Guidelines on the Act on the Protection of Personal Information

(Version for Provision to Third Parties in Foreign Countries)

NOTICE

*This translation has not yet been proofread or corrected by a native English speaker or legal translation expert; this translation may be revised in the future.

*Only the original Japanese text has a legal effect, and the translations are to be used solely as reference materials to aid in the understanding of Japanese Guidelines.

1. Positioning of the Guideline

2. General Remarks

   2-1 Consent From the Person to the Effect that They Approve of Provision of Personal Data to Third Parties in Foreign Countries

   2-2 Third Party in a Foreign Country

3. Foreign Countries That Have a Policy on the Protection of Personal Information Recognized to be of the Same Standard as Japan When Protecting the Rights and Interests of Individuals

4. Standard for a System Necessary for Continuously Taking Measures That Correspond to Measures That Should be Taken by Business Operators Handling Personal Information

   4-1 Proper and Reasonable Methods (Related to Item 1 of Article 16 of the Rules)

   4-2 Measures Conforming to the Purport of Stipulations Under Section 2, Chapter 4 of the Act (Related to Item 1 of Article 16 of the Rules)

      4-2-1 Specifying a Utilization Purpose (Measures Conforming to the Purport of Article 17 of the Act)

      4-2-2 Restriction due to Utilization Purpose (Measures Conforming to the Purport of
<table>
<thead>
<tr>
<th>Article Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-2-3</td>
<td>Prohibition of Improper Use (Measures Conforming to the Purport of Article 19 of the Act)</td>
</tr>
<tr>
<td>4-2-4</td>
<td>Proper Acquisition (Measures Conforming to the Purport of Article 20 of the Act)</td>
</tr>
<tr>
<td>4-2-5</td>
<td>Notification etc. of a Utilization Purpose when Acquiring (Measures Conforming to the Purport of Article 21 of the Act)</td>
</tr>
<tr>
<td>4-2-6</td>
<td>Assurance etc. about the Accuracy of Data Contents (Measures Conforming to the Purport of Article 22 of the Act)</td>
</tr>
<tr>
<td>4-2-7</td>
<td>Security Control Measures (Measures Conforming to the Purport of Article 23 of the Act)</td>
</tr>
<tr>
<td>4-2-8</td>
<td>Supervision of Employees (Measures Conforming to the Purport of Article 24 of the Act)</td>
</tr>
<tr>
<td>4-2-9</td>
<td>Supervision of Trustees (Measures Conforming to the Purport of Article 25 of the Act)</td>
</tr>
<tr>
<td>4-2-10</td>
<td>Report on Leakage etc. (Measures Conforming to the Purport of Article 26 of the Act)</td>
</tr>
<tr>
<td>4-2-11</td>
<td>Restriction on Third Party Provision (Measures Conforming to the Purport of Article 27 of the Act)</td>
</tr>
<tr>
<td>4-2-12</td>
<td>Restriction on Provision to a Third Party in a Foreign Country (Measures Conforming to the Purport of Article 28 of the Act)</td>
</tr>
<tr>
<td>4-2-13</td>
<td>Public Disclosure etc. on Matters relating to Retained Personal Data (Measures Conforming to the Purport of Article 32 of the Act)</td>
</tr>
<tr>
<td>4-2-14</td>
<td>Disclosure (Measures Conforming to the Purport of Article 33 of the Act)</td>
</tr>
<tr>
<td>4-2-15</td>
<td>Correction etc. (Measures Conforming to the Purport of Article 34 of the Act)</td>
</tr>
<tr>
<td>4-2-16</td>
<td>Utilization Cease etc. (Measures Conforming to the Purport of Article 35 of the Act)</td>
</tr>
<tr>
<td>4-2-17</td>
<td>Explanation of Reasons (Measures Conforming to the Purport of Article 36 of the Act)</td>
</tr>
<tr>
<td>4-2-18</td>
<td>Procedures for Response to Request for Disclosure etc. (Measures Conforming to the Purport of Article 37 of the Act)</td>
</tr>
</tbody>
</table>
4-2-19 Charges (Measures Conforming to the Purport of Article 38 of the Act) 34

4-2-20 Processing of Complaints by Entities Handling Personal Information (Measures Conforming to the Purport of Article 40 of the Act) 35

4-3 That an Entity to be Provided with Personal Data Is Certified Based on an International Framework Pertaining to the Handling of Personal Information (Related to Item 2 of Article 16 of the Rules) 36

5. Provision of Information at the Time of Obtaining Consent 36

5-1 Method of Providing Information (Related to Article 17(1) of the Rules) 37

5-2 Information That Should be Provided (Related to Article 17(2) of the Rules) 37

5-3 Handling of Cases in Which Destination of Transfer Cannot Be Specified at the Time of Acquiring Consent (Related to Article 17(3) and (4) of the Rules) 42

5-3-1 Cases in Which a Foreign Country Where a Third Party Who is the Recipient Cannot be Specified (Related to Article 17(3) of the Rules) 42

5-3-2 Cases in Which Information Related to Measures for the Protection of Personal Information Taken by a Third Party, Who is the Recipient, Cannot be Provided (Related to Article 17(4) of the Rules) 44

6 Measures to be Taken In Cases In Which Personal Data Has Been Provided to Those That Have Prepared a System Necessary for Continuously Taking Measures That Correspond to Measures That Should be Taken by Business Operators Handling Personal Information 45

6-1 Measures that are Necessary for Ensuring the Continuous Implementation of Corresponding Measure (Related to Article 18(1) of the Rules) 46

6-2 Provision of Information Related to Measures that are Necessary for Ensuring the Continuous Implementation of Corresponding Measure (Related to Article 18(2) and (3) of the Rules) 49

6-2-1 Method of Providing Information (Related to Article 18(2) of the Rules) 49

6-2-2 Information That Should be Provided (Related to Article 18(3) of the Rules) 49

6-2-3 Notification or the Like for At the Time of Decision to the Effect of Not Providing Information (Related to Article 18(4) and (5) of the Rules) 54
1. Positioning of the Guideline

In order to support the activities for assurance of proper handling of personal information by business operators and to have measures taken by the business operators by the said support be properly and efficiently executed, the Personal Information Protection Commission has defined the “Guideline on the Act on the Protection of Personal Information (General Rule)” (Personal Information Protection Commission Notice No. 6 of 2016; hereinafter referred to as the “General Rule Guideline”) as a specific guide based on Articles 4, 9, and 128 of the Act on the Protection of Personal Information (Law No. 57 of 2003; hereinafter referred to as the “Act”). However, in view of ease of understanding and unification by specialization in the portions on the provision of personal data to third parties in foreign countries among the duties of business operators defined by the Act, this guideline is defined separately from the General Rule Guideline.

Article 23 of the Act before amendment by the act (Law No. 65 of 2015) (hereinafter referred to as the “2015 Amendment Act”) that amends portions of the Act on the Protection of Personal Information and the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures defined rules on the provision of personal data to third parties but did not distinguish between third parties in Japan and foreign countries. However, with the globalization of economic and social activities as well as the advancement of information communication technologies, the distribution of data that includes personal information across borders has increased, and due to an increase in the necessity for an establishment of certain regulations on the transferring of personal data to foreign countries and in order to achieve consistency with international frameworks on the protection of personal information, new stipulations on the provision of personal data to third parties in foreign countries under Article 24 of the Act after amendment by the 2015 Amendment Act.

Based on the deliberations in the Diet on the 2015 Amendment Act, it had been deemed that the said stipulations do not impose new restrictions on business operators but need to ratify the handling of personal information properly performed by the business operators.

In addition, based on an additional resolution in a committee of the House of Representatives of the Diet (May 20, 2015) and an additional resolution in a committee of the House of Councillors of the Diet (August 27, 2015), it has been deemed that it is necessary to achieve protection of personal information overseas while setting realistic restrictions so as not to
unfairly hinder the transfer of personal information across the border.

Furthermore, as it becomes more common to entrust work overseas and business models become more complex, opening up opportunities to transfer personal information across the border, risks that are involved in the transfer of personal data across the border change. In view of response to such changes in risk, enhancement of provision of information to the person on the transfer of their personal data across the border is required by the act (Law No. 44 of 2020) (hereinafter referred to as the "2020 Amendment Act") that amends portions of the Act on the Protection of Personal Information.

In this guideline, the approach and specific examples for the provision of personal data to third parties in foreign countries will be described.

Regarding matters that have been noted as "shall" and "shall not" in this guideline, not observing these may be determined as a violation of the laws. Meanwhile, regarding the matter that has been noted as "shall endeavor to", "preferred", and the like, although not observing these will not be immediately determined as a violation of the laws, it is preferred that these are observed as much as possible in accordance with the characteristics and scale of business operators based on the purpose of the laws.

Note that the terminologies used in this guideline accords with the terminologies used in the General Rule Guideline unless otherwise specified.

2. General Remarks

Cases in which personal data is provided to third parties in foreign countries, a business operator handling personal information is required to obtain in advance "consent of the person to the effect that they approve of provision of personal data to third parties in foreign countries" unless the case applies to the following (1) to (3) in accordance with Article 28(1) of the Act.

1. Cases in which the said third parties are in countries that are defined in the Enforcement Rules for the Act on the Protection of Personal Information (Personal Information Protection Commission Rules No. 3 of 2016; hereinafter referred to as the "Rules") as countries that have a personal information protection policy that is recognized to be of the same standard as Japan (*1)
2. Cases in which the said third parties have prepared a system that meets the standard defined by the Rules as a system that is necessary for continuously taking measures that correspond to measures that should be taken by business operators handling personal information (*2)

3. Cases in which the case applies to any of the following ① to ⑦ (related to each item in Article 27(1) of the Act)

① Cases in which the provision of personal data is based on laws and regulations (*3) (related to Paragraph 1)

② Cases in which there is a risk of violation of a specific right or interest, such as the life, body, or property, of an individual (including corporations), in which the provision of personal data is necessary for the protection of the life, body, or property of an individual, and in which it is difficult to obtain the consent of the person (related to Paragraph 2) (*4)

③ Cases in which the provision of personal data is especially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person (related to Paragraph 3)

④ Cases in which a national institution or the like need to cooperate with a private enterprise or the like when executing affairs prescribed by laws and regulations (*3) and in which the private enterprise or the like obtaining the consent of the person for providing personal data to the national institutions or the like is likely to impede the execution of the affairs concerned (related to Paragraph 4)

⑤ Cases in which an academic research institute provides personal data and in which the said provision of personal data is necessary for the public disclosure of academic research results or for professors (excluding cases in which the rights and interests of an individual is unfairly violated) (related to Paragraph 5)

⑥ Cases in which an academic research institute or the like provides personal data and provide the said personal data to a third party (regardless of whether they are an academic research institute or the like) performing academic research in cooperation with the said academic research institute or the like (including cases in which a part of the purpose of providing the said personal data and excluding cases in which there is a risk of unfairly violating the rights or interests of an individual) (related to Paragraph 6)

⑦ Cases in which an academic research institute or the like is provided with personal data and cases in which the said academic research institute or the like needs to handle the said personal data for academic research purposes (including cases in which a part of the purpose of providing the said personal data and excluding cases in which there is a risk of unfairly violating the rights or interests of an individual) (related to Paragraph 7)
(*1) The countries defined in the Rules refer to countries that are defined in the Personal Information Protection Commission Notice No. 1 of 2019. For details, refer to 3 (Foreign Countries That Have a Policy on the Protection of Personal Information Recognized to be of the Same Standard as Japan When Protecting the Rights and Interests of Individuals).

(*2) For details on the standard for a system necessary for continuously taking measures that correspond to measures that should be taken by business operators handling personal information, refer to 4 (Standard Necessary for Continuously Taking Measures That Correspond to Measures That Should be Taken by Business Operators Handling Personal Information). Cases in which personal data is provided to a third party in a foreign country on the grounds that the said third party in a foreign country has prepared a system that meets the said standard, based on Article 28(3) of the Act, a business operator handling personal information is required to take measures that are necessary for ensuring the continuous implementation of corresponding measures by the said third party in a foreign country and provide the person with information related to the said necessary measures in accordance with the said person's request. For details, refer to 6 (Measures to be Taken In Cases In Which Personal Data Has Been Provided to Those That Have Prepared a System Necessary for Continuously Taking Measures That Correspond to Measures That Should be Taken by Business Operators Handling Personal Information).

(*3) These "laws and regulations" do not include the laws and regulations of foreign countries. The same applies to other items of this guideline.

(*4) For example, when an insured event occurs to a policyholder of an overseas travel insurance at an overseas remote location and an urgent response is necessary, cases in which information is provided to local claim agents hired by the insurer are conceivable. In the case of the above (1), a country that the said third party is located does not correspond to a "foreign country" in Article 28(1) of the Act. In addition, in the case of the above (2), the said third party does not correspond to a "third party" in Article 28(1) of the Act. Accordingly, in these cases, Article 28(1) does not apply. Therefore, a business operator handling personal information does not need to obtain "consent of the person to the effect that they approve of provision of personal data to third parties in foreign countries" when providing personal data to the said third person.

However, the provision of personal data to the said third person needs to be performed by any of the following (a) to (e) methods stipulated by Article 27 of the Act.

(a) Method of provision based on the consent of the person (Introductory Clause, Article 27
(b) Method of provision by cases set forth in each item of Article 27(1) of the Act (for details on "cases set forth in Article 27(1) of the Act", refer to the above (3))
(c) Method of provision by opt-out (Article 27(2) of the Act)
(e) Method of provision by entrustment, business succession, or joint use (each item of Article 27(5) of the Act)

2-1 Consent From the Person to the Effect that They Approve of Provision of Personal Data to Third Parties in Foreign Countries

Here, the "consent from the person" refers to the person indicating the intent to approve the provision of personal data of the said person to third parties in foreign countries by a business operator handling personal information.

In addition, "obtaining the consent of the person" refers to a business operator handling personal information recognizing the person's indication of the intent of approval and shall be performed by a reasonable and proper method that is considered necessary for the person to make a decision in accordance with the characteristics of the business and the state of handling of personal information.

Note that in cases in which a minor, adult ward of the state, conservatee, or person under limited guardianship does not have the ability to determine the result of consenting to the handling of personal information, it is necessary to obtain consent from a guardian, legal representative, or the like.

In cases of obtaining the consent of the person required in Article 28(1) of the Act, it is necessary to provide information based on Article 28(2) of the Act to the person. For information that should be provided to the person at the time of obtaining consent, refer to 5 (Provision of Information at the Time of Obtaining Consent).

Note that in cases in which there is consent to the handling of personal information by the person, which has been obtained before the date of enforcement of the 2015 Amendment Act, if that consent corresponds to the consent that approves the provision of personal data to a third party in a foreign country under the stipulation of Article 24 of the Act after amendment by the 2015 Amendment Act (Article 28 of the current Act), it is deemed that
there has been consent under the same article (Article 3 of supplementary provisions of the 2015 Amendment Act).

In addition, in cases in which there is consent to the handling of personal information by the person for a corporation or the like of the attached Table 2 before the date of enactment of the 2021 Amendment Act (refers to a corporation in Table 2 of the Act; a business operator handling personal information under the stipulation of Article 58(2) of the Act; the same business operator handling personal information that is Japan Organization of Occupational Health and Safety, an academic research institute, or the like deemed to be a pseudonymized information handling business operator or a business operator handling information related to individuals; hereinafter the same), if that consent corresponds to the consent that approves the provision of personal data to a third party in a foreign country under the stipulation of Article 28(1) of the Act, it is deemed that there has been consent under the same paragraph (Article 7(5) of supplementary provisions of the 2021 Amendment Act).

2-2 Third Party in a Foreign Country

A “third party” of the “third party in a foreign country” is an entity other than a business operator handling personal information and providing personal data and the person who is identified by the said personal data, and foreign governments are also included in this. More specifically, applicability is determined as follows.

In cases of a corporation, it is determined whether the corporation corresponds to a “third party” based on whether the corporation has a legal personality that is different from a business operator handling personal information and providing personal data.

For example, in cases where a Japanese corporation provides personal data to their local subsidiary that has obtained a foreign legal personality, the case corresponds to the provision of personal data to a “third party in a foreign country” for the said Japanese corporation. However, in cases of transferring personal data within the same legal personality, such as local office or branch, it does not correspond to the provision of personal data to a “third party in a foreign country”.

Case) In a case in which a Japanese corporation of a foreign corporation provides personal data to its parent company in a foreign country, the said parent company corresponds to a “third party in a foreign country”.
In addition, even in the case of a foreign corporation incorporated under foreign laws and regulations and having a location in a foreign country, if it is recognized that the corporation has a “personal information database or the like” in Japan for their business (*1), such as in cases in which the corporation has an office in Japan or performs business activities in Japan, the said foreign corporation does not correspond to a “third party in a foreign country”.

Case) In a case where a Tokyo main office of a Japanese corporation provides personal data to a Tokyo branch of a foreign corporation, the said Tokyo branch of a foreign corporation corresponds to a “business operator handling personal information” that has a “personal information database or the like” in Japan for their business (*2) and does not correspond to a “third party in a foreign country”.

(*1) Here, the “business” in “has...for...business” are acts of the same kind that are repeatedly and continuously executed with a certain purpose and are recognized as a business under normal social conventions, and it does not matter whether they are commercial or non-profit.

(*2) A “business operator handling personal information” (Article 16(2) of the Act) refers to an entity excluding national institutions, regional public organizations, independent administrative corporations, or the like stipulated in Article 2(9) of the Act (excluding corporations set forth in attached Table 2), and regional independent administrative corporations stipulated in Article 2(10) of the Act.

Note that those having a personal information database or the like for their business corresponds to business operators handling personal information regardless of the number of specific individuals to be identified by personal information constituting the said personal information database or the like.

3. Foreign Countries That Have a Policy on the Protection of Personal Information Recognized to be of the Same Standard as Japan When Protecting the Rights and Interests of Individuals

The EU and the UK correspond to foreign countries that have a policy on the protection of
personal information recognized to be of the same standard as Japan when protecting the
rights and interests of individuals. Here, the EU refers to countries defined in the "Foreign
Countries That Have a Policy on the Protection of Personal Information Recognized to be of
the Same Standard as Japan When Protecting the Rights and Interests of Individuals" (Rules
refer to countries that are defined in the Personal Information Protection Commission Notice
No. 1 of 2019) (however, the UK is not included).

Note that the EU and the UK have been designated in accordance with the adequacy
decision for Japan by the European Commission (a decision in which the European
Commission recognizes that a country, region, or the like ensures an adequate level of
protection for personal data based on Article 45 of GDPR (†)) in order to achieve smooth
transferring of personal data between Japan and the EU.

(†) REGULATION 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, and repealing Directive 95/46/EC (General Data Protection
Regulation)

4. Standard for a System Necessary for Continuously Taking
Measures That Correspond to Measures That Should be Taken
by Business Operators Handling Personal Information

The standard for a system necessary for continuously taking measures that correspond to
measures that should be taken by business operators handling personal information is
stipulated in Article 16 of the Rules. Note that it is not necessary to notify in advance Personal
Information Protection Commission that necessary systems have been prepared.

4-1 Proper and Reasonable Methods (Related to Item 1 of Article 16 of the
Rules)

A “proper and reasonable method” should be determined for each individual case. However,
it is necessary that the method is such that a third party in a foreign country to which personal
data is provided can ensure continuous measures corresponding to measures that should be taken by business operators handling personal information in Japan.

For example, the following cases apply.

Case 1) A case of entrusting a business operator in a foreign country with the handling of personal data
   Agreements between a provider and a recipient, notes of confirmation, memoranda, and the like
Case 2) A case of transferring personal data between the same corporate group
   Bylaws applying in common between a provider and a recipient, privacy policies, and the like

In addition, it is deemed that business operators certified by Asia Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System (*) need to, as a requirement for certification, prepare, with a third party, measures ensuring that duties that the said business operators have in respect to the person are fulfilled in the same manner by the said third party even in cases in which the said third party handles personal information in place of the said business operators.

Accordingly, in cases in which a business operator handling personal information, who is the provider, is certified by CBPR and a “third party in a foreign country”, who is the recipient, handles personal information in place of the said business operator handling personal information, it is interpreted that one of the “proper and reasonable methods” is that the said business operator handling personal information fulfills the requirements for certification by CBPR. Note, in cases in which a “third party in a foreign country”, who is the recipient, is certified by CBPR, refer to 4-3 (That an Entity to be Provided with Personal Data Is Certified Based on an International Framework Pertaining to the Handling of Personal Information)

(*) APEC CBPR System
   A system that internationally certifies the adequacy of a business operator with regard to APEC Privacy Framework.
   Participating countries and regions request to join this system, and countries that have been approved to participate register an accountability agent (AA). This AA certifies the adequacy of a business operator with regard to APEC Privacy Framework based on their application.
   Note that the target of these measures to be taken is “the said personal data” that has actually
been provided. Therefore, it is not necessary for the said measures to be taken with respect to the handling of other personal information at the recipient.

4-2 Measures Conforming to the Purport of Stipulations Under Section 2, Chapter 4 of the Act (Related to Item 1 of Article 16 of the Rules)

Those corresponding to “measures corresponding to measures that should be taken by business operators handling personal information” under Article 28(1) are stipulated as “measures conforming to the purport of stipulations under Section 2, Chapter 4 of the Act” under Item 1 of Article 16 of the Rules.

Regarding the “measures conforming to the purport of stipulations under Section 2, Chapter 4 of the Act”, in addition to the view of realization of the protection of the rights and interests of the person to an extent that corresponds to cases in which personal data is handled by business operators handling personal information in Japan also in cases in which personal data is handled by a third party in a foreign country, international consistency is considered taking standards of international frameworks such as the Privacy Guideline by Organisation for Economic Co-operation and Development (OECD) and Privacy Framework by APEC into account.

More specifically, matters noted in 4-2-1 to 4-2-20 as “measures conforming to the purport of stipulations under Section 2, Chapter 4 of the Act” shall be ensured by methods noted under Proper and Reasonable Methods (refer to 4-1) (*1).

It is not necessary for a business operator handling personal information to stipulate all the matters noted in 4-2-1 to 4-2-20 in an agreement or the like. Execution of “measures” need only be ensured within a range that is necessary for the protection of rights and interests of the person pertaining to personal data, which has been provided to a third party in a foreign country, by a substantively proper and reasonable method in view of the “purport of stipulations under Section 2, Chapter 4 of the Act”.

In the following 4-2-1 to 4-2-20, concrete examples of measures that should be taken by a third party in a foreign country or a business operator handling personal information in Japan, who is the provider, (hereinafter referred to as a “third party in a foreign country or the like”) are indicated for typical cases related to the provision of personal data to a third party in a
foreign country: [Case 1] a case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data and [Case 2] a case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country.

(*1) The “measures conforming to the purport of stipulations under Section 2, Chapter 4 of the Act” are as noted in the following table (*2) (*3).

Measures Conforming to the Purport of Stipulations Under Section 2, Chapter 4 of the Act
Article 17 Specifying a Utilization Purpose
Article 18 Restriction due to Utilization Purpose
Article 19 Prohibition of Improper Use
Article 20 Proper Acquisition
Article 21 Notification etc. of a Utilization Purpose when Acquiring
Article 22 Assurance etc. about the Accuracy of Data Contents
Article 23 Security Control Measures
Article 24 Supervision of Employees
Article 25 Supervision of Trustees
Article 26 Report on Leakage etc.
Article 27 Restriction on Third Party Provision
Article 28 Restriction on Provision to a Third Party in a Foreign Country
Article 32 Public Disclosure etc. on Matters relating to Retained Personal Data
Article 33 Disclosure
Article 34 Correction etc.
Article 35 Utilization Cease etc.
Article 36 Explanation of Reasons
Article 37 Procedures for Response to Request for Disclosure etc.
Article 38 Charges
Article 40 Processing of Complaints by Entities Handling Personal Information

(*2) Regulations on Special Care-Required Personal Information-2 (Article 20(2) of the Act), Provision of Personal Data to Third Parties by Opt-Out (Article 27(2) and (3) of the Act), Duties of Confirmation and Recording at the Time of Provision to Third Parties (Articles 29 and 30 of the Act), Regulations on Provision of Information on Individuals (Article 32 of the Act), Disclosure of Recording of Provision to Third Parties (Article 33(5) of the Act), and other procedures related to these (Other Procedures Related to Disclosure of Recording of
Provision to Third Parties) are not included in the measures that should be taken by third parties in foreign countries or the like as “measures conforming to the purport of stipulations under Section 2, Chapter 4 of the Act” stated here.

(* 3) Even in cases in which a third party provided with personal data from a business operator handling personal information in Japan meets the requirements in Article 166 of the Act and is a target of extraterritorial application, this does not mean that the third party immediately meets the standards of Article 16 of the Rules. In order to meet the standards of the same article, it is necessary for the third party to additionally prepare a system that is necessary for continuously taking measures that correspond to measures that should be taken by business operators handling personal information with regard to the handling of the said personal data.

Note that, in these cases, the said third party in a foreign country has the duty of handling the said personal data in accordance with the stipulations of the Act including the regulations (refer to the above (*2)) that are not included in the measures that should be taken as “measures conforming to the purport of stipulations under Section 2, Chapter 4 of the Act”.

For details on extraterritorial application, refer to the General Rule Guideline “8 (Extraterritorial Application)”.

4-2-1 Specifying a Utilization Purpose (Measures Conforming to the Purport of Article 17 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data

Utilization purposes by the business operator in a foreign country are specified in a trust agreement.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country

Utilization purposes are specified in labor regulations.

A third party in a foreign country or the like shall concretely specify utilization purposes to the best of their ability when handling personal information. However, when specifying utilization purposes, it is preferred that utilization purposes are specified not in an abstract or general manner but specifically to an extent that the person can generally and reasonably envision for what business and for what purpose personal information will be used in the end (*1) (*2).
(*1) The purport of “specifying a utilization purpose” is to establish and enable the person to predict a range in which personal information is handled by those handling personal information clearly recognizing for what business and for what purpose personal information will be used by specifying and clarifying to the best of their ability.

In cases in which the person cannot reasonably predict or envision from the utilization purposes how their personal information will be handled, it is not deemed that utilization purposes have been specified to the best of one’s ability conforming to the purport.

For example, in cases in which information such as behaviors and interests of the person is analyzed from the information obtained from the person, a third party in a foreign country or the like shall specify utilization purposes to an extent by which the person can predict and envision how the information is being handled.

[Cases in which utilization purposes are concretely specified in cases in which information such as behaviors and interests is analyzed from information obtained from the person]

Case 1) “Obtained information such as browsing history and purchase history is analyzed and used for marketing related to new products and services that accords with interests and preferences.”

Case 2) “Obtained information such as behavior history is analyzed, a credit score is calculated, and then the said score is provided to a third party.”

(*2) Cases in which a range in which the personal information of the person is used can be reasonably predicted by the person to be identified from personal information by referring to the content of a trust agreement, labor regulations, or the like or cases in which a range of utilization purposes is envisioned by explicitly indicating the type of business, it may be deemed sufficient. However, in most cases, it is interpreted that utilization purposes have not been concretely specified to the best of one’s ability by simply explicitly indicating the type of business. Note that also cases in which a business is explicitly indicated such as “OO business” when specifying utilization purposes, under normal social conventions, it is preferred that a range that is recognized to contribute to the specification by the person is specified.

In addition, it is interpreted that concrete specification has not been performed to the best of one’s ability by simply deeming abstract and general content, such as “business activity” and “enhancement of services for clients”, as a utilization purpose.

Note that specified utilization purposes can be changed within a range that is reasonably
recognized as relating to the utilization purposes before the change, that is, under normal social conventions, the utilization purposes after the change is within a range that is objectively recognized to be an extent that is normally predictable by the person (*) given the utilization purposes before the change.

(*) A "range that is objectively recognized to be an extent that is normally predictable by the person" is not subjectively determined by the person or arbitrarily determined by a business operator. It is a range that can be predicted by comparing the initial utilization purposes and the utilization purposes after the change by a determination of an ordinary person and is determined by generally taking into consideration to what extent the utilization purposes after the change is related to the initially specified utilization purposes.

4-2-2 Restriction due to Utilization Purpose (Measures Conforming to the Purport of Article 18 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data Administrative processes within a range of utilization purposes by a business operator in a foreign country are stipulated as the content of the entrustment in a trust agreement.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country Employee information is utilized within a range of utilization purposes specified in labor regulations. Note that in cases in which the range of utilization purposes is exceeded, it is necessary to obtain the consent of the said employee (*). In such cases, it is interpreted that a business operator handling personal information in Japan is allowed to obtain consent. In cases of handling personal information outside of the range that is necessary to accomplish the specified utilization purposes, a third party in a foreign country or the like shall obtain in advance the consent of the person (*). However, utilizing personal information to obtain the said consent (such as emailing or calling) does not correspond to being outside of utilization purposes even in cases in which it has not been indicated as an initially specified utilization purpose.

(*) The "consent of the person" refers to the said person indicating the intent to approve the handling of personal data of the said person by a method indicated by a third party in a foreign
country or the like (on the premise that the said person has been confirmed).

In addition, "obtaining the consent of the person" refers to the said third party in a foreign country or the like recognizing the person's indication of the intent of approval and shall be performed by a reasonable and proper method that is considered necessary for the person to make a decision in accordance with the characteristics of the business and the state of handling of personal information.

Note that in cases in which a minor, adult ward of the state, conservatee, or person under limited guardianship does not have the ability to determine the result of consenting to the handling of personal information, it is necessary to obtain consent from a guardian, legal representative, or the like.

[Cases in which the person's consent has been obtained]
Case 1) Oral indication of the intent of approval by the person
Case 2) Reception of the intent of approval by the person in writing (including electromagnetic records)
Case 3) Reception of an email of the intent of approval by the person
Case 4) Checking of a confirmation field for approval by the person
Case 5) Clicking a button on a homepage for the intent of approval by the person
Case 6) Voice input, a touch on a touch panel, or input by a button, switch, or the like for intent of approval by the person

4-2-3 Prohibition of Improper Use (Measures Conforming to the Purport of Article 19 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data. Utilization by methods that risk promoting or inducing illegal or unfair acts by business operators in foreign countries using trust agreements is prohibited.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country. Utilization by methods that risk promoting or inducing illegal or unfair acts by parent companies in foreign countries using bylaws or the like is prohibited.

Third parties in foreign countries or the like shall not utilize personal information by methods
that risk (*2) promoting or inducing illegal or unfair acts (*1).

(*1) Although it cannot be said that “illegal or unfair acts” are acts that violate the Act (Act on the Protection of Personal Information) or other laws, regulations, and policies or are immediately illegal, “illegal or unfair acts” refer to acts that cannot be recognized to be appropriate under normal social conventions, such as violating the purport of the Act (Act on the Protection of Personal Information) and other laws, regulations, and policies.

(*2) Whether there is “risk” is determined by whether it is recognized that, under normal social conventions, there is a probability that the utilization of personal information by a third party in a foreign country or the like may promote or induce illegal or unfair acts. When making this determination, in addition to objective matters such as the method of utilization of personal information, it is necessary to take the recognition and foreseeability of a third party in a foreign country or the like at the time of utilization of personal information into account. For example, in cases in which a third party in a foreign country or the like provides personal information to another business operator, even in cases in which the said another business operator has used the said personal information for an illegal act, in cases in which the said third party in a foreign country or the like, having a general level of attentiveness, could not have predicted that the provided personal information would be used illegally at the time of provision of the said personal information, such as the said another business operator having falsified the purpose of acquiring the said personal information, it is interpreted that it is not recognized that there is “risk”.

4-2-4 Proper Acquisition (Measures Conforming to the Purport of Article 20 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data

So long as it is obvious that a business operator in a foreign country is properly acquiring personal data based on a trust agreement, it is not an acquisition by illegal means.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country

So long as it is obvious that a parent company in a foreign country is properly acquiring personal data based on bylaws or the like, it is not an acquisition by illegal means.
Note that, regarding regulations on special care-required personal information, since the target of so-called sensitive information may differ depending on the country (Explanatory Memorandum to the OECD Privacy Guideline (1980)) and also in view of international consistency, it is not necessary to take “measures” (refer to 4-2 (Measures Conforming to the Purport of Stipulations Under Section 2, Chapter 4 of the Act)).

4-2-5 Notification etc. of a Utilization Purpose when Acquiring (Measures Conforming to the Purport of Article 21 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data Utilization purposes and the like are notified to clients from a business operator handling personal information in Japan.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country Utilization purposes and the like are notified to employees from a business operator handling personal information in Japan.

It is preferred that, in cases of acquiring personal information, third parties in foreign countries or the like have publicly disclosed (*) in advance the utilization purposes thereof. In cases in which the utilization purposes are not disclosed, upon acquiring personal information, the third parties in foreign countries or the like shall promptly notify the person (*2) or disclose the utilization purposes thereof.

(*1) To “publicly disclose” refer to broadly and generally notifying one’s intent (to announce so as to inform an unspecified large number of people), and public disclosure shall be performed by a reasonable and proper method in accordance with the characteristics of the business and the state of handling of personal information.

[Cases corresponding to public disclosure]
Case 1) Posting on locations that can be accessed by approximately one operation from the top page of a company’s own homepage
Case 2) Posting posters or the like or placing or distributing pamphlets or the like at locations where it is anticipated to be visited by customers, such as a company’s stores or offices
Case 3) (In cases of mail-order), posting on mail-order pamphlets, catalogs, and the like
(*2) To "notify the person" refers to directly informing the person and shall be performed by a reasonable and proper method by which the person recognizes the content in accordance with the characteristics of the business and the state of handling of personal information.

[Cases corresponding to notifying the person]
Case 1) Informing by directly handing a document such as a flyer.
Case 2) Informing orally or by automatic response devices or the like.
Case 3) Informing by sending electronic emails, faxes, or the like or by sending documents via postal services.
For additional details, refer to General Rule Guideline 3-3-3 (Notification or Public Disclosure of Utilization Purposes) to “3-3-5 (Cases in Which Notification of Utilization and the Like Need Not Be Performed)”. 

4-2-6 Assurance etc. about the Accuracy of Data Contents (Measures Conforming to the Purport of Article 22 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data. Assurance and the like of accuracy of data content is stipulated in a trust agreement, or a business operator handling personal information, who is the provider of personal data, is responsible for the assurance and the like of accuracy of data content.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country. Accuracy of employee information is ensured through a business operator handling personal information in Japan.

Third parties in foreign countries or the like shall endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of utilization purposes by preparing procedures for referencing and confirmation at the time of inputting personal information to a personal information database or the like, preparing procedures for correction or the like for when errors or the like are found, updating recorded matters, setting a retention period, and the like within a range that is necessary for achieving utilization purposes.
Note that it is not necessary to uniformly or always update held personal data. It is sufficient so long as accuracy and currentness are ensured within respective necessary ranges in accordance with respective utilization purposes.

In addition, when it is no longer necessary to use the held personal data (i.e., cases in which there no longer is a reasonable reason to hold the said personal data in relation to a purpose concerned due to the achievement of a utilization purpose, cases in which although a utilization purpose has not been accomplished the business that was the premise of a purpose concerned has become discontinued, or the like), third parties in foreign countries or the like shall endeavor to delete the said personal data without delay (*). Note that limitation is not made to this in cases in which retention periods or the like are defined under laws and regulations.

[Cases corresponding to cases in which it is no longer necessary to use personal data]
Case) A case in which personal data for sending prizes for a campaign to applicants for the said campaign is held but the prizes have been sent and a period that is reasonable for responding to undelivered prizes and the like has passed
(*) “Deletion of personal data” includes disallowing the use of the said personal data as personal data, deleting the said data, and making it impossible to identify a specific individual from the said data.

For additional details, refer to the General Rule Guideline “3-4-1 (Assurance and the Like of Accuracy of Data Content)”.

4-2-7 Security Control Measures (Measures Conforming to the Purport of Article 23 of the Act)
[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data
It is stipulated in a trust agreement that security control measures are taken by a business operator in a foreign country.
[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country
It is stipulated in bylaws or the like that security control measures are taken by a parent company in a foreign country.
Third parties in foreign countries or the like shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data. However, it is necessary that the said measures are necessary and proper in accordance with the scale and characteristics of the business, the state of handling of personal data (including the characteristics and amount of personal data to be handled), and risk attributable to the characteristics of the medium on which personal data is recorded in consideration of the magnitude of violation of rights and interests of the person in cases in which personal data has been leaked or the like. For specific measures that shall be taken, examples of methods for practicing the said measure, and the like, refer to the General Rule Guideline “7 (Attachment) Content of Security Control Measures That Should be Taken”.

4-2-8 Supervision of Employees (Measures Conforming to the Purport of Article 24 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data. Measures pertaining to supervision of employees by a business operator in a foreign country are stipulated in a trust agreement.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country. Measures pertaining to supervision of employees by a parent company in a foreign country are stipulated in bylaws or the like.

When a third party in a foreign country or the like has an employee handle personal data, it shall exercise necessary and appropriate supervision over the employee to ensure the security control of the personal data such that security control measures conforming to Article 23 of the Act are observed. At that time, it is preferred that necessary and proper measures are taken such as improving the content and frequency of education, training, and the like of employees handling personal data in accordance with the scale and characteristics of the business, the state of handling of personal data (including the characteristics and amount of personal data to be handled), and risk attributable to the characteristics of the medium on which personal data is recorded in consideration of the magnitude of violation of rights and interests of the person in cases in which personal data has been leaked or the like.

“Employees” are those who are in an organization such as a third party in a foreign country and is engaged in the work of a business operator under the direct or indirect command and
supervision of the said operator and includes not only employees that are employed (such as full-time employees, contract employees, and part-time employees) but also executives, operating officers, auditors, and contract employees.

[Cases in which necessary and proper supervision of employees is not performed]
Case 1) A case in which personal data has leaked as a result of an employee not confirming that they are performing their work in accordance with rules or the like defining security control measures for personal data
Case 2) A case in which, despite a notebook PC or an external storage medium having personal data repeatedly being taken outside against internal rules or the like, as a result of not addressing that act, the said PC or the said storage medium is lost, and then personal data is leaked

4-2-9 Supervision of Trustees (Measures Conforming to the Purport of Article 25 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data
Measures pertaining to supervision of trustees re-entrusted by a business operator in a foreign country are stipulated in a consignment contract.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country
Measures pertaining to supervision of trustees re-entrusted by a parent company in a foreign country are stipulated by bylaws or the like.

When entrusting the handling of personal data (*1) in whole or in part, a third party in a foreign country or the like shall exercise necessary and appropriate supervision over an entity that has been entrusted (hereinafter, referred to as the “trustee”) to ensure the security control of the entrusted personal data. More specifically, a third party in a foreign country or the like shall exercise supervision such that measures that are equivalent to the security control measures that they should take in conformity with Article 23 of the Act are taken (*2).

At that time, personal data that is not necessary for the content of the affairs to be entrusted is not provided as a matter of course, and in view of the content of personal data for which handling is entrusted, necessary and proper measures set forth in the following (1) to (3) shall be taken in accordance with risk attributable to the scale and characteristics of the
affairs to be entrusted and the state of handling of personal data (including the characteristics and amount of personal data to be handled) in consideration of the magnitude of violation of rights and interests of the person in cases in which personal data has been leaked or the like (*3).

(1) Selection of proper trustee
When selecting a trustee, in order to confirm that security control measures of the trustee are equivalent to what is required of the trustor, it shall be confirmed in advance that each item defined in the General Rule Guideline “10 (Attachment) Content of Security Control Measures That Should be Taken” is reliably implemented in conformity with the content of the affairs to be entrusted.

(2) Conclusion of a trust agreement
In a trust agreement, it is preferred to include that a trustor has a reasonable understanding of the content upon which both the trustor and trustee have agreed as necessary and proper security control measures as well as the state of handling of entrusted personal data at the trustee.

(3) Understanding the state of handling of personal data at the trustee
In order to understand the state of handling of personal data at the trustee, it is preferred that proper evaluation is performed including considering a revision of the content of entrustment after surveying the extent of execution of the content included in the trust agreement by periodic audits.

In addition, in cases of re-entrustment by the trustee, similarly to cases of entrustment, it is preferred that the trustor sufficiently confirms that the trustee properly executes the supervision of trustees of this article on the trustees of re-entrustment by requesting advanced report or approval from the trustor on parties to be re-entrusted, the content of the affairs to be re-entrusted, handling of personal data by the trustees of re-entrustment, and the like and that the trustees of re-entrustment take security control measures conforming to the purport of Article 23 of the Act (*4). The case of re-entrustment applies to cases in which the trustees of re-entrustment perform further re-entrustment.

Note, regarding re-entrustment, refer to 4-2-12 (Restriction on Provision to a Third Party in a Foreign Country).

[Cases in which necessary and proper supervision of trustees is not executed]
Case 1) A case in which a trustee has leaked personal data as a result of entrusting an external business operator without a proper understanding of the state of security control measures for personal data at the time of concluding an agreement and
thereafter
Case 2) A case in which a trustee has leaked personal data as a result of not instructing the trustee with the content of necessary security control measures related to handling personal data
Case 3) A case in which, as a result of a trustee entrusting the processing of personal data without instructing a trustee on the conditions of re-entrustment and not confirming the state of handling of personal data by the trustee, the said trustee of the re-entrustment leaks personal data
Case 4) A case in which, as a result of re-entrustment unrecognized by a trustor being executed due to the trustor not performing necessary measures such as requesting a trustee to report on re-entrustment despite an agreement including that the trustor understands the state of implementation of re-entrustment by the trustee, a trustee of the said re-entrustment leaks personal data

(*1) Here, “entrusting the handling of personal data” refers to having another entity handle personal data regardless of the form or type of contract. More specifically, it is anticipated that processing, such as inputting (including obtaining from the person), editing, analyzing, and outputting, of personal data is entrusted.

(*2) In cases where a trustor is taking safety control measures that exceed the standard that is required by Article 23 of the Act, the purport is not to require the trustee to take the same measures. From a legal standpoint, it is interpreted to be sufficient so long as safety control measures of the standard required by Article 23 of the Act are taken.

(*3) For the selection of trustees and understanding of the state of handling of personal data by the trustees, it is necessary to take a proper method in accordance with the content and scale of personal data for which handling is entrusted. For example, it is conceivable to perform confirmation by visiting, as necessary, the location at which personal data is handled or a reasonable alternative method (including oral confirmation).

(*4) In cases in which “necessary and proper supervision” of a trustee has not been executed by a trustor, when the trustee executes re-entrustment and a re-entrusted trustee executes improper handling, it may be determined that the trustor has violated the law. Therefore, caution is necessary in cases of re-entrustment.

4-2-10 Report on Leakage etc. (Measures Conforming to the Purport of Article 26 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data
In cases in which a situation (hereinafter referred to as the “situation to be reported”) pertaining to ensuring the safety of personal data, such as leakage, loss, or damage of personal data, which are targets of reporting duties defined in Article 26(1) of the Act, has occurred at a business operator in a foreign country, it is made clear by a trust agreement that a business operator handling personal information in Japan takes measures pertaining to reporting to Personal Information Protection Commission and notifying the person.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country

In cases where a situation to be reported occurs at a parent company in a foreign country, it is made clear by bylaws or the like that a business operator handling personal information in Japan takes measures pertaining to reporting to Personal Information Protection Commission and notifying the person.

For details on situations to be reported and measure that should be taken by a third party in a foreign country or the like in cases where a situation to be reported occurs, refer to the General Rule Guideline “3-5 (Reporting and the Like of Leakage of Personal Data and the Like)".  

For details on situations to be reported and measure that should be taken by a third party in a foreign country or the like in cases where a situation to be reported occurs, refer to the General Rule Guideline “3-5 (Reporting and the Like of Leakage of Personal Data and the Like)".

4-2-11 Restriction on Third Party Provision (Measures Conforming to the Purport of Article 27 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data

The provision of personal data to a third party from a business operator in a foreign country is prohibited by a trust agreement.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country
The provision of personal data to a third party from a parent company in a foreign country is prohibited by bylaws or the like.

When providing to another “third party” from a “third party in a foreign country”, measures conforming to the purport of Article 27(1), (5), and (6) of the Act shall be taken. Note, in cases in which a third party, who is the provider, is a “third party in a foreign country” (including a third party in Japan who is the same as the third party in a foreign country, who is the provider), refer to 4-2-12 Restriction on Provision to a Third Party in a Foreign Country.

A third party in a foreign country or the like shall not provide personal data without obtaining, in advance, the consent of the person when providing personal data to a third party. When obtaining consent, it is necessary to clearly indicate the content of a reasonable and proper range considered to be necessary for the person to make a decision pertaining to the consent in accordance with the scale and characteristics of the business, the state of handling of personal data (including the characteristics and amount of personal data to be handled). Note that, in cases in which provision of personal information to a third party is anticipated in advance, that shall be specified in the utilization purposes (refer to 4-2-1 Specifying a Utilization Purpose).

Note that, since the provision of personal data to a third party by opt-out (Article 27(2) and (3) of the Act) is a stipulation defining notification or the like to Personal Information Protection Commission, due to its characteristics, it is excluded from the measure that should be taken by a third party in a foreign country or the like (refer to 4-2 (Measures Conforming to the Purport of Stipulations Under Section 2, Chapter 4 of the Act)).

4-2-12 Restriction on Provision to a Third Party in a Foreign Country (Measures Conforming to the Purport of Article 28 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data

The provision of personal data to a third party from a business operator in a foreign country is prohibited by a trust agreement.

In cases in which a business operator further re-entrusts a third party in a foreign country with the handling of personal data, execution of measures conforming to the purport of stipulations under Section 2, Chapter 4 of the Act in addition to the duties of supervision of
trustees (4-2-9) in Article 25 of the Act are ensured.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country

The provision of personal data to a third party from a parent company in a foreign country is prohibited by bylaws or the like.

Also in cases in which personal data is further transferred from a parent company in a foreign country to a subsidiary in another country, execution of measures conforming to the purport of stipulations under Section 2, Chapter 4 of the Act is ensured by bylaws or the like.

In cases of provision from a “third party in a foreign country” to another “third party in a foreign country” (including a third party in Japan who is the same as the third party in a foreign country, who is the provider), a response shall be taken conforming to the arrangement in “2. General Remarks”.

4-2-13 Public Disclosure etc. on Matters relating to Retained Personal Data

(Measures Conforming to the Purport of Article 32 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data

In cases in which “retained personal data” (*) applies for a business operator whose personal data to be provided is in a foreign country, it is made clear by a trust agreement that a business operator handling personal information in Japan fulfills duties pertaining to public disclosures etc. on matters relating to retained personal data.

Note that, in cases in which “retained personal data” does not apply for a business operator whose personal data to be provided is in a foreign country, in conclusion, it is not necessary to take “measures”.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country

Fulfillment of duties pertaining to public disclosures etc. on matters relating to retained personal data by a business operator handling personal information in Japan is clarified by bylaws or the like.

(*) “Retained personal data” refers to “personal data” over which a third party in a foreign
country or the like has the authority to disclose, to correct, add or delete the content, to
discontinue its utilization, to erase, and to discontinue its provision to a third party (hereinafter
referred to as “disclosure and the like”) requested by the person or their representative.

However, among personal data, the following is not “retained personal data”.

(1) Those for which the knowledge of presence or absence of the said personal data may
risk harm to the life, body, or property of the person or a third party.
Case) Personal data of persons, who are the perpetrator (spouse or person with parental
rights) and the victim (spouse or child), held by an organization that assists victims of
domestic violence or child abuse
(2) Those for which the knowledge of presence or absence of the said personal data may
promote or induce illegal or unfair acts.
Case 1) Personal data of a person, who corresponds to an anti-social force, held by a
business operator in order to prevent damage from unfair demands by anti-social
forces such as a criminal syndicate
Case 2) Personal data of a person, who has taken corresponding acts, held by a business
operator in order to prevent damage from unfair demands by suspicious persons,
chronic complainers, and the like
(3) Those for which the knowledge of presence or absence of the said personal data may
risk harm to the safety of a country, risk loss of credibility from another country or an
international institution, or risk suffering disadvantage in negotiation with another country or
an international institution.
Case 1) Personal data of a person, who is a person in charge, recording the name of the
person in charge of design or development of a weapon, facility, equipment,
software, and the like related to defense held by a manufacturer, information service
business operator, or the like
Case 2) Personal data, such as itinerary of a person who is a very important person, held by
a destination or the security company thereof of the very important person
(4) Those for which the knowledge of presence or absence of the said personal data may
risk impedance to prevention, suppression, or investigation of crimes; safety of the public;
and maintenance of order.
Case 1) Personal data obtained for the first time by request for matters related to an
investigation by the police
Case 2) Personal data such as a register of reception of a request, register of transmission
of response, and list of targets of request created by a business operator who
received the request for matters related to an investigation or the like regarding
information and the like on a party to a contract from the police (* note that information and the like on a party to a contract corresponds to “retained personal data”)

Case 3) Personal data that has been newly created for whether or not there is a notification of suspicious transaction or when notifying a suspicious transaction based on Article 8(1) of Act on Prevention of Transfer of Criminal Proceeds (Law No. 22 of 2007)

Case 4) Personal data included in information related to a bank account used for bank transfer fraud

In cases in which personal data to be provided corresponds to “retained personal data” for a third party in a foreign country, for details on measures that should be taken by a third party in a foreign country or the like, refer to the General Rule Guideline “3-8-1 (Public Disclosure etc. on Matters relating to Retained Personal Data)”.

4-2-14 Disclosure (Measures Conforming to the Purport of Article 33 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data

In cases in which “retained personal data” applies for a business operator whose personal data to be provided is in a foreign country, it is made clear by a trust agreement that a business operator handling personal information in Japan fulfills duties pertaining to disclosure.

Note that, in cases in which “retained personal data” does not apply for a business operator whose personal data to be provided is in a foreign country, in conclusion, it is not necessary to take “measures”.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country

It is made clear by bylaws or the like that a business operator handling personal information in Japan fulfills duties pertaining to disclosure.

In cases in which personal data to be provided corresponds to “retained personal data” for a third party in a foreign country, for details on measures that should be taken by a third party in a foreign country or the like, refer to the General Rule Guideline “3-8-2 (Disclosure of Retained Personal Data)”.

Note that, regarding duties of confirmation and recording at the time of provision to third parties, since it is not necessary to take “measures” (refer to 4-2 (Measures Conforming to the Purport of Stipulations Under Section 2, Chapter 4 of the Act)), it is also not necessary to
take "measures" with regard to the disclosure of recording of provision to third parties (the same applies to "measures" related to other procedures (*) related to this).

(*) The "measures" related to "other related procedures" refer to measures related to procedures and the like related to disclosure of recording of provision to third parties among 4-2-13 (Public Disclosure etc. on Matters relating to Retained Personal Data (Measures Conforming to the Purport of Article 32 of the Act)), 4-2-17 (Explanation of Reasons (Measures Conforming to the Purport of Article 36 of the Act)), 4-2-18 (Procedures for Response to Request for Disclosure etc. (Measures Conforming to the Purport of Article 37 of the Act)), and 4-2-19 (Charges (Measures Conforming to the Purport of Article 38 of the Act)).

4-2-15 Correction etc. (Measures Conforming to the Purport of Article 34 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data

In cases in which “retained personal data” applies for a business operator whose personal data to be provided is in a foreign country, it is made clear by a trust agreement that a business operator handling personal information in Japan fulfills duties pertaining to correction and the like.

Note that, in cases in which “retained personal data” does not apply for a business operator whose personal data to be provided is in a foreign country, in conclusion, it is not necessary to take “measures”.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country

It is made clear by bylaws or the like that a business operator handling personal information in Japan fulfills duties pertaining to correction and the like.

In cases in which personal data to be provided corresponds to “retained personal data” for a third party in a foreign country, for details on measures that should be taken by a third party in a foreign country or the like, refer to the General Rule Guideline “3-8-4 (Correction and the Like of Retained Personal Data)".
4-2-16 Utilization Cease etc. (Measures Conforming to the Purport of Article 35 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data. In cases in which “retained personal data” applies for a business operator whose personal data to be provided is in a foreign country, it is made clear by a trust agreement that a business operator handling personal information in Japan fulfills duties pertaining to cease of utilization and the like. Note that, in cases in which “retained personal data” does not apply for a business operator whose personal data to be provided is in a foreign country, in conclusion, it is not necessary to take “measures”.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country. It is made clear by bylaws or the like that a business operator handling personal information in Japan fulfills duties pertaining to cease of utilization and the like. In cases in which personal data to be provided corresponds to “retained personal data” for a third party in a foreign country, for details on measures that should be taken by a third party in a foreign country or the like, refer to the General Rule Guideline “3-8-5 (Case of Utilization and the Like of Retained Personal Data)”.

4-2-17 Explanation of Reasons (Measures Conforming to the Purport of Article 36 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data. In cases in which “retained personal data” applies for a business operator whose personal data to be provided is in a foreign country, it is made clear by a trust agreement that a business operator handling personal information in Japan fulfills duties pertaining to the explanation of reasons. Note that, in cases in which “retained personal data” does not apply for a business operator whose personal data to be provided is in a foreign country, in conclusion, it is not necessary to take “measures”.

[Case 2] A case in which a business operator handling personal information in Japan provides
employee information to a parent company in a foreign country

It is made clear by bylaws or the like that a business operator handling personal information in Japan fulfills duties pertaining to the explanation of reasons.

In cases in which personal data to be provided corresponds to "retained personal data" for a third party in a foreign country, for details on measures that should be taken by a third party in a foreign country or the like, refer to the General Rule Guideline “3-8-6 (Explanation of Reasons)”.

4-2-18 Procedures for Response to Request for Disclosure etc. (Measures Conforming to the Purport of Article 37 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data

In cases in which "retained personal data" applies for a business operator whose personal data to be provided is in a foreign country, it is made clear by a trust agreement that a business operator handling personal information in Japan fulfills procedures for responding to a request for disclosure and the like.

Note that, in cases in which "retained personal data" does not apply for a business operator whose personal data to be provided is in a foreign country, in conclusion, it is not necessary to take "measures".

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country

It is made clear by bylaws or the like that a business operator handling personal information in Japan fulfills procedures for responding to a request for disclosure and the like.

In cases in which personal data to be provided corresponds to "retained personal data" for a third party in a foreign country, for details on measures that should be taken by a third party in a foreign country or the like, refer to the General Rule Guideline “3-8-7 (Procedures to Meet Requests for Disclosure and the Like)”.

4-2-19 Charges (Measures Conforming to the Purport of Article 38 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data
In cases in which “retained personal data” applies for a business operator whose personal data to be provided is in a foreign country, it is made clear by a trust agreement that a business operator handling personal information in Japan fulfills measures pertaining to charges.

Note that, in cases in which “retained personal data” does not apply for a business operator whose personal data to be provided is in a foreign country, in conclusion, it is not necessary to take “measures”.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country
It is made clear by bylaws or the like that a business operator handling personal information in Japan fulfills measures pertaining to charges.

In cases in which personal data to be provided corresponds to “retained personal data” for a third party in a foreign country, for details on measures that should be taken by a third party in a foreign country or the like, refer to the General Rule Guideline “3-8-8 (Charges)”.

4-2-20 Processing of Complaints by Entities Handling Personal Information
(Measures Conforming to the Purport of Article 40 of the Act)

[Case 1] A case in which a business operator handling personal information in Japan entrusts a business operator in a foreign country with the work of inputting client data
In cases in which “retained personal data” applies for a business operator whose personal data to be provided is in a foreign country, it is made clear by a trust agreement that a business operator handling personal information in Japan fulfills duties pertaining to Article 40 of the Act.
Note that, in cases in which “retained personal data” does not apply for a business operator whose personal data to be provided is in a foreign country, in conclusion, it is not necessary to take “measures”.

[Case 2] A case in which a business operator handling personal information in Japan provides employee information to a parent company in a foreign country
It is made clear by bylaws or the like that a business operator handling personal information in Japan fulfills duties pertaining to Article 40 of the Act.
In cases in which personal data to be provided corresponds to “retained personal data” for a
third party in a foreign country, for details on measures that should be taken by a third party in a foreign country or the like, refer to the General Rule Guideline “3-9 (Regarding Processing of Complaints Related to Handling of Personal Information)”.

4-3 That an Entity to be Provided with Personal Data Is Certified Based on an International Framework Pertaining to the Handling of Personal Information (Related to Item 2 of Article 16 of the Rules)

A “certification based on an international framework pertaining to the handling of personal information” refers to certification by a certification institution authorized based on regulations that have been agreed on by international institutions, and it is necessary that the said framework that enables the continuation of measures that correspond to measures that should be taken by a business operator handling personal information.

This applies to when a third party in a foreign country, who is the recipient, is certified by the CBPR system by APEC. Note, in cases in which a person providing personal data is certified by CBPR, refer to 4-1 (Proper and Reasonable Methods).

5. Provision of Information at the Time of Obtaining Consent

In cases of attempting to obtain the consent of the person approving the provision of personal data to a third party in a foreign country under the stipulations of Article 28(1) of the Act, a business operator handling personal information shall provide the person with information that is required by the stipulations of Article 17(2) of the Rules (Article 28(2) of the Act) (*1) (*2).

When transferring personal data across the border, it is important for a business operator handling personal information, who is the provider, to evaluate the risk of transferring personal data to a foreign country where a third party, who is the recipient, is located and, after careful consideration of the necessity of transferring personal data, provide the person with information in a manner that is easy to understand.

(*1) The stipulations of Article 24(2) of the Act (Article 28(2) of the current Act) related to the
provision of information at the time of obtaining consent is applied to cases in which a business operator handling personal information obtains the consent of the person under the stipulations of Article 24(1) of the Act (Article 28(1) of the current Act) on or after the date of enactment of the 2020 Amendment Act (Article 4(1) of supplementary provisions of the 2020 Amendment Act).

(*2) The stipulations of Article 28(2) of the Act related to the provision of information at the time of obtaining consent is applied to cases in which a corporation or the like of the attached Table 2 (refer to 2-1 (Consent From the Person to the Effect that They Approve of Provision of Personal Data to Third Parties in Foreign Country)) obtains the consent of the person under the stipulations of Article 28(1) of the Act on or after the date of enactment of the 2021 Amendment Act (Article 7(6) of supplementary provisions of the 2021 Amendment Act).

5-1 Method of Providing Information (Related to Article 17(1) of the Rules)

The provision of information to the person shall be performed in a proper method by which it is considered that the person can soundly recognize the information that is required by the stipulations of Article 17(2) to (4) of the Rules. Note that it is important that the information to be provided is easy to understand for the person.

[Cases corresponding to a proper method]
Case 1) Method of transmitting necessary information to the person by electronic email
Case 2) Method of directly issuing a document noting necessary information to the person
Case 3) Method of orally explaining necessary information to the person
Case 4) Method of posting necessary information on a home page and prompting the person to view it

5-2 Information That Should be Provided (Related to Article 17(2) of the Rules)

In cases of attempting to obtain the consent of the person approving the provision of personal data to a third party in a foreign country under the stipulations of Article 28(1) of the Act, information of the following (1) to (3) shall be provided to the person.

“Name of a corresponding foreign country” (Related to Item 1 of Article 17(2) of the Rules)
It refers to the name of the foreign country (*1) where a third party, who is the recipient, is located (*2). It need not necessarily be the official name. However, it shall be a name by which it is considered that the person can reasonably recognize the destination of transfer of their
個人データ。

処理に関する場合は、外国に所在地を特定できない場合に同意を取得する。持続性の第三者が受領者である可能性がある場合、5-3-1（第三者が受領者を特定できない場合）を参照すること。

（*1）外国に保険品の「外国」は、日本の地域域から除外される。全国のルールで定義されている外国を参照とし、個人情報の保護を日本と同等のレベルで認定されている国である。ただし、個人の権利を尊重すると、個人が個人データのリスクを予想する可能性を増加させる目的から、公表された情報やその他の方法で可能な国を特定し、その他に、国ごとの情報の可能性を示すために、他に国名を示す必要はありません。ただし、国等の国である場合も含みます。第三者が受領者であるとき、国から国の政策に関する情報を提供することを推奨します。国等の国の政策に関する情報を提供することは、個人が国等の国の国間の個人情報のリスクを予想する可能性を増加させる目的から、適正かつ合理的な方法で確認すること。

①「適正かつ合理的な方法」

「第三者が受領者である国等の国の政策に関する情報を提供することを推奨します。」

【適正かつ合理的な方法】

1）第三者が受領者である国等の国の查詢方法

2）行政機関等の公開情報による確認方法

これ等の方法で、個人が個人情報のリスクを予想する可能性を増加させる目的から、国等の国の政策に関する情報を提供することが推奨されます。
related to the protection of personal information in a corresponding foreign country” shall be information by which the person can reasonably recognize essential differences between the policies related to the protection of personal information in a foreign country where a third party, who is the recipient, is located and the laws (Act on the Protection of Personal Information) of Japan. More specifically, it is necessary to consider the views of the following (a) to (d).

Note that the “policies related to the protection of personal information in a corresponding foreign country” here are limited to policies that apply to a third party in a foreign country, who is the recipient, among the policies in the said foreign country and do not include policies that do not apply to the said third party.

(a) Presence or absence of policies related to the protection of personal information in a corresponding foreign country
In cases in which there is no policy related to the protection of personal information in a corresponding foreign country among the policies in a foreign country where a third party, who is the recipient, is located, that in itself indicates the presence of risk involved in transferring personal data across the border. Therefore, information shall be provided to the person that there is no policy related to the protection of personal information (*1).

Note that, in cases of providing information that may be the said index, it is preferred to provide information to the person also on the meaning of the information that may be the said index with respect to the risk involved in transferring personal data across the border.

[b) Presence of information that may be an index for policies related to the protection of personal information in a corresponding foreign country
In cases in which there is information that may be an objective index related to the standard or the like of protection of personal information for policies related to the protection of personal information in a corresponding foreign country, it is thought that providing the information to be the said index ensures, to a certain degree, the possibility for the person to predict the risk involved in transferring personal data across the border. Accordingly, in these cases, it is sufficient so long as information that may be the said index is provided, and information pertaining to the following (c) is not required.

[Cases corresponding to information that may be an index for policies related to the protection of personal information in a corresponding foreign country]
Case 1) That a foreign country where a corresponding third party is located is a country of adequacy decision based on Article 45 of GDPR
Case 2) That a foreign country where a corresponding third party is located is a member nation of the CBPR system of APEC
(c) Absence of duties of a business operator or rights of the person corresponding to the eight principles of the OECD privacy guideline
In cases in which there are no duties of a business operator or rights of the person corresponding to the eight principles of the OECD privacy guideline (*2) in the policies related to the protection of personal information in a corresponding foreign country, the absence of duties of a corresponding business operator or rights of the person indicates an essential difference from the laws (Act on the Protection of Personal Information) of Japan. Therefore, the person shall be informed of that content.

Note that, in cases in which the policies related to the protection of personal information in a corresponding foreign country includes all the duties of a business operator and rights of the person corresponding to the eight principles of the OECD privacy guideline, it is sufficient so long as the person is informed of that.

[Cases corresponding to the absence of duties of a business operator or rights of the person corresponding to the eight principles of the OECD privacy guideline]
Case 1) Absence of restricting utilization to the range of utilization purposes specified in advance as a principle for personal information
Case 2) Absence of rights of the person related to the request of disclosure of personal information held by a business operator
(d) Presence of other systems that may have a significant influence on the rights and interests of the person
In cases in which, in a foreign country where a third party, who is the recipient, is located, there are other systems, which may have a greater influence on the rights and interests of the person pertaining to personal data that accompanies the transfer of the said personal data to a foreign country than the systems of Japan, the person shall be informed of the presence of the said policies.

[Cases corresponding to a system that may have a significant influence on the rights and interests of the person]
Case 1) A system that makes it possible for a government to extensively collect information regarding personal information held by a business operator by the government
imposing a duty of extensive cooperation in information collection activities on the business operator

Case 2) A system pertaining to the duties of storing, in Japan, personal information for which there is a risk that a business operator may not be able to respond to a request of deletion or the like from the person

(*1) In cases in which there is a policy related to personal information in a foreign country where a third party, who is the recipient, is located, it is not required to inform the person of separate names of the laws and regulations pertaining to the said policy. However, it is preferred that information can be provided at the request of the person.


“Information related to measures for the protection of personal information taken by a corresponding third party”

(Related to Item 3 of Article 17(2) of the Rules) In view of the purport of the policy to increase the possibility for the person to predict the risks involved in transferring personal data across the border, “information related to measures for the protection of personal information taken by a corresponding third party” shall be information that the person can reasonably recognize the essential differences between the measures for the protection of personal information taken by the corresponding third party in a foreign country and the measures required of a business operator handling personal information regarding the handling of personal data by the laws (Act on the Protection of Personal Information) of Japan.

More specifically, in cases in which the corresponding third party in a foreign country does not take measures that correspond to the eight principles of the OECD privacy guideline (including measures related to response for requests based on the rights of the person), information by which the person can reasonably recognize the content of the said measures that are not being taken shall be provided.

Note that a third party, who is the recipient, in a foreign country takes all the measures that correspond to the eight principles of the OECD privacy guideline, it is sufficient so long as the person is informed of that.

For handling of cases in which information related to measures for the protection of personal information taken by a third party, who is the recipient, in a foreign country cannot be provided
when obtaining the consent of the person approving the provision of personal data to a third party in a foreign country, refer to 5-3-2 (Cases in Which Information Related to Measures for the Protection of Personal Information Taken by a Third Party, Who is the Recipient, Cannot be Provided)

[Cases corresponding to the provision of information related to measures for the protection of personal information taken by a third party, who is the recipient, in a foreign country (cases in which a third party, who is the recipient, does not notify or publicly disclose utilization purposes)]

Case) To provide information to the effect that “although the recipient takes measures that are roughly of the same standard as the measures required of a business operator handling personal information in Japan with respect to the handling of personal data, the recipient does not notify or publicly disclose utilization purposes regarding obtained personal information”

5-3 Handling of Cases in Which Destination of Transfer Cannot Be Specified at the Time of Acquiring Consent (Related to Article 17(3) and (4) of the Rules)

5-3-1 Cases in Which a Foreign Country Where a Third Party Who is the Recipient Cannot be Specified (Related to Article 17(3) of the Rules)

Cases in which a business operator handling personal information cannot specify the foreign country where a third party, who is the recipient, is located at the time of attempting to obtain the consent of the person approving the provision of personal data to a third party in a foreign country under the stipulations of Article 28(1) of the Act, the business operator handling personal information shall provide the following information of 1 and 2 in place of the name of the said foreign country and the information of on the policies related to the protection personal information of the said foreign country.

Note that, in cases in which a foreign country where a third party, who is the recipient, is specified later, it is preferred to provide information in accordance with the request of the person.

[Cases corresponding to cases in which a foreign country where a third party, who is the recipient, cannot be specified]
Case 1) When a pharmaceutical company in Japan researches and developments medicines or the like, a case in which a foreign country to which the personal data of the said test subject will be provided cannot be specified due to the pharmaceutical company not having decided a reviewing authority of which country to apply for approval at the time a principal investigator or the like provides explanation and obtain consent from a test subject.

Case 2) When an insurance company in Japan assumes reinsurance from a reinsurance company in view of the distribution of underwriting risk, a case in which a foreign country to which personal data of a customer will be provided cannot be specified due to the insurance company not having decided from which reinsurance company to assume reinsurance at the time of underwriting and obtaining consent from the customer.

Inability to specify and reasons thereof (Related to Item 1 of Article 17(3) of the Rules)

Even in cases in which a foreign country where a third party, who is recipient, is located cannot be specified, in view of the purport of increasing the possibility for the person to predict the risk involved in transferring personal data across the border, a business operator handling personal information shall provide information to the effect that a foreign country where a third party, who is recipient, is located cannot be specified and the reason thereof.

Note that, when providing information, it is preferred that a specific explanation is provided as to in what situation personal data is provided to a third party in a foreign country.

Information to be useful for the person in place of the name of a foreign country where a third party, who is the recipient, is located (related to Item 2 of Article 17(3) of the Rules)

Even when a foreign country where a third party, who is the recipient, is located cannot be specified, if it is possible to provide information to be useful for the person in place of the name of a foreign country where a third party, who is the recipient, is located, the said information shall also be provided to the person.

It is necessary to separately determine the correspondence to "information to be useful for the person in place of the name of a foreign country where a third party, who is the recipient, is located" taking the purport of the policy that requires the provision of information to the person into account. For example, in cases in which a specific range of foreign countries to be the destination of transfer has been determined, the information related to the said range corresponds to the "information to be useful for the person in place of the name of a foreign country where a third party, who is the recipient, is located" described herein.
[Cases corresponding to information to be useful for the person in place of the name of a foreign country where a third party, who is the recipient, is located]
Case) In a case in which specific candidates for foreign countries to be the destination of transfer is determined at the time of trying to obtain the consent of the person, the names of countries that are the said candidates

5-3-2 Cases in Which Information Related to Measures for the Protection of Personal Information Taken by a Third Party, Who is the Recipient, Cannot be Provided (Related to Article 17(4) of the Rules)

In cases in which information related to measures for the protection of personal information taken by a third party, who is the recipient, in a foreign country cannot be provided at the time of attempting to obtain the consent of the person approving the provision of personal data to a third party in a foreign country under the stipulations of Article 28(1) of the Act, a business operator handling personal information shall provide information to the effect that the said information cannot be provided and the reason thereof in place of the said information.

Note that, when providing information, it is preferred that a specific explanation is provided as to in what situation personal data is provided to a third party in a foreign country.

In addition, in cases in which it has later become possible to provide information regarding measures for the protection of personal information taken by a third party, who is the recipient, in foreign country, it is preferred to provide information in accordance with the request of the person.

[Cases corresponding to cases in which information related to measures for the protection of personal information taken by a third party, who is the recipient, in a foreign country cannot be provided]
Case 1) When a pharmaceutical company in Japan researches and developments medicines or the like, a case in which the recipient of the personal data of the said test subject cannot be specified due to the pharmaceutical company not having decided a reviewing authority of which country to apply for approval at the time a principal investigator or the like provides explanation and obtain consent from a test subject
Case 2) When an insurance company in Japan assumes reinsurance from a reinsurance
company in view of the distribution of underwriting risk, a case in which the recipient of personal data of a customer cannot be specified due to the insurance company not having decided from which reinsurance company to assume reinsurance at the time of underwriting and obtaining consent from the customer.

6 Measures to be Taken In Cases In Which Personal Data Has Been Provided to Those That Have Prepared a System Necessary for Continuously Taking Measures That Correspond to Measures That Should be Taken by Business Operators Handling Personal Information

In cases in which a business operator handling personal information provides personal data to a third person in a foreign country that has prepared a system conforming to the standard defined in Article 16 of the Rules (hereinafter referred to as the “standard conforming system”), the business operator handling personal information shall take measures that are necessary for ensuring the continuous implementation of corresponding measures (referring to measures corresponding to measures that should be taken by business operators handling personal information under the stipulations of Section 2, Chapter 4 of the Act regarding the handling of personal data; hereinafter the same) by the said third party in a foreign country and provide the person with information related to the said necessary measures in accordance with the said person’s request (Article 28(3) of the Act) (*1) (*2).

Article 28(3) of the Act specifies that, in cases in which personal data is provided to a third party in a foreign country on the grounds of the recipient preparing the standard conforming system, from thereon, a business operator handling personal information has a duty to continuously ensure the proper handling of the said personal data by the said third party. Therefore, it is necessary for a business operator handling personal information to take measures based on Article 28(3) as long as the handling of the said personal data by the said third party continues.

However, in view of the above purport of the policy, in cases in which a business operator handling personal information provides personal data to a third party in a foreign country on
the grounds of the consent of the person, for example, even in cases in which the said third party has prepared the standard conforming system, the measures based on Article 28(3) is not required.

(*1) The stipulations of Article 24(3) of the Act (Article 28(3) of the current Act) applies to cases in which a business operator handling personal information provides personal data to a third party in a foreign country stipulated under the same paragraph on or after the date of enactment of the 2020 Amendment Act (Article 4(2) of supplementary provisions of the 2020 Amendment Act).

(*2) The stipulation of Article 28(3) of the Act applies to cases in which a corporation or the like of the attached Table 2 (refer to 2-1 (Consent From the Person to the Effect that They Approve of Provision of Personal Data to Third Parties in Foreign Country)) provides data to a third party in a foreign country stipulated under the same paragraph on or after the date of enactment of the 2021 Amendment Act (Article 7(7) of supplementary provisions of the 2021 Amendment Act).

6-1 Measures that are Necessary for Ensuring the Continuous Implementation of Corresponding Measure (Related to Article 18(1) of the Rules)

In cases of providing personal data to a third party in a foreign country on the grounds of the recipient preparing the standard conforming system, a business operator handling personal information shall take the measures in the following (1) and (2) as measures that are necessary for ensuring the continuous implementation of corresponding measures by the said third party in a foreign country.

Periodically confirm by a proper and reasonable method the presence or absence of a system of the said foreign country that is likely to affect the state of implementation of the corresponding measure and the implementation of the corresponding measure by the said third party and the content thereof (related to Item 1 of Article 18(1) of the Rules)

A business operator handling personal information shall periodically confirm by a proper and reasonable method the presence or absence of a system of the said foreign country that is likely to affect the state of implementation of the corresponding measure and the implementation of the corresponding measure by the said third party, who is the recipient of
personal data, and the content thereof.

“Periodically confirm” here refers to executing confirmation approximately once a year or more frequently than that.

It is necessary to confirm by a proper and reasonable method the state of implementation of the corresponding measure in accordance with the content and scale of personal data to be provided to a third party in a foreign country. For example, it is conceivable to perform confirmation by visiting, as necessary, the location at which personal data is handled or a reasonable alternative method (including oral confirmation) (*).

[Cases corresponding to confirmation of the state of implementation of the corresponding measure]

Case 1) When entrusting a business operator in a foreign country with the handling of personal data, in a case in which the standard conforming system of the corresponding recipient is prepared by concluding an agreement between the provider and the recipient, confirming the state of execution of the said agreement

Case 2) When transferring personal data within the same corporate group, in a case in which the standard conforming system of the corresponding recipient is prepared by a privacy policy that is applied in common to the provider and the recipient, confirming the state of execution of the said privacy policy

In addition, it is necessary to confirm the presence or absence of a system of the said foreign country that is likely to affect the state of implementation of the corresponding measure and the implementation of the corresponding measure by the said third party and the content thereof by a proper and reasonable method with a general level of attentiveness. For example, a method of querying the said third party and a method of confirming information that has been publicly disclosed by an administrative institution or the like of Japan or a foreign country are conceivable.

[Cases corresponding to a system of a foreign country that is likely to affect the state of implementation of a corresponding measure]

Case 1) A system that makes it possible for a government to extensively collect information regarding personal information held by a business operator by the government imposing a duty of extensive cooperation in information collection activities on the business operator

Case 2) A system pertaining to the duties of storing, in Japan, personal information for which
there is a risk that a business operator may not be able to respond to a request of deletion or the like from the person

(*) A target of implementation of a corresponding measure at a third party, who is the recipient, in a foreign country is “personal data”. Therefore, when confirming the state of execution of a corresponding measure, it is not required to execute confirmation regarding the handling of other personal information being handled by the recipient.

When the implementation of a corresponding measure by the said third party has been impeded, a necessary and proper measure shall be taken and when it becomes difficult to ensure the continuous implementation of the said corresponding measure, provision of personal data to the said third party shall be stopped (related to Item 2 of Article 18(1) of the Rules)

When the implementation of a corresponding measure by the said third party, who is the recipient of personal data, has been impeded, a business operator handling personal information shall take necessary and proper measures to resolve or improve the said impedance.

[Cases corresponding to necessary and proper measures when there is an impedance]

Case) When a business operator handling personal information in Japan prepares the standard conforming system of the corresponding recipient by concluding a trust agreement with a business operator in a foreign country, who is the recipient, in a case where the said recipient is handling personal data in violation of a party of the duties in the said trust agreement, requesting to correct this

In addition, in cases in which it has become difficult to ensure the continuous implementation of a corresponding measure by a third party in a foreign country, it is considered that it cannot be said that the said third party has substantially prepared the standard conforming system. Therefore, the provision of personal data to the said third party shall be stopped thereafter.

[Cases corresponding to cases in which it has become difficult to ensure the continuous implementation of a corresponding measure]

Case 1) When a business operator handling personal information in Japan prepares the standard conforming system of the corresponding recipient by concluding a trust agreement with a business operator in a foreign country, who is the recipient, in a case where the said recipient is handling personal data in violation of a party of the duties in the said trust agreement, despite a request being made to correct this, a case in which the recipient does not correct this within a reasonable period
Case 2) In a case in which, after there has been a serious leakage pertaining to personal data that has been provided by a business operator handling personal information in Japan at a business operator in a foreign country, necessary and proper measures for preventing the occurrence of similar leaks have not been taken.

6-2 Provision of Information Related to Measures that are Necessary for Ensuring the Continuous Implementation of Corresponding Measure (Related to Article 18(2) and (3) of the Rules)

6-2-1 Method of Providing Information (Related to Article 18(2) of the Rules)

It is necessary that the provision of information to the person is performed in a proper method by which it is considered that the person can soundly recognize the information that needs to be provided to the person under the stipulations of Article 18(3) of the Rules. Note that it is important that the information to be provided is easy to understand for the person.

[Cases corresponding to a proper method]

Case 1) Method of transmitting necessary information to the person by electronic email
Case 2) Method of directly issuing a document noting necessary information to the person
Case 3) Method of orally explaining necessary information to the person
Case 4) Method of posting necessary information on a home page and prompting the person to view it

6-2-2 Information That Should be Provided (Related to Article 18(3) of the Rules)

In cases in which a request by the person under the stipulation of Article 28(3) of the Act has been received, a business operator handling personal information shall provide the person with information of the following (1) to (7).

However, in cases in which providing information is likely to significantly impede the proper execution of the affairs of the business operator handling personal information, it is possible not to provide the information in whole or in part.
[Cases corresponding to cases in which providing information is likely to significantly impede the proper execution of the affairs of the business operator handling personal information]

Case) A case that is likely to significantly impede affairs, such as when the work of responding to inquiries become backlogged due to the inquiry desk substantially becoming occupied by the same person repeatedly requesting the provision of information regarding the same content, which requires a complex response

“Method of preparing a system stipulated under Article 28(1) of the Act by a corresponding third party” (Related to Item 1 of Article 18(3) of the Rules)

Information shall be provided regarding a method by which a third party, who is the recipient of personal data, in a foreign country prepares the standard conforming system.

[Cases corresponding to the provision of information regarding a method of preparing the standard conforming system]

When a business operator handling personal information in Japan entrusts the handling of personal data to a business operator in a foreign country, a case in which the standard conforming system of the corresponding recipient is prepared by concluding an agreement between the provider and the recipient

Case) Providing information to the effect of an “agreement with the recipient”

“Overview of a corresponding measure to be implemented by a corresponding third party” (Related to Item 2 of Article 18(3) of the Rules)

Information shall be provided regarding an overview of a corresponding measure to be implemented by a third party, who is the recipient of personal data, in a foreign country. Information that should be provided shall be determined for each individual case. It is necessary to provide information by which it can be known how the measures conforming to the purport of stipulations under Section 2, Chapter 4 of the Act are being ensured at the said third party in a foreign country.

Note that it is not required to provide information regarding an overview of all the stipulations of an agreement or the like that has been concluded between a business operator handling personal information and the said third party in a foreign country.

[Cases corresponding to the provision of information regarding an overview of a corresponding measure]

When a business operator handling personal information in Japan entrusts the handling of personal data to a business operator in a foreign country, a case in which the standard
conforming system of the corresponding recipient is prepared by concluding an agreement between the provider and the recipient

Case) Provide information to the effect that “personal data is handled within a range of specified utilization purposes, improper utilization is prohibited, necessary and proper safety control measures are taken, necessary and proper supervision of employees is executed, re-entrustment is prohibited, the recipient reports to Personal Information Protection Commission and notifies the person in cases leakage or the like has occurred, provision of personal data to a third party is prohibited, and the like are defined in an agreement” “Frequency and method of confirmation under the stipulation of Item 1 of Paragraph 1” (Related to Item 3 of Article 18(3) of the Rules)

Information shall be provided regarding the method and frequency of confirmation for the presence or absence of a system that is likely to affect the state of implementation of a corresponding measure and the implementation of the corresponding measure by a third party, who is the recipient of personal data, in a foreign country and the content thereof.

Note that, in cases in which the method and frequency of confirmation of the state of implementation of a corresponding measure by a third party in a foreign country and the method and frequency of confirmation of the presence or absence of a system that is likely to affect the state of implementation of the corresponding measure and the content thereof are different, it is necessary to provide information for each.

[Cases corresponding to the provision of information regarding the method and frequency of confirmation]

Cases)

① Method and frequency of confirmation regarding the state of implementation of a corresponding measure by a third party in a foreign country

Provide information to the effect that “confirmation is executed annually by written report”

② Method and frequency of confirmation of the presence or absence of a system that is likely to affect the state of implementation of the corresponding measure and the content thereof

Provide information to the effect that “information publicly disclosed by a governing body of Japan is confirmed annually”

“Name of a corresponding foreign country” (Related to Item 4 of Article 18(3) of the Rules)

Information shall be provided regarding the name of a foreign country (*1) where a third party, who is the recipient of personal data, is located (*2) The official name is not necessarily
required. However, information shall be provided in a form by which the person can reasonably recognize the transfer destination of their personal data.

(*1) A “foreign country” refers to a country or region that is outside the region of Japan and excludes those defined under the Rules as foreign countries that have a policy on the protection of personal information recognized to be of the same standard as Japan (Article 28(1) of the Act).

(*2) Regarding the provision of information of the “name of a foreign country” here, it is sufficient so long as a name of a foreign country where a third party, who is the recipient, is located is indicated. It is not necessary to additionally indicate a name of a state or the like where the said third party is located. However, in view of the purport of a system to enable the person to understand the state of handling of their personal data at a third party in a foreign country, in cases in which provision of information related to state laws contributes to the person’s understanding of the state or the like of handling of personal data at the said third party, such as a case in which there is a system that is likely to affect the state of implementation of the corresponding measure by a third party in a foreign country in the state laws, it is preferred that information is provided also regarding the said system after indicating the state where the said third party is located.

“Presence or absence of a system of a corresponding foreign country that is likely to affect the implementation of a corresponding measure by a corresponding third party and the overview thereof” (Related to Item 5 of Article 18(3) of the Rules)
Information shall be provided regarding the presence or absence of a system of a foreign country that is likely to affect the implementation of a corresponding measure by a third party, who is the recipient of personal data, in the said foreign country and the overview thereof.

Cases corresponding to the provision of information regarding an overview of a system of a foreign country that is likely to impede the implementation of a corresponding measure

Case 1) Provide information to the effect that “there is a system that makes it possible for a government to extensively collect information regarding personal information held by a business operator by the government imposing a duty of extensive cooperation in information collection activities on the business operator”

Case 2) Provide information to the effect that “there is a system pertaining to the duties of storing, in Japan, personal information for which there is a risk that a business operator may not be able to respond to a request of deletion or the like from the
Information shall be provided regarding the presence or absence of impedance related to the execution of a corresponding measure by a third party, who is the recipient of personal data, in a foreign country and the overview thereof.

Cases corresponding to the provision of information regarding the impedance related to the implementation of a corresponding measure

When a business operator handling personal information in Japan entrusts the handling of personal data to a business operator in a foreign country, cases in which, despite preparing the standard conforming system of the said recipient by concluding an agreement between the provider and the recipient, the said recipient has handled the said personal data beyond the range of utilization purposes specified in the said agreement

Case 1) Provide information to the effect that “the recipient has handled personal data beyond the range of utilization purposes specified in an agreement”

“Overview of measures to be taken by a corresponding business operator handling personal information under the stipulation of Item 2 of Paragraph 1 regarding the impedance of the previous item” (Related to Item 7 of Article 18(3))

When the implementation of a corresponding measure by the said third party, who is the recipient of personal data, has been impeded, information shall be provided regarding the overview of measures to be taken by a business operator handling personal information, who is the provider, to resolve or improve the said impedance.

Cases corresponding to the provision of information regarding the overview of measure to be taken by a business operator handling personal information regarding impedance related to the execution of a corresponding measure

When a business operator handling personal information in Japan entrusts the handling of personal data to a business operator in a foreign country, cases in which, despite preparing the standard conforming system of the said recipient by concluding an agreement between the provider and the recipient, the said recipient has handled the said personal data beyond the range of utilization purposes specified in the said agreement

Case 1) Provide information to the effect that “since the recipient has been handling personal data beyond the range of utilization purposes specified in an agreement, request
has been made to immediately correct the said handling"

Case 2) Provide information to the effect that "since the recipient has been handling personal data beyond the range of utilization purposes specified in an agreement, request has been made to immediately correct the said handling; however, this has not been corrected within a reasonable period, and it is difficult to ensure the continuous implementation of a corresponding measure; therefore, provision of data has been stopped on and after Month Day, Year and a request has been made to delete the personal data that has already been provided"

6-2-3 Notification or the Like for At the Time of Decision to the Effect of Not Providing Information (Related to Article 18(4) and (5) of the Rules)

When deciding not to provide information in whole or in part pertaining to a request by the person under the stipulation of Article 28(3), a business operator handling personal information shall notify the person (*) of that without delay.

In this case, the business operator handling personal information shall endeavor to explain the reason for not providing information to the person.

(*) Regarding “notifying the person”, refer to the General Rule Guideline “2-14 (Notifying the Person)”. 