ANNEX 1

SUPPLEMENTARY RULES UNDER THE ACT ON THE PROTECTION OF PERSONAL INFORMATION FOR THE HANDLING OF PERSONAL DATA TRANSFERRED FROM THE EU BASED ON AN ADEQUACY DECISION

[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)
'Rules'	Enforcement Rules for the Act on the Protection of Personal Information (Rules 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. 65, 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)
'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

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 24 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. 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 personal information handling business operator 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 special care-required personal information pursuant to Article 2, paragraph 3, of the Act and

retained personal data pursuant to Article 2, paragraph 7, of the Act (including as to the relevant retention period).

On this basis, the Supplementary Rules are binding on a personal information handling business operator 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 personal information handling business operator 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 42 of the Act. Regarding generally personal information received from the EU based on an adequacy decision, failure by a personal information handling business operator to take action in line with a recommendation received pursuant to Article 42, paragraph 1, of the Act, without legitimate ground[(2)], is considered as a serious infringement of an imminent nature of an individual's rights and interests within the meaning of Article 42, paragraph 2, of the Act.

(1) Special care-required personal information (Article 2, paragraph 3 of the Act)

Article 2 (paragraph 3) of the Act

(3) Special care-required personal information" in this Act means personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.

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 rules 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 Rules

Physical and mental functional disabilities prescribed by rules of the Personal Information Protection Commission under Article 2, item (i) of the 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 Minister of Health, Labor and Welfare under the said paragraph

If personal data received from the EU 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, personal information handling business operators are required to handle that personal data in the same manner as special care-required personal information within the meaning of Article 2, paragraph 3 of the Act.

(2) Retained personal data (Article 2, paragraph 7 of the Act)

Article 2 (paragraph 7) of the Act

(7) 'Retained personal data' in this Act means personal data which a personal information handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of, and which shall be neither those prescribed by cabinet order as likely to harm the public or other interests if their presence or absence is made known nor those set to be deleted within a period of no longer than one year that is prescribed by Cabinet Order.

Article 4 of the Cabinet Order

Those prescribed by cabinet order under Article 2, paragraph 7 shall be those set forth in the following.

(i) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would harm a principal or third party's life, body or fortune;

(ii) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would encourage or induce an illegal or unjust act;

(iii) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would undermine national security, destroy

a trust relationship with a foreign country or international organization, or suffer disadvantage in negotiations with a foreign country or international organization;

(iv) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would hinder the maintenance of public safety and order such as the prevention, suppression or investigation of a crime.

Article 5 of the Cabinet Order

A period prescribed by Cabinet Order under Article 2, paragraph 7 of the Act shall be six months.

Personal data received from the EU based on an adequacy decision is required to be handled as retained personal data within the meaning of Article 2, paragraph 7 of the Act, irrespective of the period within which it is set to be deleted.

If personal data received from the EU based on an adequacy decision falls within the scope of personal data prescribed by Cabinet Order as being "likely to harm the public or other interests if their presence or absence is made known," such data is not required to be handled as retained personal data (see Article 4 of the Cabinet Order; General Rules Guidelines, "2-7. Retained personal data").

(3) Specifying a utilization purpose, restriction due to a utilization purpose (Article 15, paragraph 1, Article 16, paragraph 1 and Article 26, paragraphs 1 and 3 of the Act)

Article 15 (paragraph 1) of the Act

(1) A personal information handling business operator shall, in handling personal information, specify the purpose of utilizing the personal information (hereinafter referred to as a ‘utilization purpose’) as explicitly as possible.

Article 16 (paragraph 1) of the Act

(1) A personal information handling business operator shall not handle personal information without obtaining in advance a principal’s consent beyond the necessary scope to achieve a utilization purpose specified pursuant to the provisions under the preceding Article.

Article 26 (paragraphs 1 and 3) of the Act

(1) A personal information handling business operator shall, when receiving the provision of personal data from a third party, confirm those matters set forth in the following pursuant to rules of the Personal Information Protection Commission. (omitted)

(i) (omitted)

(ii) circumstances under which the said personal data was acquired by the said third party

(3) A personal information handling business operator shall, when having confirmed pursuant to the provisions of paragraph 1, keep a record pursuant to rules of the Personal Information Protection Commission on the date when it received the provision of personal data, a matter concerning the said confirmation, and other matters prescribed by rules of the Personal Information Protection Commission.

If personal information handling business operators handle personal information beyond the necessary scope to achieve a utilization purpose specified under Article 15, paragraph 1 of the Act, they shall obtain the relevant principal's consent in advance (Article 16, paragraph 1 of the Act). When receiving the provision of personal data from a third party, personal information handling business operators shall, pursuant to the Rules, confirm matters such as the circumstances under which the said personal data was acquired by the said third party, and record these matters (Article 26, paragraphs 1 and 3 of the Act).

In the case where a personal information handling business operator receives personal data from the EU 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 26, paragraphs 1 and 3, include the utilization purpose for which it was received from the EU.

Similarly, in the case where a personal information handling business operator receives from another personal information handling business operator personal data previously transferred from the EU 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 26, paragraphs 1 and 3, include the utilization purpose for which it was received.

In the above-mentioned cases, the personal information handling business operator is required to specify the purpose of utilizing the said personal data within the scope of the utilization purpose for which the data was originally or subsequently received, as confirmed and recorded pursuant to Article 26, paragraphs 1 and 3, and utilize that data within the said scope (as prescribed by Articles 15, paragraph 1 and Article 16, paragraph 1 of the Act).

(4) Restriction on provision to a third party in a foreign country (Article 24 of the Act; Article 11-2 of the Rules)

Article 24 of the Act

A personal information handling business operator, except in those cases set forth in each item of the preceding Article, paragraph 1, shall, in case of providing personal data to a third party (excluding a person establishing a system conforming to standards prescribed by rules of the Personal Information Protection Commission as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data pursuant to the provisions of this Section; hereinafter the same in this Article) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same) (excluding those prescribed by rules 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; hereinafter the same in this Article), in advance obtain a principal's consent to the effect that he or she approves the provision to a third party in a foreign country. In this case, the provisions of the preceding Article shall not apply.

Article 11-2 of the Rules

Standards prescribed by rules of the Personal Information Protection Commission under Article 24 of the Act are to be falling under any of each following item.

(i) a personal information handling business operator 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 1 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 personal information handling business operator, in cases of providing a third party in a foreign country with personal data that it has received from the EU 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 24 of the Act, after having been provided information on the circumstances surrounding the transfer necessary for the principal to make a decision on his/her consent, excluding the cases falling under one of the following (i) through (iii).

(i) when the third party is in a country prescribed by the Rules 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 personal information handling business operator 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 23, paragraph 1 of the Act

(5) Anonymously processed information (Article 2, paragraph 9 and Article 36, paragraphs 1 and 2 of the Act)

Article 2 (paragraph 9) of the Act

(9) 'Anonymously processed information' in this Act means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each following item in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information.

(i) personal information falling under paragraph 1, item (i);

Deleting a part of descriptions etc. contained in the said personal information (including replacing the said part of descriptions etc. with other descriptions etc. using a method with no regularity that can restore the said part of descriptions etc.)

(ii) personal information falling under paragraph 1, item (ii);

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

Article 36 (paragraph 1) of the Act

(1) A personal information handling business operator shall, when producing anonymously processed information (limited to those constituting anonymously processed information database etc.; hereinafter the same), process personal information in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to make it impossible to identify a specific individual and restore the personal information used for the production.

Article 19 of the Rules

Standards prescribed by rules of the Personal Information Protection Commission under Article 36, 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 personal information handling business operator) 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 descriptions etc. (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the idiosyncratic descriptions etc.)

(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 descriptions etc. contained in other personal information constituting the personal information database etc. that encompass the said personal information

Article 36 (paragraph 2) of the Act

(2) A personal information handling business operator, when having produced anonymously processed information, shall, in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to prevent the leakage of information relating to those descriptions etc. and individual identification codes deleted from personal information used to produce the anonymously processed information, and information relating to a processing method carried out pursuant to the provisions of the preceding paragraph, take action for the security control of such information.

Article 20 of the Rules

Standards prescribed by rules of the Personal Information Protection Commission under Article 36, paragraph 2 of the Act shall be as follows.

(i) defining clearly the authority and responsibility of a person handling information relating to those descriptions etc. and individual identification codes which were deleted from personal information used to produce anonymously processed information and information relating to a processing method carried out pursuant to the provisions of Article 36, 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 based on an adequacy decision shall only be considered anonymously processed information within the meaning of Article 2, paragraph 9 of the Act if the personal information handling business operator 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 anonymously processed information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph 1 of the Act (limited to those which can restore the personal information by use of such relating information)).

(**1**) Article 4, Article 6, Article 8, Article 24, Article 60 and Article 78 of the Act, and Article 11 of the Rules.

(**2**) Legitimate ground shall be understood as meaning an event of an extraordinary nature outside the control of the personal information handling business operator 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 42, paragraph (1), of the Act has disappeared because the personal information handling business operator has taken alternative action that fully remedies the violation.