consent in the following cases.

(i) Cases based on laws and regulations.
(ii) Cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a data subject's consent.
(iii) Cases in which there is a special need to enhance public hygiene or promote the fostering of healthy children, and when it is difficult to obtain a data subject's consent.
(iv) Cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing tasks prescribed by laws and regulations, and when there is a possibility that obtaining a data subject's consent would interfere with the performance of those tasks.

Under the APPI, the provision of personal data to a branch or business office of a single legal entity in a foreign country is not considered provision to a "third party in a foreign country."[14] The details of the circumstances surrounding the transfer to be provided to a data subject should be determined on a case-by-case basis with a view to whether those are necessary for the data subject to make a decision on consent.[15] Further, "in advance" does not necessarily mean that a data subject's consent must be obtained in advance each time personal information is provided, and it is considered sufficient to obtain comprehensive consent when acquiring personal information.[16]

(5) Anonymously processed information

Under the APPI, when producing "anonymously processed information" as defined in Article 2, paragraph (9) of the same act, a business operator handling personal information must process personal information in accordance with the standards prescribed in each item of Article 19 of the rules of the PPC so as not to identify a specific individual or restore the personal information used for the production (Article 36, paragraph (1) of the same act). In addition, when having produced anonymously processed information, a business operator handling personal information must take measures necessary to prevent the leakage of information related to the processing method, etc. in accordance with the standards prescribed in Article 20 of the rules (Article 36, paragraph (2) of the same act).

Meanwhile, under the GDPR, "anonymous information" does not relate to an identifiable natural person and means information by which a natural person is no longer identifiable (recital (26) of the GDPR).

Under the Supplementary Rules, personal information transferred from the EEA based on the adequacy decision can only be considered anonymously processed information within the meaning of Article 2, paragraph (9) of the APPI if a business operator takes measures that make the de-identification of the individual irreversible by deleting information related to the processing method, etc.

II. Practical implementation at an establishment in Japan after Japan receives the adequacy decision

First, it is advisable for each establishment in Japan to decide its method(s) for transferring personal data from the EEA to Japan. If the establishment takes any methods specified under the GDPR (SCCs, BCRs, etc.) other than the adequacy decision, the Supplementary Rules do not apply to these methods; therefore, the establishment would not have to take any special actions in relation to the Supplementary Rules.

If an establishment in Japan transfers personal data from the EEA based on the adequacy decision, the Supplementary Rules apply to the transfer. In this case, the establishment should review its existing internal rules and operation

---

14 Public Comment Results No. 131.

15 Public Comment Results No. 135, No. 136, No. 137, No. 138, and No. 139.

16 Public Comment Results No. 136.

manuals regarding personal information, amend them as necessary, and raise employee awareness of the Supplementary Rules to ensure their compliance.

Considering that the Supplementary Rules provide specific rules different from those for other personal data, we recommend that such establishment newly set special provisions for such personal data by amending the internal rules and operation manuals.

Specifically, the following five matters are those that should be amended:

(i) the scope of data handled as "special care-required personal information" is to be expanded;

For example, establishing a provision such as "[i]f personal information transferred based on the adequacy decision includes information concerning sex life, sexual orientation, or trade union, that information should be handled as 'special care-required personal information.'" should be considered.

(ii) the scope of retained personal data is to be expanded;

For example, establishing a provision such as "[p]ersonal information transferred based on the adequacy decision should be handled as 'retained personal data' regardless of the period within which it will be erased." should be considered.

(iii) a rule should be established that the establishment specify and record the utilization purpose when receiving personal data, and utilize it within the scope of that purpose as a recipient of personal data;

(iv) a rule should be established that (if a transfer relies on the data subject's consent) when providing personal data to a third party in a foreign country and obtaining the data subject's consent, a sufficient explanation regarding the circumstances surrounding the transferee must be provided;

(v) if anonymously processed information is handled, a special provision is to be added that nobody can reverse the de-identification of an individual.

By way of example, the provision would be: "as for personal information transferred based on the adequacy decision, the information can be handled as 'anonymously processed information' only if nobody can reverse the de-identification of an individual by deleting 'information related to the processing method, etc.' "

Our firm has been supporting many foreign companies with establishment(s) in Japan, including compliance with the APPI at those establishments. Please feel free to contact us by using a contact form.

Noriya Ishikawa
Partner
E-mail: n_ishikawa@jurists.co.jp

Noriya Ishikawa specializes in corporate law, M&A, intellectual property, and data protection laws and regulations. He handles M&A transactions in the EU, IP/IT-related matters and matters relating to the Japanese Personal Information Protection Act and the GDPR. He also has experience in IP disputes such as patent infringement litigation and trade secret misappropriation litigation. He was admitted to practice in Japan in 2006, as well as in New York in 2017 after graduating from University of Virginia School of Law (LL.M.) in 2015. He also mastered LL.M. of Munich Intellectual Property Law Center in 2016.

Yuko Kawai
Attorney-at-Law
E-mail: y_kawai@jurists.co.jp

Yuko Kawai is a senior associate at Nishimura & Asahi and advises numerous multinational companies on various matters, including the handling of personal information, data protection and data transfer, as well as cross-border transactions such as mergers and acquisitions, joint ventures, licenses, etc. She was admitted to practice in Japan in 2006, as well as in New York in 2014 after graduating from Columbia Law School (LL.M.) in 2013. She is also a member of the Association of Law and Information Systems of Japan.

Yujin Suga
Attorney-at-Law
E-mail: y_suga@jurists.co.jp

Yujin Suga is a senior associate at Nishimura & Asahi, advising on data protection, regulatory affairs and dispute resolution. He was admitted to practice in Japan in 2009, in France in 2017, and in New York in 2018. He graduated from Columbia Law School in 2016 (LL.M.), and from Université Panthéon-Assas (Paris II) in 2017 (LL.M. de droit français, européen et international des affaires). He is fluent in both English and French.

Yui Sugiyama
Attorney-at-Law
E-mail: yu_sugiyama@jurists.co.jp

Yui Sugiyama is an associate at Nishimura & Asahi, specializing in data protection laws and regulations, corporation law, Financial Instruments and Exchange Act and labor law. She was admitted in Japan in 2017 after graduating the University of Tokyo in 2016.