Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU and the United Kingdom based on an Adequacy Decision

Table of Contents

[Terms]

“Act”	The Act on the Protection of Personal Information (Act No. 57, 2003)
“Cabinet Order”	Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507, 2003)
“Order”	Enforcement Rules for the Act on the Protection of Personal Information (Order of the Personal Information Protection Commission No. 3, 2016)
"General Rules Guidelines"	Guidelines for the Act on the Protection of Personal Information (Volume on General Rules) (Notice of the Personal Information Protection Commission No. 6, 2015)
“EU”	European Union, including its Member States and, in the light of the EEA Agreement, Iceland, Liechtenstein and Norway
“GDPR”	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）
“UK GDPR”	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation)
“adequacy decision”	The European Commission’s decision that a third country or a territory within that third country, etc. ensures an adequate level of protection of personal data pursuant to Article 45 of the GDPR and the corresponding decision of the government of the United Kingdom

The Personal Information Protection Commission, for the purpose of conducting mutual and smooth transfer of personal data between Japan and the EU, designated the EU as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests based on Article 28 of the Act and the European Commission concurrently decided that Japan ensures an adequate level of protection of personal data pursuant to Article 45 of the GDPR.

Hereby, mutual and smooth transfer of personal data will be conducted between Japan and the EU in a way that ensures a high level of protection of an individual's rights and interests. Based on the Basic Policy on the Protection of Personal Information, in order to ensure that high level of protection regarding personal information received from the EU based on an adequacy decision and in light of the fact that, despite a high degree of convergence between the two systems, there are some relevant differences, the Personal Information Protection Commission has adopted these Supplementary Rules, based on the provisions of the Act concerning implementation etc. of cooperation with the governments in other countries and in view of ensuring appropriate handling of personal information received from the EU based on an adequacy decision by a business handling personal information and proper and effective implementation of the obligations laid down in such rules (*1).

In particular, Article 6 of the Act provides for the power to take necessary legislative and other action with a view to ensure the enhanced protection of personal information and construct an internationally conformable system concerning personal information through stricter rules that supplement and go beyond those laid down in the Act and the Cabinet Order. Therefore, the Personal Information Protection Commission, as the authority competent for governing the overall administration of the Act, has the power to establish pursuant to Article 6 of the Act stricter regulations by formulating the present Supplementary Rules providing for a higher level of protection of an individual's rights and interests regarding the handling of personal data received from the EU based on an adequacy decision, including with respect to the definition of sensitive personal information pursuant to Article 2, paragraph (3) of the Act.

On this basis, the Supplementary Rules are binding on a business handling personal information that receives personal data transferred from the EU based on an adequacy decision which is thus required to comply with them. As legally

binding rules, any rights and obligations are enforceable by the Personal Information Protection Commission in the same way as the provisions of the Act that they supplement with stricter and/or more detailed rules. In case of infringement of the rights and obligations resulting from the Supplementary Rules, individuals can also obtain redress from courts in the same way as with respect to the provisions of the Act that they supplement with stricter and/or more detailed rules.

As regards enforcement by the Personal Information Protection Commission, in case a business handling personal information does not comply with one or several obligations under the Supplementary Rules, the Personal Information Protection Commission has the power to adopt measures pursuant to Article 148 of the Act. Regarding generally personal information received from the EU based on an adequacy decision, failure by a business handling personal information to take action in line with a recommendation received pursuant to Article 148, paragraph (1) of the Act, without legitimate ground (*2), is considered as a situation where ”a serious infringement of an individual’s rights and interests is impending” within the meaning of Article 148, paragraph (2) of the Act.

The Supplementary Rules also apply to handling of personal data received from the United Kingdom based on an adequacy decision after the United Kingdom left the EU.

(*1) Article 4, Article 6, Article 9, Article 28, Article 131 and Article 172 of the Act, and Article 15 of the Order.

(*2) Legitimate ground shall be understood as meaning an event of an extraordinary nature outside the control of the business handling personal information which cannot be reasonably foreseen (for example, natural disasters) or when the necessity to take action concerning a recommendation issued by the Personal Information Protection Commission pursuant to Article 148, paragraph (1) of the Act has disappeared because the business handling personal information has taken alternative action that fully remedies the violation.

(1) Sensitive personal information (Article 2, paragraph (3) of the Act)

Article 2 (paragraph (3)) of the Act

(3) "Sensitive personal information" in this Act means personal information as to an identifiable person's race, creed, social status, medical history, criminal record, the fact of having suffered damage by a crime, or other identifiers or their equivalent prescribed by Cabinet Order as those of requiring special care so as not to cause unjust discrimination, prejudice or other disadvantages to that person.

Article 2 of the Cabinet Order

Those descriptions etc. prescribed by cabinet order under Article 2, paragraph (3) of the Act shall be those descriptions etc. which contain any of those matters set forth in the following (excluding those falling under a principal's medical record or criminal history)

(i) the fact of having physical disabilities, intellectual disabilities, mental disabilities (including developmental disabilities), or other physical and mental functional disabilities prescribed by Order of the Personal Information Protection Commission;

(ii) the results of a medical check-up or other examination (hereinafter referred to as a "medical check-up etc." in the succeeding item) for the prevention and early detection of a disease conducted on a principal by a medical doctor or other person engaged in duties related to medicine (hereinafter referred to as a "doctor etc." in the succeeding item);

(iii) the fact that guidance for the improvement of the mental and physical conditions, or medical care or prescription has been given to a principal by a doctor etc. based on the results of a medical check-up etc. or for reason of disease, injury or other mental and physical changes;

(iv) the fact that an arrest, search, seizure, detention, institution of prosecution or other procedures related to a criminal case have been carried out against a principal as a suspect or defendant;

(v) the fact that an investigation, measure for observation and protection, hearing and decision, protective measure or other procedures related to a juvenile protection case have been carried out against a principal as a juvenile delinquent or a person suspected thereof under Article 3, paragraph (1) of the Juvenile Act.

Article 5 of the Order

Physical and mental functional disabilities prescribed by Order of the Personal Information Protection Commission under Article 2, item (i) of the Cabinet Order shall be those disabilities set forth in the following.

(i) physical disabilities set forth in an appended table of the Act for Welfare of Persons with Physical Disabilities (Act No.283 of 1949)

(ii) intellectual disabilities referred to under the Act for the Welfare of Persons with Intellectual Disabilities (Act No.37 of 1960)

(iii) mental disabilities referred to under the Act for the Mental Health and Welfare of the Persons with Mental Disabilities (Act No.123 of 1950) (including developmental disabilities prescribed in Article 2, paragraph (1) of the Act on Support for Persons with Development Disabilities, and excluding intellectual disabilities under the Act for the Welfare of Persons with Intellectual Disabilities)

(iv) a disease with no cure methods established thereof or other peculiar diseases of which the severity by those prescribed by cabinet order under Article 4, paragraph (1) of the Act on Comprehensive Support for Daily and Social Lives of Persons with Disabilities (Act No. 123 of 2005) is equivalent to those prescribed by the competent ministers under the said paragraph

If personal data received from the EU or the United Kingdom based on an adequacy decision contains data concerning a natural person's sex life or sexual orientation or trade-union membership, which are defined as special categories of personal data under the GDPR and the UK GDPR, businesses handling personal information are required to handle that personal data in the same manner as sensitive personal information within the meaning of Article 2, paragraph (3) of the Act.

(2) Specifying the purpose of use, restriction due to purpose of use (Article 17, paragraph (1), Article 18, paragraph (1) and Article 30, paragraphs (1) and (3) of the Act)

Article 17 (paragraph (1)) of the Act

(1) In handling personal information, the business handling personal information must specify as much as possible the purpose for which it uses that information (hereinafter referred to as the "purpose of use").

Article 18 (paragraph (1)) of the Act

(1) A business handling personal information must not handle personal information beyond the scope necessary for achieving the purpose of use specified pursuant to the provisions of the preceding Article without obtaining the identifiable person's consent to do so in advance.

Article 30 (paragraphs (1) and (3)) of the Act

(1) When receiving personal data from a third party, businesses handling personal information must confirm matters set forth in the following pursuant to Order of the Personal Information Protection Commission; provided, however, that this does not apply to cases in which the provision of personal data falls under any of the items of Article 27, paragraph (1) or paragraph (5):

(i) (omitted)

(ii) background of the acquisition of the personal data by the third party.

(3) When having given confirmation under paragraph (1), a business handling personal information must prepare a record pursuant to Order of the Personal Information Protection Commission on the date when it received the personal data, matters concerning the confirmation, and other matters prescribed by Order of the Personal Information Protection Commission.

If businesses handling personal information handle personal information beyond the necessary scope to achieve the purpose of use specified under Article 17, paragraph (1) of the Act, they shall obtain the relevant principal's consent in advance (Article 18, paragraph (1) of the Act). When receiving the provision of personal data from a third party, businesses handling personal information shall, pursuant to the Order, confirm matters such as the

circumstances under which the said personal data was acquired by the said third party, and record these matters (Article 30, paragraphs (1) and (3) of the Act).

In the case where a business handling personal information receives personal data from the EU or the United Kingdom based on an adequacy decision, the circumstances regarding the acquisition of the said personal data which shall be confirmed and recorded as prescribed by Article 30, paragraphs (1) and (3), include the purpose of use for which it was received from the EU or the United Kingdom.

Similarly, in the case where a business handling personal information receives from another business handling personal information personal data previously transferred from the EU or the United Kingdom based on an adequacy decision, the circumstances regarding the acquisition of the said personal data which shall be confirmed and recorded as prescribed by Article 30, paragraphs (1) and (3), include the purpose of use for which it was received.

In the above-mentioned cases, the business handling personal information is required to specify the purpose of utilizing the said personal data within the scope of the purpose of use for which the data was originally or subsequently received, as confirmed and recorded pursuant to Article 30, paragraphs (1) and (3), and utilize that data within the said scope (as prescribed by Articles 17, paragraph (1) and Article 18, paragraph (1) of the Act).

(3) Restriction on provision to a third party in a foreign country (Article 28 of the Act; Article 16 of the Order)

Article 28 of the Act

(1) Except cases set forth in the items of paragraph (1) of the preceding Article, before businesses handling personal information provide personal data to a third party (excluding a person that establishes a system that conforms to standards prescribed by Order of the Personal Information Protection Commission as necessary for continuously taking measures equivalent to those that a business handling personal information must take concerning the handling of personal data pursuant to the provisions of this Section (referred to as "equivalent measures" in paragraph (3)); hereinafter the same applies in this paragraph, the following paragraph and Article 31, paragraph (1), item(ii)) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same applies in this Article and Article 31, paragraph (1), item (ii)) (excluding those prescribed by Order of the Personal Information Protection Commission as a foreign country that has established a personal information protection system recognized to have equivalent standards to that in Japan regarding the protection of individual rights and interests; hereinafter the same applies in this Article and Article 31, paragraph (1), item (ii)), the businesses must obtain an identifiable person's consent to the effect that the person approves the provision to a third party in a foreign country. In this case, the provisions of the preceding Article do not apply.

(2) Before intending to obtain the identifiable person's consent pursuant to the provisions of the preceding paragraph, businesses handling personal information must provide that person with information on the personal information protection system of the foreign country, on the measures the third party takes for the protection of personal information, and other information that is to serve as a reference to that person, pursuant to Order of the Personal Information Protection Commission.

(3) When having provided personal data to a third party (limited to a person establishing a system prescribed in paragraph (1)) in a foreign country, businesses handling personal information must take necessary measures to ensure continuous implementation of the equivalent measures by the third party, and provide information on the necessary measures to the

identifiable person at the request of that person, pursuant to Order of the Personal Information Protection Commission.

Article 16 of the Order

Standards prescribed by Order of the Personal Information Protection Commission under Article 28, paragraph (1) of the Act are to be falling under any of each following item.

(i) a business handling personal information and a person who receives the provision of personal data have ensured in relation to the handling of personal data by the person who receives the provision the implementation of measures in line with the purport of the provisions under Chapter IV, Section 2 of the Act by an appropriate and reasonable method

(ii) a person who receives the provision of personal data has obtained a recognition based on an international framework concerning the handling of personal information

A business handling personal information, in cases of providing a third party in a foreign country with personal data that it has received from the EU or the United Kingdom based on an adequacy decision, shall obtain in advance a principal's consent to the effect that he or she approves the provision to a third party in a foreign country pursuant to Article 28 of the Act, excluding the cases falling under one of the following (i) through (iii).

(i) when the third party is in a country prescribed by Order of the Personal Information Protection Commission as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests

(ii) when a business handling personal information and the third party who receives the provision of personal data have, in relation to the handling of personal data by the third party, implemented together measures providing an equivalent level of protection to the Act, read together with the present Rules, by an appropriate and reasonable method (meaning a contract, other forms of binding agreements, or binding arrangements within a corporate group).

(iii) in cases falling under each item of Article 27, paragraph (1) of the Act

(4) Pseudonymized personal information (Article 2, paragraph (5), Article 16, paragraph (5), and Article 41 of the Act)

Article 2 (paragraph (5)) of the Act

(5) "Pseudonymized personal information" in this Act means information relating to an individual that can be prepared in a way that makes it not possible to identify a specific individual unless collated with other information by taking any of the measures prescribed in each following item in accordance with the divisions of personal information set forth in those items:

(i) personal information falling under paragraph (1), item (i): deleting a part of the identifiers or their equivalent contained in the personal information (including replacing the part of the identifiers or their equivalent with other identifiers or their equivalent without following patterns that enable its restoration);

(ii) personal information falling under paragraph (1), item (ii): deleting all individual identification codes contained in the personal information (including replacing the individual identification codes with other identifiers or their equivalent without following patterns that enable restoration of the individual identification codes).

Article 16 (paragraph (5)) of the Act

(5) "Business handling pseudonymized personal information" in this Chapter and Chapters VI and VII means a person that uses a collective body of information consisting of pseudonymized personal information for business, which has been systematically organized to be searchable using a computer or is the equivalent as prescribed by Cabinet Order as systematically organized in order to be easily searchable for particular pseudonymized personal information (referred to as a "pseudonymized personal information database or the equivalent" in Article 41, paragraph (1)); provided, however, that this excludes persons set forth in each item of paragraph (2).

Article 41 of the Act

(1) When preparing pseudonymized personal information (limited to those compiled in a pseudonymized personal information database or the

equivalent; hereinafter the same applies in this Chapter and Chapter VI), businesses handling personal information must process personal information in accordance with standards prescribed by Order of the Personal Information Protection Commission as those necessary to make it impossible to identify a specific individual unless collated with other information.

(2) When having prepared pseudonymized personal information or having acquired pseudonymized personal information and deleted or other related information (meaning information related to identifiers or their equivalent and individual identification codes that were deleted from personal information used to prepare the pseudonymized personal information, and the means of processing carried out pursuant to the provisions of the preceding paragraph; hereinafter the same applies in this Article and paragraph (7) as applied mutatis mutandis pursuant to paragraph (3) of the following Article following the deemed replacement of terms) related to the pseudonymized information, businesses handling personal information must take measures for the management of the security of deleted or other related information in accordance with standards prescribed by Order of the Personal Information Protection Commission as those necessary to prevent the leaking of deleted or other related information.

(3) Notwithstanding the provision of Article 18 and except cases based on laws and regulations, a business handling pseudonymized personal information (limited to a business handling personal information; hereinafter the same applies in this Article) must not handle pseudonymized personal information (limited to personal information; hereinafter the same applies in this Article) beyond the necessary scope to achieve the purpose of use specified pursuant to the provisions of Article 17, paragraph (1).

(4) With regard to applying the provisions of Article 21 related to pseudonymized personal information, the phrase "notify the identifiable person of that purpose of use or disclose this to the public" in paragraphs (1) and (3) of that Article is deemed to be replaced with "disclose that purpose of use"; the phrase "notifying the identifiable person of the purpose of use or disclosing this to the public" in the provisions of items (i) through (iii) of paragraph (4) of that Article is deemed to be replaced with "disclosing the purpose of use".

(5) Businesses handling pseudonymized personal information must endeavor to erase personal data that constitutes pseudonymized personal information

and deleted or other related information without delay when utilization of the personal data and the deleted or other related information has become unnecessary. In this case, the provisions of Article 22 do not apply.

(6) Notwithstanding the provisions of Article 27, paragraphs (1) and (2), and Article 28, paragraph (1), and except cases based on laws and regulations, businesses handling pseudonymized personal information must not provide a third party with personal data that constitutes pseudonymized personal information. In this case, the term "each preceding paragraph" in Article 27, paragraph (5) is deemed to be replaced with "Article 41, paragraph (6)"; the phrase "notifies the person identifiable by that data of this in advance as well as the details of that data, the extent of the joint users, the users' purpose of use, and the name and address of the person responsible for managing the personal data, and, if the user is corporation, the name of its representative; or the business makes the foregoing information readily accessible to the person identifiable by that data in advance" in item (iii) of that paragraph is deemed to be replaced with "disclose this in advance as well as the details of that data, the extent of the joint users, the users' purpose of use, and the name and address of the person responsible for managing the personal data, and, if the user is corporation, the name of its representative"; the phrase "notify the person identifiable by that data of this or make this readily accessible to the person identifiable by that data, without delay" in Article 27, paragraph (6) is deemed to be replaced with "disclose this without delay"; the phrase "any of the items of Article 27, paragraph (1) or paragraph (5) (or any of the items of Article 27, paragraph (1), in cases of a provision of personal data under paragraph (1) of the preceding Article)" in the proviso of Article 29, paragraph (1), and the term "any of the items of Article 27, paragraph (1) or paragraph (5)" in the proviso of Article 30, paragraph (1) are deemed to be replaced with "cases based on laws and regulations or any of the items of Article 27, paragraph (5)".

(7) Businesses handling pseudonymized personal information, in handling that information, must not collate the pseudonymized personal information with other information in order to identify a person identifiable by personal information that was used to prepare the pseudonymized personal information.

(8) Businesses handling pseudonymized personal information, in handling that information, must not use contact addresses and other information contained

in the pseudonymized personal information for telephoning, for sending by mail or by correspondence delivery prescribed in Article 2, paragraph (2) of the Act on Correspondence Delivery by Private Business Operators (Act No. 99 of 2002) conducted by a general correspondence delivery operator prescribed in Article 2, paragraph (6) or a specified correspondence delivery operator prescribed in Article 2, paragraph (9), for delivering a telegram, for transmitting information using a facsimile machine or electronic or magnetic means (meaning means that use electronic data processing system or means that utilize other information communication technology as prescribed by Order of the Personal Information Protection Commission), or for visiting a residence.

(9) The provisions of Article 17, paragraph (2), Article 26 and Articles 32 through 39 do not apply regarding pseudonymized personal information, personal data that constitutes pseudonymized personal information, and personal data the business holds that constitutes pseudonymized personal information.

Pseudonymized personal information acquired by processing personal information received from the EU or the United Kingdom based on an adequacy decision will be processed pursuant to Article 41. Furthermore, the pseudonymized personal information will be processed only for statistical purposes. In this case, statistical purposes means any processing for statistical surveys or for the production of statistical results, which will be aggregate data and shall not be used in support of measures or decisions regarding any particular individual.

(5) Anonymized personal information (Article 2, paragraph 6 and Article 43, paragraphs (1) and (2) of the Act)

Article 2 (paragraph (6)) of the Act

(6) "Anonymized personal information" in this Act means information relating to an individual that can be prepared in a way that makes it not possible to identify a specific individual by taking any of the measures prescribed in each following item in accordance with the divisions of personal information set forth in those items; and also make it not possible to restore that personal information:

(i) personal information falling under paragraph (1), item (i): deleting a part of the identifiers or their equivalent contained in the personal information (including replacing the part of the identifiers or their equivalent with other identifiers or their equivalent without following patterns that enable its restoration);

(ii) personal information falling under paragraph (1), item (ii): deleting all individual identification codes contained in the personal information (including replacing the individual identification codes with other identifiers or their equivalent without following patterns that enable restoration of the individual identification codes).

Article 43 (paragraph (1)) of the Act

(1) When preparing anonymized personal information (limited to those compiled in an anonymized personal information database or the equivalent; hereinafter the same applies in this Chapter and Chapter VI), businesses handling personal information must process personal information in accordance with standards prescribed by Order of the Personal Information Protection Commission as those necessary to make it impossible to identify a specific individual and restore the information to its original state.

Article 34 of the Order

Standards prescribed by Order of the Personal Information Protection Commission under Article 43, paragraph (1) of the Act shall be as follows.

(i) deleting a whole or part of those descriptions etc. which can identify a

specific individual contained in personal information (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the whole or part of descriptions etc.)

(ii) deleting all individual identification codes contained in personal information (including replacing such codes with other descriptions etc. using a method with no regularity that can restore the individual identification codes)

(iii) deleting those codes (limited to those codes linking mutually plural information being actually handled by a business handling personal information) which link personal information and information obtained by having taken measures against the personal information (including replacing the said codes with those other codes which cannot link the said personal information and information obtained by having taken measures against the said personal information using a method with no regularity that can restore the said codes)

(iv) deleting idiosyncratic the identifiers or their equivalent (including replacing such the identifiers or their equivalent with other the identifiers or their equivalent using a method with no regularity that can restore the idiosyncratic the identifiers or their equivalent)

(v) besides action set forth in each preceding item, taking appropriate action based on the results from considering the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information and the identifiers or their equivalent contained in other personal information constituting the personal information database etc. that encompass the said personal information

Article 43 (paragraph (2)) of the Act

(2) When having prepared anonymized personal information, businesses handling personal information must take measures for the management of the security of information relating to identifiers or their equivalent and individual identification codes that were deleted from personal information used to prepare the anonymized personal information, and information on the means of processing carried out pursuant to the provisions of the preceding paragraph, in accordance with standards prescribed by Order of the Personal Information Protection Commission as those necessary to prevent the leaking of that information.

Article 35 of the Order

Standards prescribed by Order of the Personal Information Protection Commission under Article 43, paragraph (2) of the Act shall be as follows.

(i) defining clearly the authority and responsibility of a person handling information relating to identifiers or their equivalent and individual identification codes that were deleted from personal information used to prepare the anonymized personal information and information on the means of processing carried out pursuant to the provisions of Article 43, paragraph (1) (limited to those which can restore the personal information by use of such relating information) (hereinafter referred to as “processing method etc. related information” in this Article.)

(ii) establishing rules and procedures on the handling of processing method etc. related information, handling appropriately processing method etc. related information in accordance with the rules and procedures, evaluating the handling situation, and based on such evaluation results, taking necessary action to seek improvement

(iii) taking necessary and appropriate action to prevent a person with no legitimate authority to handle processing method etc. related information from handling the processing method etc. related information

Personal information received from the EU or the United Kingdom based on an adequacy decision shall only be considered anonymized personal information within the meaning of Article 2, paragraph (6) of the Act if the business handling personal information takes measures that make the de-identification of the individual irreversible for anyone including by deleting processing method etc. related information (meaning information relating to those descriptions etc. and individual identification codes which were deleted from personal information used to produce anonymized personal information and information relating to a processing method carried out pursuant to the provisions of Article 43, paragraph (1) of the Act (limited to those which can restore the personal information by use of such relating information)).