○ Bylaws for the Implementation of Personal Information Protection

(Bylaws (Gen) No. 11 dated April 1, 2005)

Amendments

Bylaws (Gen) No. 5 dated April 1, 2008

Bylaws (Info) No. 51 dated November 14, 2008

Bylaws (Info) No. 8 dated March 16, 2009

Bylaws (Info) No. 33 dated June 28, 2010

Bylaws (Info) No. 9 dated March 31, 2011

Bylaws (Info) No. 49 dated December 12, 2011

Bylaws (Info) No. 13 dated June 12, 2015

Bylaws (Info) No. 20 dated September 30, 2015

Bylaws (Info) No. 12 dated May 2, 2017

Bylaws (Info) No. 21 dated November 27, 2017

Bylaws (Info) No. 26 dated December 12, 2018

Table of Contents

Chapter 14: Miscellaneous (Article 47)
Supplementary Provisions

Chapter 1: General Provisions

Article 1 (Purpose)
These Bylaws for the Implementation of Personal Information Protection (hereinafter referred to as the “Bylaws”) shall provide for basic matters concerning the handling of personal, specific personal, and other information at the Japan International Cooperation Agency (hereinafter referred to as "JICA”) in accordance with Article 24 of the Information Security Management Rules of the Japan International Cooperation Agency (Rules (Info) No. 14 of 2017) (hereinafter referred to as the "Management Rules”), the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, Etc. (Act No. 59 of 2003) (hereinafter referred to as the "Protection Act”), and the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 27 of 2013) (hereinafter referred to as the "Number Act”).

Article 2 (Definitions)
Article 2: The definitions of terms used herein shall be specified in the items of this Article. The meanings of those terms that are not defined in the items of this Article shall have the meanings as defined in Article 2 of the Protection Act and Article 2 of the Number Act.
(1) “Personal information” means information about living individuals including the following.
(i) Information that enables identification of a certain individual from a name, date of birth, or other description (which means documents, drawings, or electromagnetic records (which means records created by electromagnetic means (which means electronic means, magnetic means and other means that cannot be recognized by human perception; the same shall apply hereinafter); the same shall apply hereinafter), or anything expressed by voice, movement or any other means (excluding individual identification codes); the same shall apply hereinafter) contained therein (including information that can be cross-checked with other information and identify a certain person by such cross-checking).
(ii) Information that contains an individual identification code.
(2) “Individual identification code” means any characters, numbers, symbols, and other codes which fall under any of the following and are specified by government order.
(i) A characteristic of a part of an individual person’s body converted into characters, numbers, symbols, and other codes that can be used by computer to identify the person.

(ii) Characters, numbers, symbols, and other codes which are assigned to the use of services for individuals, the purchase of products sold to individuals, written on cards or other documents issued to individuals, or recorded by electromagnetic means, and can identify all users, purchasers, and receivers by being allocated, described, or recorded differently for each person.
(3) “Personal information held by JICA” means personal information that JICA officers and employees create or acquire in the course of their duties and JICA holds for official use by its officers and employees; provided, however, that this definition shall be applicable only to such information recorded in Corporate Documents (as defined in Article 2 paragraph 2 of the Act on Access to Information Held by Incorporated Administrative Agencies, Etc. (Act No. 140 of 2001); hereinafter referred to as the "Information Access Act”) (the term includes documents specified in item (3) of the same paragraph; hereinafter simply referred to as a "Corporate Document”).
(4) “Personal information file” means a set of information which contains personal information held by JICA and falls under any of the following.
(i) Personal information held by JICA which is systematically structured to enable personal information retrieval by computer for the purpose of official work.
(ii) Except for information specified in (i) above, information which is systematically structured to facilitate the retrieval of personal information held by JICA based on names, dates of birth, and other descriptions for the purpose of official work.
(5) “Personal number” means a number which is obtained by converting a resident card code and designated for identifying a person related to the resident card on which the resident card code is written.
(6) “Subject” means a person who can be identified by personal information and the personal number.
(7) “Information system” means an information system as specified in Article 1 paragraph 3 item (1) of the Management Rules.
(8) “Departments and other units” means “departments and other units” as defined in Article 2 item (2) of the Information Security Management Bylaws (Bylaws (Info) No. 11 of 2017) (hereinafter referred to as the "Management Bylaws”).
(9) “JICA Member” means a JICA Member as specified in Article 2 item (1) of the Management Rules.
(10) “Information Handling Official Worker” means an “Information Handling Official Worker” as specified in Article 2 item (2) of the Management Rules.
(11) “Incorporated administrative agencies, etc.” means incorporated administrative agencies, etc. as defined in Article 2 paragraph 1 of the Protection Act.

(12) “Specific personal information” means personal information containing personal numbers (including numbers, symbols, and other codes corresponding to personal numbers and used in place of the personal number; resident card codes are excluded).
(13) “Specific personal information file” means a personal information file which contains a personal number.
(14) “Personal number-related official work” means official work that is conducted in relation to the use of personal numbers using personal numbers to the extent necessary.
(15) “Personal number-related official worker” means a person who carries out the personal number-related official work or is commissioned to do all or part of the personal number-related official work.
(16) “Non-identifying processed information” means such information about individuals that can be obtained by taking measures as defined in each item of Article 2 paragraph 8 of the Protection Act so as to disable the identification of any person (which means that it is impossible to identify a certain person through any description or other matters contained in information about the person or, in the case of information about the particular person that can be cross-checked with other information (excluding personal information of the person containing all or part of information about the person or any information as specified in the rules of the Personal Information Protection Committee (hereinafter referred to as the "PIPC Rules”))) and by processing personal information according to the classification of personal information (excluding information (excluding information that can be easily cross-checked with other information and identify a certain person by such cross-checking) that can be cross-checked with other information and identify a certain person by such cross-checking; the same shall apply to the rest of this Article) so as to disable the restoration of original personal information.
(17) “Non-identifying processed information of incorporated administrative agencies, etc.” means non-identifying processed information obtained by processing all or part of personal information held by JICA (excluding any non-disclosing part of information if any non-disclosing information as defined in Article 5 of the Act on Access to Information Held by Incorporated Administrative Agencies, Etc. (excluding information specified in item (1) of the same Article) is contained therein) held by an independent administrative agency constituting a personal information file as defined in each item of Article 2 paragraph 9 of the Protection Act (excluding such information (excluding such information that can be easily cross-checked and identify a certain person by the cross-checking) that can be cross-checked and identify a certain person by the cross-checking).
(18) “Non-identifying processed information file of incorporated administrative agencies, etc.” means a set of information which contains non-identifying processed information of

incorporated administrative agencies, etc. and is systematically structured to enable information retrieval.
(19) “Handler of non-identifying processed information of incorporated administrative agencies, etc.” means a person or entity (excluding state organizations, incorporated administrative agencies, local governments, and local incorporated administrative agencies (which means local incorporated administrative agencies as specified in Article 2 paragraph 1 of the Local Independent Administrative Agency Act (Act No. 118 of 2003))) who repeatedly uses non-identifying processed information files of incorporated administrative agencies, etc. for business purposes.
(20) “Non-identifying processed information, etc. of incorporated administrative agencies, etc.” means non-identifying processed information of incorporated administrative agencies, etc. descriptions removed from personal information held by JICA, individual identification codes, and information about the method of processing conducted in accordance with Article 35.

Chapter 2: Personal Information Protection System

Article 3 (Improvement of Personal Information Protection Management System)
The management system for securing the personal information protection system of JICA shall be as specified in Article 5 of the Management Rules and Article 11 of the Management Bylaws.

Article 4 (Chief Information Security Officer, etc.)
1. The Chief Information Security Officer (hereinafter referred to as the "CISO”) shall supervise the affairs concerning the management of personal information held by JICA and personal numbers (hereinafter referred to as "personal or other information held by JICA") as stipulated in Article 5 of the Management Rules.
2. A Head Information Security Officer (hereinafter referred to as "Head Information Security Officer”) shall assist the CISO and supervise and control related official work as stipulated in Article 11 paragraph 2 of the Management Bylaws.
3. Information Security Officers (hereinafter referred to as "Information Security Officers”) shall manage personal information held by JICA at its departments and other units as stipulated in Article 11 paragraph 1 of the Management Bylaws.
4. When handling information systems with personal or other information held by JICA, the Information Security Officers shall conduct such handling in cooperation with the personnel in charge of such information systems as defined in Article 9 of the Management Rules.

5. Information Security Officers of divisions or other offices (hereinafter referred to as "Division/Office Information Security Officers") shall adequately manage personal information held by JICA at its divisions or other units as stipulated in Article 11 paragraph 4 of the Management Bylaws and under the instruction of the Information Security Officers.
6. The Information Security Officers shall designate JICA Members (hereinafter referred to as "Official Work Handlers") to handle personal numbers and specific personal information (hereinafter referred to as "Specific Personal and Other Information"), determine their roles, and specify the scope of Specific Personal and Other Information that they handle.

Article 5 (Audit Manager)
JICA shall establish the position of an audit manager and assign the position to the Director General of Office of Audit. The audit manager shall audit the management situations of personal or other information held by JICA.

Article 6 (Deliberations on the Management of Personal Information etc.)
Deliberations on important matters related to the management of personal information etc. held by JICA shall be made according to the provisions of Article 6 of the Management Rules.

Article 7 (Contact Point for Personal Information Consultation)
1. A contact point for personal information consultation shall be established as a place to provide consultation services for requests for disclosure, amendments, and suspensions of use in accordance with the Protection Act, and to deliver non-identifying processed information, etc. of incorporated administrative agencies, etc.
2. The contact point for information disclosure as specified in Article 4 of the Implementation Bylaws for Procedures of Corporate Document Disclosure, Etc. (Bylaws (Gen) No. 2 of 2003) shall serve as the contact point for personal information consultation.
3. The head of a unit in which a contact point for personal information consultation will be established shall appoint a person in charge of the contact point for personal information consultation who will staff the contact point at the Headquarters to accept requests for disclosure, amendment, and suspension of use.

Chapter 3: Duties and Responsibilities of JICA Members and Information Handling Official Workers

Article 8 (Duties and Responsibilities of JICA Members and Information Handling Official Workers)

1. JICA Members and Information Handling Official Workers shall respect the intentions of the Protection Act and the Number Act, comply with provisions of related laws, regulations and these Bylaws, and follow instructions from those personnel specified in Article 4 to handle personal or other information held by JICA.
2. JICA Members and Information Handling Official Workers shall not perform the following.
(1) Disclosure, without good reason, to an outside party or use for any unjustifiable purpose of the contents of personal information, specific personal information, or non-identifying processed information, etc. of incorporated administrative agencies, etc. that they have learned in relation with their duties.
(2) Abuse of their authority to collect documents, graphic materials, or electromagnetic records which contain data belonging to personal secrets exclusively for purposes other than their duties.
3. The provisions of the preceding paragraphs shall apply mutatis mutandis to JICA Members and Information Handling Official Workers after their retirement.

Chapter 4: Handling of Personal Information, Specific Personal Information, and Other Information

Article 9 (Restrictions on Retention of Personal Information]

1. The retention of personal information shall be restricted to the extent necessary to perform operations as specified by laws and regulations and the Purpose of Use shall be specified as clearly as possible.
2. Personal information shall not be retained beyond the scope necessary to achieve the purpose of use as specified in the preceding paragraph (hereinafter referred to as the "Purpose of Use").
3. If the Purpose of Use is to be altered, the alteration shall not go beyond the scope that can be reasonably recognized as having considerable relations with the previous Purpose of Use before alteration.
4. The personal information noted below shall be referred to as “personal information that needs special consideration” and shall not be retained at JICA. Notwithstanding the foregoing, this provision shall not apply to such cases where the consent of the Subject has been obtained, where any special provision is stipulated by laws or regulations, where it is indispensable for judicial proceedings, and where it is essential to achieve the purpose of official work handling such personal information.
(1) Such personal information which needs special consideration for its handling so as not to cause discrimination, prejudice, or any disadvantage against the Subject as the said personal information contains any of the descriptions in the following items, including the Subject’s

race, creed, social status, medical history, criminal record, the fact of suffering injury due to crime, or other unfair discrimination against the Subject himself/herself.
(2) Information about impairment of the Subject's mental or physical functions such as physical disability, intellectual disability, and mental disorder (including developmental impairment).
(3) Results of medical or other checkups performed by a medical doctor or other personnel for prevention and/or early detection of disease.
(4) Information about advice, medical care, or medication given to the Subject by a medical doctor or other personnel based on the results of medical or other checkups or because of disease, injury, or any other mental and/or physical change in order to improve the Subject's mental and/or physical condition.
(5) Information about any fact of arrest, investigation, seizure, custody, prosecution, or other proceedings related to a criminal case having been carried out with respect to the Subject as a suspect or defendant.
(6) Information about any fact of investigation, measures for observation and protection, hearings and decisions of a family court, protective measures, or any other procedures related to a juvenile protection case having been carried out with respect to the Subject as a juvenile or person suspected to be a juvenile as defined in Article 3 paragraph 1 of the Juvenile Act.

Article 10 (Indication of the Purpose of Use)
If JICA acquires any personal information recorded on documents (including electromagnetic records) directly from a Subject, JICA shall indicate the Purpose of Use of such personal information to the Subject except in the following cases.
(1) When such personal information is urgently needed to protect a human life, human body, or property.
(2) When the indication of the Purpose of Use to the Subject may jeopardize the life, body, or property of the Subject or a third party.
(3) When the indication of the Purpose of Use to the Subject may hinder official work or other services conducted by incorporated administrative agencies, etc. or local governments.
(4) When the Purpose of Use can be considered to be obvious because of the situation under which such personal information is acquired.

Article 11 (Fair Acquisition)
JICA Members and Information Handling Official Workers shall not acquire any personal information in an untruthful or dishonest manner.

Article 12 (Restrictions of Use of Specific Personal and Other Information)

The Information Security Officers shall comply with the following when they use any personal or other information.
(1) The use of personal numbers shall be restricted to such official work as restrictively defined in the Number Act.
(2) The Information Security Officers shall not ask for the provision of a personal number unless it is necessary in order to do any official work related to the personal number.
(3) The Information Security Officers shall not create any specific personal information file unless it is necessary in order to do official work related to the personal number or it is stipulated in the Number Act.
(4) If the Information Security Officers will hold any specific personal information, they shall conduct a specific personal information protection assessment in advance. This shall exclude such official work for which specific personal information protection assessment is not obliged by the specific personal information protection assessment guidelines pursuant to Article 27 paragraph 1 of the Number Act.
(5) The Information Security Officers shall not collect or store any specific personal number or other personal information of other people unless any of the provisions of Article 19 of the Number Act apply.

Article 13 (Ensuring Correctness)
1. JICA Members and Information Handling Official Workers shall endeavor to match personal or other information held by JICA with past or present facts as far as necessary to achieve the Purpose of Use.
2. If a JICA Member or Information Handling Official Worker finds an error or other defect in personal or other information held by JICA, he/she shall make correction or other adjustment according to the instructions of the chief administrator.

Article 14 (Access Control)
1. The Division/Office Information Security Officers shall limit, according to the confidentiality and other contents (*) of personal information held by JICA, the scope of JICA Members and Information Handling Official Workers having a right of access to such information and shall restrict the content of their authority to the minimum extent necessary for such JICA Members and Information Handling Official Workers to perform their duties.
* Consider the ease of personal identification (degree of anonymity etc.), whether it is personal information that needs special consideration and the nature and degree of possible damage from leakage. The same shall apply below.

2. Any JICA Member or Information Handling Official Worker who does not have a right of access shall not access any personal or other information held by JICA.
3. Even a JICA Member or Information Handling Official Worker who has a right of access shall not access any personal or other information held by JICA for any purpose other than the purpose of his/her duties.

Article 15 (Password and Encryption)
1. The Head Information Security Officer shall take necessary action to set up and encrypt passwords for electromagnetic records according to the confidentiality and other contents of personal or other information held by JICA.
2. According to the confidentiality and other contents of personal or other information held by JICA, JICA Members and Information Handling Official Workers shall appropriately encrypt any personal or other information held by JICA which should be processed in accordance with the preceding paragraph.

Article 16 (Restrictions on Duplication, etc.)
Even in the case that JICA Members and Information Handling Official Workers handle personal or other information held by JICA for the purpose of their duties, the Division/Office Information Security Officers shall, according to the confidentiality and other contents of personal or other information held by JICA, define situations in which JICA Members and Information Handling Official Workers can perform the following activities, and JICA Members and Information Handling Official Workers shall follow the instructions of the Division/Office Information Security Officers.
(1) Duplication of personal or other information held by JICA.
(2) Transmission of personal or other information held by JICA.
(3) Sending out or taking out of any media on which personal or other information held by JICA is recorded.
(4) Any other activities that may hinder the appropriate management of personal or other information held by JICA.

Article 17 (Management of Media)
JICA Members and Information Handling Official Workers shall follow the instructions from the Division/Office Information Security Officers to store media on which personal or other information held by JICA is recorded in an area with physical security level 3 as defined by Article 42 of the Management Bylaws and lock up the same area after the end of work. They

shall store such media in a fire-proof safe or take other precautions when they find it necessary to do so.

Article 18 (Abolishment, etc.)
Following the instructions from the Division/Office Information Security Officers, JICA Members and Information Handling Official Workers shall delete, in an unrecoverable manner, personal or other information held by JICA for which the storage period as defined in the Corporate Document Management Rules has expired and/or abolish media (including those built into terminals or servers) on which such expired information is recorded.

Article 19 (Use and Provision Outside the Purpose of Use)
1. JICA Members and Information Handling Official Workers shall not use or provide any personal or other information held by JICA for a use outside the Purpose of Use unless otherwise provided for by laws or regulations.
2. Notwithstanding the foregoing, JICA Members and Information Handling Official Workers may use personal information held by JICA for a use outside the Purpose of Use if the Division/Office Information Security Officers acknowledge that any of the following applies; provided, however, that this shall not apply if it is recognizable that such use of personal information held by JICA outside the Purpose of Use may unjustly infringe any right or interest of the Subject or a third party.
(1) When the consent of the Subject has been obtained.
(2) When the personal or other information held by JICA is internally used within the limit necessary for the execution of duties as stipulated by laws or regulations and there is a good reason for such use of the information.
3. When personal information held by JICA is used in accordance with the provisions of the preceding paragraph, the Division/Office Information Security Officers shall limit such internal use other than the Purpose of Use to certain JICA officers and/or employees if the Division/Office Information Security Officers recognize it to be especially necessary to protect rights or interest of individuals.
4. Notwithstanding the provisions of the preceding paragraph, any Division/Office Information Security Officer may provide personal information held by JICA for a use outside the Purpose of Use if his/her Information Security Officer acknowledges that any of the following applies; provided, however, that this shall not apply if it is recognizable that the provision of such information for any use outside the Purpose of Use may unjustly infringe any right or interest of the Subject or a third party.

(1) When the consent of the Subject has been obtained or the information will be provided to the Subject.
(2) When the receiver of personal information held by JICA uses the same information for official work or duties as stipulated by laws or regulations and has a good reason for such use in a case in which personal information held by JICA is provided to administrative agencies (as defined in Article 2 paragraph 1 of the Act on the Protection of Personal Information Held by Administrative Agencies (Act No. 58 of 2003); the same shall apply hereinafter), other incorporated administrative agencies, etc., or local governments.
(3) When personal information held by JICA is provided exclusively for the purpose of preparing statistics or academic research purposes, when it is obviously to the benefit of the Subject to provide such information to a person other than the Subject, and when there is a special reason for providing such information, in addition to cases mentioned in the two paragraphs above.
5. The provisions of the preceding two paragraphs shall not prevent the application of any other laws or regulations which limit the use or provision of personal information held by JICA.
6. The Information Security Officers shall not provide any specific personal information unless any of the provisions of Article 19 of the Number Act applies.

Article 20 (Request for Action to a Receiver of Personal Information Held by JICA for Use Outside the Purpose of Use)
1. When providing personal information held by JICA to any party other than administrative agencies or incorporated administrative agencies, etc. in accordance with the provisions of paragraph 4 item (2) or item (3) of the preceding Article, the Division/Office Information Security Officers shall, as a general rule, exchange with the receiver documents pertaining to the receiver's Purpose of Use, the law that is the basis for operations for which the information is used, the recording range and record items to be used, the form of usage, and other matters.
2. When providing personal information held by JICA to any party other than administrative agencies or incorporated administrative agencies, etc. in accordance with the provisions of paragraph 4 item (2) or item (3) of the preceding Article, the Division/Office Information Security Officers shall request actions to ensure the safety of such information. If the Division/Office Information Security Officers find it necessary to do so, they shall conduct an on-site investigation prior to the provision of information or from time to time, to confirm the status of the receiver's measures, record the results, and take action including requests for improvement.
3. When providing personal information held by JICA to any party other than administrative agencies or incorporated administrative agencies, etc. in accordance with the provisions of

paragraph 4 item (2) of the preceding Article, the Division/Office Information Security Officers shall take action as defined in paragraph 2 above if they find it necessary to do so. If the exchange of documents is not conducted as provided for in paragraph 1 of this Article, the Division/Office Information Security Officers shall make a record of the fact that personal information held by JICA has been provided.

Article 21 (Record on Handling Status of Personal or Other Information Held by JICA)
The Division/Office Information Security Officers shall improve ledgers and other documents according to the confidentiality and other contents of personal or other information held by JICA and shall make a record of the handling status including the usage and storage of such information.

Chapter 5: Ensuring Security of Information Systems and Other Related Matters

Article 22 (Ensuring Security of Information Systems and Other Related Matters)
The security control of rooms and other locations where core servers and other equipment that secure information systems and handle personal or other information held by JICA are installed shall be in accordance with the provisions of the Management Rules and Management Bylaws. Necessary precautions shall be placed depending upon the importance of such information including its confidentiality.

Chapter 6: Consignment of Operations Pertaining to Handling of Personal or Other Information Held by JICA

Article 23 (Consignment of Operations, etc.)
1. When outsourcing operations related to the handling of personal or other information held by JICA, the Information Security Officers shall take necessary measures so that they will not select any contractor who does not have the ability to properly manage personal information.
2. When outsourcing operations related to the handling of personal or other information held by JICA, the Information Security Officers shall define the following matters in the contract and confirm in writing necessary issues including inspecting items about the management of responsible and working personnel, the implementation structure, and the information control of the outsourcing contractor.
(1) Measures to ensure the safety of personal information.
(2) Obligations to maintain confidentiality, prevention of use outside the Purpose of Use, etc.

(3) Restrictions on re-consignment (Including where the re-consignment is to the subsidiary of the contractor (in accordance with the provisions of Article 2 paragraph 1 item 3 of the Companies Act (Act No. 86 of 2005)). The same shall apply in this item and paragraph 4.) (*) or matters related to conditions for the prior approval etc. of re-consignment.
* Clearly state in the contractor agreement that the matters to be asked of the sub-contractor when re-consigned are the same even if it is the subsidiary of the contractor.
(4) Matters related to the restriction of personal information duplication, etc.
(5) Matters related to measures regarding the occurrence of incidents including the leakage of personal information.
(6) Matters related to the deletion of personal information and the return of media when consignment terminates or expires.
(7) The right to terminate a contract, liability for damages, and other necessary matters if violation of any of the above-mentioned occurs.
3. When outsourcing operations related to the handling of personal or other information held by JICA, the Division/Office Information Security Officers shall conduct, according to the confidentiality and other content or quantities of such information in relation to the outsourcing operations, regular investigations at least once a year, in principle on-site, to confirm the management systems, implementation systems and management of personal information at the outsourcing contractor.
4. If the outsourcing contractor re-consigns to its sub-contractor the operations related to the handling of personal information held by JICA, the Information Security Officers shall cause the outsourcing contractor to take action as defined in paragraph 2 above, and JICA shall cause the outsourcing contractor to take measures or the same organization itself shall take measures as specified in the foregoing according to the confidentiality and other contents of such information. The same shall apply if the sub-contractor further consigns such operations to another contractor.
5. When having a dispatched worker conduct the operations s related to the handling of personal information, the responsible person acting for the client (having the meaning defined in Article 41 of the Act for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers (Act No. 88 of 1985)) shall clearly indicate in the worker dispatch contract such matters related to the handling of personal information including an obligation of confidentiality.
6. From the perspective of reducing the risk of damage due to leaks etc., when providing personal information held by JICA or outsourcing operations, consideration shall be given to the purpose of use at provided entity, the details of consignment work, the confidentiality of the

personal information held by JICA etc., and its contents, and, as necessary, measures shall be taken to anonymize such as replacing names with numbers etc.

Article 24 (Consignment of Official Work Related to Personal Numbers)
When consigning all or part of official work related to personal numbers, the Information Security Officers shall take the following measures in addition to those mentioned in the preceding Article.
(1) Ensuring in advance whether or not the consignee takes any measures equivalent to the safety management measures that JICA is obligated to do under the Number Act.
(2) Taking necessary and appropriate measures to ensure that the consignee takes action equivalent to the safety management measures that JICA is obligated to do under the Number Act.
(3) Deciding to accept or reject re-consignment after checking to see if specific personal information and other information will be secured during consigned operations pertaining to personal numbers when the consignee intends to re-consign such operations to another contractor.

Chapter 7: Preparation and Publication of Personal Information File Register

Article 25 (Preparation and Publication of Personal Information File Register)
1. The secretariat as mentioned in Article 6 paragraph 3 of the Management Rules (referred to as the "Secretariat" in this Article) shall immediately prepare a register (hereinafter referred to as the "Personal Information File Register") when JICA comes to hold a personal information file (including a specific personal information file and excluding those specified in the items under paragraph 7 of this Article and those which will not be contained in a personal information file register by virtue of the provisions of paragraph 8 of this Article; the same shall apply to paragraph 2 of this Article).
2. The Personal Information File Register shall be the one register respectively for every personal information file that JICA holds.
3. When any data which should be put in the Personal Information File Register is changed, any Division/Office Information Security Officer who manages such personal information shall immediately report the change to the Secretariat. The Secretariat shall immediately amend such personal information when it receives such a report.
4. If JICA ceases to hold any personal information file contained in the Personal Information File Register or if the provisions of Article 7 paragraph 7 come to apply to a personal information file, any Division/Office Information Security Officer who manages such personal

information shall report the fact to the Secretariat without delay. The Secretariat shall delete such a personal information file without delay when it receives such a report.

5. When the Secretariat creates a Personal Information File Register, the Secretariat shall make it available for public review at JICA without delay and release it to the public by means of the Internet or other information and communications technology.

6. The Secretariat shall prepare and make public a Personal Information File Register which contains the items mentioned below concerning each personal information file that JICA holds.

(1) Title of the personal information file.

(2) JICA's name and the name of an organization that conducts official work related to the use of the personal information file.

(3) Purpose of use of the personal information file.

(4) Items (referred to as "recording items" in this Article) to be recorded in the personal information file and the range of records (referred to as the "recording range" in this Article) to be contained in the file about the Subject (a person who can be identified without using the name of another person, the date of birth, or any other description; the same shall apply to item (7) of the next paragraph).

(5) Method for collecting personal information (referred to as the "record information" in this Article) to be recorded in the personal information file.

(6) Receiver of record information if the record information is recurrently provided to a party other than JICA.

(7) Name and address of an organization that accepts the request as defined in the next Article

(8) If the provisions of either Article 27 paragraph 1 or Article 36 paragraph 1 of the Protection Act are applicable to the personal information file, such fact.

(9) Which provision of Article 2 item (4) (i) or (ii) is applicable to the personal information file.

(10) If any personal information file as defined in paragraph 7 item (10) below exists among those files to which Article 2 (4) (i) is applicable, such fact.

(11) If "personal information that needs special consideration" is included in record information, such fact.

(12) Other items designated by government decree.

7. The provisions of the preceding paragraph shall not apply to personal information files mentioned below.

(1) Personal information files that are related to JICA officers, employees, or those who were JICA officers or employees and exclusively contain personnel, payroll, welfare, or similar data (including personal information files related to the employment examination).

(2) Personal information files that are used only for experimental computer processing.

(3) Personal information files which contain all or part of the record information recorded in personal information files to be made public as provided for by the preceding paragraph and their Purposes of Use, recording items, and recording ranges within the scope of such items to be made public.
(4) Personal information files which contain only record information to be deleted within a year.
(5) Personal information files which contain record information to be used for sending materials or other goods, remitting money, or making necessary contact for duties, and which only contain names and addresses of contacts and other data necessary for such sending, remitting, or making contact.
(6) Personal information files that JICA officers and/or employees voluntarily create for academic research purposes and use record information exclusively for that purpose.
(7) Personal information files which have less than 1,000 Subjects.
(8) Personal information files that are related to people as defined below and exclusively contain personnel, payroll, welfare, or similar data (including personal information files related to the employment examination of those provided for in (i) below).
(i) People who are employed by any administrative agency and give their services to any entity other than the State.
(ii) People who fell under (i) above in the past.
(iii) Dependents or bereaved family members of those specified in item (1), or those who fall under (i) or (ii).
(9) Personal information files that have data on those specified in item (1), or those who fall under (i), (ii), or (iii) of the preceding item, and exclusively contain personnel, payroll, welfare, or similar data.
(10) Personal information files that are related to Article 2 item (4) (ii), and the Purpose of Use and recording range is within the Purpose of Use and recording range of personal information files related to Article 2 item (4) (i) hereof which provides for the publication as defined in paragraph 6.
(11) Personal information files which fall under non-identifying processed information files of incorporated administrative agencies, etc.
(12) Personal information files which have record information including deleted information.
8. Notwithstanding the provisions of paragraph 6, when the Secretariat determines that the proper performance of official work or operations may be hindered by describing some of the recording items or items specified in item (5) or item (6) of the same paragraph in the Personal Information File Register or by entering personal information files in the Personal Information File Register because of the characteristics of such work or operations, the Secretariat may

decide not to describe some of such recording items or such items or not to input personal information files.

Chapter 8: Disclosure, Correction, and Suspension of Use of Personal or Other Information Held by JICA

Article 26 (Disclosure, Correction, and Suspension of Use)
1. Respecting the intentions of the Act on General Rules for Incorporated Administrative Agencies, JICA shall respond to a request for the disclosure, correction, or suspension of use of personal or other information held by JICA when JICA receives such a request from the Subject (including his/her legal representative if the Subject is a minor or adult ward).
2. Procedures necessary for the acceptance of requests from the Subject and the disclosure and other actions shall be specified separately.

Chapter 9: Provision of Non-Identifying Processed Information of Incorporated Administrative Agencies, Etc.

Article 27 (Provision of Non-Identifying Processed Information of Incorporated Administrative Agencies, Etc.)
1. JICA may create and provide non-identifying processed information, etc. of incorporated administrative agencies, etc. (only those constituting non-identifying processed information files of incorporated administrative agencies, etc.).
2. JICA shall not use or provide any non-identifying processed information, etc. of incorporated administrative agencies, etc. or deleted information for uses outside the Purpose of Use unless otherwise provided for by laws or regulations.
3. The “deleted information” mentioned in the preceding paragraph means any descriptions, individual identification codes, and so on deleted from personal or other information held by JICA (excluding information (excluding information that can be easily cross-checked and identify a certain person by means of cross-checking) that can be cross-checked and identify a certain person by means of cross-checking; the same shall apply hereinafter) used for the creation of non-identifying processed information of incorporated administrative agencies, etc.

Article 28 (Entering Matters Related to Solicitation of Proposals in Personal Information File Register)

When JICA accepts that any personal information file held by JICA falls under all items of Article 2 paragraph 9 of the Protection Act, JICA shall enter all of the following in the Personal Information File Register relating to such a personal information file.
(1) The fact that it is a personal information file for which JICA will solicit proposals.
(2) The name and address of an organization that will receive proposals.
(3) The fact that the opportunity to submit a written opinion will be given if the said personal information file falls under Article 2 paragraph 9 item (2) (limited to such part that is related to (ii) thereof) of the Protection Act

Article 29 (Solicitation of Proposals)
JICA shall solicit proposals as defined in paragraph 1 of the next Article about personal information files held by JICA (restricted to those personal information files for which the description under item (1) of the preceding Article is contained in the Personal Information File Register).

Article 30 (Proposals about Activities for Which Non-Identifying Processed Information of Incorporated Administrative Agencies, Etc. Is Used)
1. A person who responds to the solicitation of proposals as defined in the preceding Article with the intention of becoming a handler of non-identifying processed information of incorporated administrative agencies, etc. that uses such information for business purposes may make a proposal to JICA about such business.
2. For proposals under the preceding paragraph, a document containing the following items must be submitted to JICA, in accordance with regulations.
(1) Name or identity of the person making the proposal, address or place of residence and in the case of corporations or other organizations the name of the representative
(2) Name of the personal information file under the proposal
(3) The number of individuals for which the non-identifying processed information of incorporated administrative agencies, etc. is sought under the proposal
(4) In addition to the preceding items, where the method of processing is required to be identified in association with the provisions of Article 35 under the proposal to use in the creation of non-identifying processed information of incorporated administrative agencies, etc., the following items
(5) The purpose and method of use of the non-identifying processed information of incorporated administrative agencies, etc. under the proposal, and the details of other activities for which said non-identifying processed information of incorporated administrative agencies, etc. will be used

(6) The period for which the non-identifying processed information of incorporated administrative agencies, etc. in the preceding item is intended to be used under the proposal
(7) Measures to prevent the leakage of non-identifying processed information of incorporated administrative agencies, etc. under the proposal, and other measures for the appropriate management of said non-identifying processed information of incorporated administrative agencies, etc.
(8) The following matters as specified by regulation, in addition to those matters listed in the preceding items
3. The documents mentioned in the preceding paragraph shall be accompanied by the following and other forms stipulated by the PIPC Rules.
(1) A written pledge indicating that the maker of the proposal mentioned in paragraph 1 above does not fall under any of the provisions of Article 31.
(2) A document that clearly indicates that the activity mentioned in item 5 of the preceding paragraph will contribute to the creation of new industry, vitality of the economy, or enrichment of the life of the people.

Article 31 (Reasons for Disqualification)
No one who falls under any of the following may make a proposal as defined in paragraph 1 of the preceding Article.
(1) A minor, adult ward, or warrantee.
(2) A person for whom the commencement of bankruptcy proceedings has been decided and the restoration of rights has not yet been achieved.
(3) A person who was sentenced to imprisonment without work or heavier punishment or punished under the provisions of the Act on the Protection of Personal Information (Act No. 57 of 2003) or the Act on the Protection of Personal Information Held by Administrative Agencies (Act No. 58 of 2003; hereinafter referred to as the "Administrative Act"), and two years have not passed since execution of the sentence has finished, or from the date on which execution of the sentence came to be no longer in effect.
(4) A person whose contract to use non-identifying processed information of incorporated administrative agencies, etc. was canceled pursuant to the provisions of Article 39 and two years have not passed from the date of such cancellation.
(5) A person whose contract related to the use of non-identifying processed information of incorporated administrative agencies, etc. in relation to the provisions of Article 2 paragraph 9 of the Administrative Act (only such information that constitutes the non-identifying processed information file of incorporated administrative agencies, etc. as defined in paragraph 10 of the

same Article) was canceled under the provisions of Article 44 paragraph 14 of the Administrative Act and two years have not passed from the date of such cancellation.
(6) A corporate person or other entity whose officer falls under any of the foregoing.

Article 32 (Examination and Other Process of Proposals)
When a proposal is made, JICA must examine whether or not the proposal conforms to the requirements by confirming the following.
(1) That the person making a proposal as set out in Article 30 paragraph 1 does not fall under any of the items of the preceding Article.
(2) That the number of Subjects contained in non-identifying processed information of incorporated administrative agencies, etc. related to a proposal as specified in Article 30 paragraph 2 item (3) hereof is 1,000 or more and is less than the number of Subjects contained in personal information held by JICA which constitutes the personal information file related to such a proposal.
(3) That the process method identified by matters specified in Article 30 paragraph 2 item (3) and item (4) is in compliance with the criteria specified in Article 35 paragraph 1.
(4) That the activity mentioned in Article 30 paragraph 2 item (5) contributes to the creation of new industry, vitality of the economy, or enrichment of the life of the people.
(5) That the period of time specified in Article 30 paragraph 2 item (6) does not exceed such duration that is necessary from the viewpoint of the effective use of non-identifying processed information of incorporated administrative agencies, etc., for the purpose and contents of activities, and the purpose and method of use of such information.
(6) That the purpose and method of use of non-identifying processed information of incorporated administrative agencies, etc. related to proposals as specified in Article 30 paragraph 2 item (5) as well as the measures specified in item (7) of the same paragraph are appropriate for the protection of the rights and interests of the Subject contained in such non-identifying processed information of incorporated administrative agencies, etc.
(7) That it does not significantly hinder the execution of JICA's operations when JICA prepares non-identifying processed information of incorporated administrative agencies, etc. in addition to the provisions of the preceding items.
2. When JICA conducts an examination pursuant to the provisions of the preceding paragraph and finds as a result of the examination that a proposal under Article 30 paragraph 1 conforms to the criteria listed in the items of the preceding paragraph, JICA shall notify the proposer of the following matters by attaching documents related to the application for execution of a contract concerning the use of non-identifying processed information of incorporated administrative agencies, etc. to the examination result notice as specified by the PIPC Rules.

(1) The possibility to execute a contract with incorporated administrative agencies, etc. concerning the use of non-identifying processed information of incorporated administrative agencies, etc. under the provisions of Article 34.
(2) Other matters specified by the PIPC Rules in addition to those defined in the preceding item.
3. When JICA conducts an examination pursuant to the provisions of paragraph 1 and finds as a result of the examination that the proposal as defined in Article 30 paragraph 1 does not conform to any one of the criteria listed in the items of paragraph 1, JICA shall give notice of the result and the reasons to the proposer.

Article 33 (Providing a Third Party with the Opportunity for Submitting a Written Opinion)
1. Regarding a proposal under Article 30 paragraph 1 related to personal information files for which the Personal Information File Register contains those matters listed in Article 28 item (3), the provisions of Article 14 paragraph 1 and paragraph 2 of the Information Access Act shall apply mutatis mutandis on the assumption that the proposal is a request under Article 3 of the Information Access Act for the disclosure of Corporate Documents on which personal information held by JICA constituting a personal information file related to the same proposal is recorded and the notification under Article 32 paragraph 2 is the decision to disclose all or part of such Corporate Documents.
2. If a third party under Article 14 paragraph 1 of the Information Access Act who is given an opportunity to submit a written opinion according to Article 14 paragraph 1 and paragraph 2 thereof which apply mutatis mutandis in the preceding paragraph indicates his/her intention to oppose the preparation of non-identifying processed information of incorporated administrative agencies, etc. related to a proposal under Article 30 paragraph 1, the provisions of this Chapter shall apply on the assumption that the personal information file pertaining to the proposal from which such personal information held by JICA containing the third party as the Subject is removed is a personal information file about the proposal.

Article 34 (Execution of Contract Pertaining to the Use of Non-Identifying Processed Information of Incorporated Administrative Agencies, Etc.)
A person who has received a notice as defined in Article 32 paragraph 2 may sign a contract with JICA regarding the use of non-identifying processed information of incorporated administrative agencies, etc. by submitting documents specified in paragraph 2 of the same Article.

Article 35 (Preparation of Non-Identifying Processed Information of Incorporated Administrative Agencies, Etc.)

1. When preparing non-identifying processed information of incorporated administrative agencies, etc., JICA shall process personal information held by JICA and used for such preparation according to the criteria specified in the PIPC Rules as necessary in order to avoid the identification of any individuals and disable the restoration of personal information held by JICA used for such preparation.

2. The provisions of the preceding paragraph shall apply mutatis mutandis to a case in which a person who has been entrusted with the preparation of non-identifying processed information of incorporated administrative agencies, etc. from JICA carries out such preparation.

Article 36 (Entering Data Related to Non-Identifying Processed Information of Incorporated Administrative Agencies, Etc. in the Personal Information File Register)

When preparing non-identifying processed information of incorporated administrative agencies, etc., JICA shall enter in the Personal Information File Register the following data about a personal information file which contains the personal information held by JICA that is used for the preparation.

(1) The number of Subjects and the titles of information contained in non-identifying processed information of incorporated administrative agencies, etc. as the outline of such information.

(2) The name and address of an organization that will receive prepared non-identifying processed information of incorporated administrative agencies, etc.

(3) The period of time that proposals can be made about prepared non-identifying processed information of incorporated administrative agencies, etc.

Article 37 (Proposals about Activities for Which Prepared Non-Identifying Processed Information of Incorporated Administrative Agencies, Etc. Is Used)

1. A person who has the intention of becoming a handler of non-identifying processed information of incorporated administrative agencies, etc. that uses non-identifying processed information of incorporated administrative agencies, etc. for which such data as defined in item (1) of the preceding Article is entered in the Personal Information File Register according to the provisions of the preceding Article for business purposes may make a proposal to JICA about such business. The same shall apply to a case in which a person who has executed a contract pertaining to the use of such non-identifying processed information of incorporated administrative agencies, etc. according to Article 34 intends to change such business.

2. Article 30 paragraphs 2 and 3, Article 31, Article 32, and Article 34 shall apply mutatis mutandis to the proposal specified in the preceding paragraph.

Article 38 (Charges)

1. A person who signs a contract pertaining to the use of non-identifying processed information of incorporated administrative agencies, etc. according to Article 34 (including cases applicable mutatis mutandis as provided in paragraph 2 of the preceding Article; the same shall apply to the next Article) must pay the charge specified by JICA.
2. The amount of the charge shall be determined by JICA taking into consideration actual costs and the charge specified in Article 44.13 of the Administrative Act.
3. Incorporated administrative agencies, etc. must make the provisions of the two preceding paragraphs available for public review.

Article 39 (Cancellation of Contract Pertaining to the Use of Non-Identifying Processed Information of Incorporated Administrative Agencies, Etc.)

If a person who has signed a contract pertaining to the use of non-identifying processed information of incorporated administrative agencies, etc. according to Article 34 falls under any of the following, JICA may cancel the contract.
(1) If the person executed the contract by false or fraudulent means.
(2) If the person falls under any item of Article 31 (including cases applicable mutatis mutandis as provided in Article 37 paragraph 2).
(3) If there is a material breach of any matter specified in the contract.

Article 40 (Measures to Ensure Safety)

1. JICA shall abide by the criteria provided for in the PIPC Rules to prevent the leakage of non-identifying processed information, etc. of incorporated administrative agencies, etc. and take the following necessary measures for the effective management of such information.
(1) JICA shall clearly define the authority and responsibilities of a handler of non-identifying processed information, etc. of incorporated administrative agencies, etc.
(2) JICA shall improve rules and regulations concerning the handling of non-identifying processed information, etc. of incorporated administrative agencies, etc., appropriately handle non-identifying processed information, etc. of incorporated administrative agencies, etc. in accordance with such rules and regulations, assess the situation of such handling, and take necessary measures to improve the situation based on the results of the assessment.
(3) JICA shall take necessary measures to prevent any unauthorized person from handling non-identifying processed information, etc. of incorporated administrative agencies, etc.

2. The provisions of the preceding paragraph shall apply mutatis mutandis to a case in which a person who has been entrusted with the handling of non-identifying processed information, etc. of incorporated administrative agencies, etc. from JICA carries out such handling.

Chapter 10: Measures for Safety Management Problems

Article 41 (Incident Report, Measures to Prevent Recurrence, and Publication)

1. When an incident that will become a safety management problem, including the leakage of personal and other information held by JICA, or a fact that has the potential to become an incident (hereinafter referred to as an "incident or potential incident") takes place or is found, JICA shall immediately take necessary measures.
2. JICA Members and Information Handling Official Workers must immediately report any incident or potential incident to their Division/Office Information Security Officers.
3. When the Division/Office Information Security Officers receive an incident report, they shall report the fact to their respective Information Security Officers. The Information Security Officers shall immediately take necessary measures including those for preventing the expansion of damage and for commencing restoration.
4. When the Information Security Officers receive a report on an incident or potential incident, they shall investigate how the incident or potential incident occurred and developed, check the damage, and report the results to the Head Information Security Officer. The Head Information Security Officer shall report to the CISO when he/she determines that the incident or potential incident may have a serious impact on the personal information management and operations of JICA.
5. The CISO shall bring proposed measures against such an incident or potential incident to the Committee when he/she receives the report as defined in the preceding paragraph.
6. The CISO shall immediately provide the Ministry of Foreign Affairs of Japan with information about the incident or potential incident including its details, development, and damage depending on the situation.
7. The Information Security Officers shall analyze the cause of an incident or potential incident and take necessary measures to prevent recurrence.
8. The CISO shall take necessary measures including the announcement of incident-related facts, preventive actions, and responses to Subjects whose information was involved in an incident or potential incident according to the contents of the incident or potential incident, its influence, etc. Regarding incidents or potential incidents followed by such an announcement, the CISO shall consult with the Ministry of Foreign Affairs of Japan and immediately provide information about details, developments, and damage to agencies that require such information.

Chapter 10-2 Processing of EEA Personal Data

Article 41-2 (Purpose of Regulations etc. on the Processing of EEA Personal Data)

1. Based on the "Regulation (EU) 2016/679 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 Regulations. Hereinafter "GDPR"), JICA shall establish basic matters related to the processing of all information with respect to data entities located in the European Economic Area (hereinafter "EEA") subject to protection (hereinafter "EEA personal data") and shall prescribe in this Chapter all necessary matters to ensure compliance with the GDPR.

Article 41-3 (Scope of Application of Regulations on the Processing of EEA Personal Data)

1. The matters in this Chapter are applicable to the processing of EEA personal data by JICA, and to JICA Members and Information Processing Officers that process EEA personal data.
2. Where, in the course of JICA's activities, JICA Members and Information Processing Officers processing EEA personal data as prescribed under the following items, and where this composes part of a personal data file or is planned to compose part of a personal data file, this shall be processed in accordance with the GDPR. In the processing of EEA personal data, the various provisions of Chapters 4 through 10 shall apply and shall be properly implemented by JICA Members and Information Processing Officers.

(1) When EEA personal data is processed at overseas offices of JICA located within the EEA region (hereinafter "EEA Regional Offices")

(2) When EEA personal data is processed at JICA headquarters, domestic organizations and at overseas offices not located within the EEA region (hereinafter "Non-EEA Regional Offices")

(3) When EEA personal data is transferred from a data entity located within the EEA region to the Non-EEA Regional Office of another JICA office, whether directly or through a JICA EEA Regional Office or a JICA Non-EEA Regional Office

Article 41-4 (Definitions of Terms related to the Processing of EEA Personal Data)

1. The terms used in this Chapter in relation to the processing of EEA personal data shall be as defined in the respective items. The definitions of terms not specified in the items of this Article shall be according to the provisions of Article 4 of the GDPR.

(1) "Controller" means any entity that determines the purposes and methods for processing EEA personal data, whether independently or in cooperation with other entities. Under these Bylaws, both JICA EEA Regional Offices and Non-EEA Regional Offices shall be Controllers.

Where two or more Controllers determine the purposes and methods for the processing of EEA personal data, each party shall be “Joint Controllers”.
(2) “Supervisory Authority” means public enforcement agencies in the various member states of the EU, with the responsibility of monitoring the application of the GDPR.
(3) “Data Entity” means any natural person that can be identified or identifiable, either directly or indirectly, with reference to EEA personal data.
(4) EEA (European Economic Area): A framework for participation of EU European Free Trade Association (EFTA) member nations in the single EU market without joining the EU, including EU member nations. Check each time for specific member nations
(5) “EEA Personal Data” means all information related to data entities located within the EEA region, including those listed below.
A Personal data processed in the activities of EEA Regional Offices (including personal data transferred or stored within the EEA region, and EEA region data entity personal data processed in EEA Regional Office activities outside of the EEA region)
B Personal data processed in Non-EEA Regional Offices etc., but collected from data entities within the EEA region
C Personal data transferred from EEA Regional Offices to Non-EEA Regional Offices etc.
(6) “EEA Personal Data Processing Records” means records of the EEA personal data processing process carried out under the responsibility of JICA. In accordance with the GDPR, EEA Personal Data Processing Records must describe the matters prescribed by each item of Article 41-11 paragraph 1, based on whether the entity is an Controller or a Processor.
(7) “Personal Data” means all information related to any natural person that can be identified or identifiable. Identifiable natural persons are persons that can be directly or indirectly identified with reference to identifiers, particularly their name, identification number, location data, or online identifier (IP address, cookie identifiers) etc., or one or multiple specific elements of physical, physiological, genetic, spiritual, economic, cultural or social identity.
Note that identification numbers and identifiers etc. which do not correspond with personal information under the definitions of items 1 and 2 of Article 2 may still correspond to personal data. In addition, personal data includes “special types of personal data” corresponding with “personal information that needs special consideration” under Article 9 paragraph 4 (prescribed under Article 9 paragraph 1 of the GDPR), and such data includes data which identifies race or ethnic origins, political views, religious or philosophical beliefs, or labor union qualification, genetic data, biological data, health related data or data related to sexual activity or sexual orientation which uniquely identifies a natural person. The definition of “personal information that needs special consideration” as defined under Article 9 paragraph 4 does not include labor

union qualifications or data related to sexual activity or sexual orientation, but these are processed in the same way as “personal information that needs special consideration”.
(8) “Personal Information Breach” means infringement of the security of EEA personal data which is transmitted, stored or otherwise processed, as a result of accidental or illegal destruction, loss, alteration, or unauthorized disclosure or access.
(9) “Processing” means any operations or series of operations (collection, recording, editing, structuring, storing, modifying or altering, restoring, referencing, using, transmitting or performing other acts which make the personal data usable such as disclosing or disseminating, aligning or binding, restricting, erasing or discarding etc.) carried out on personal data or for the collection of personal data, whether automated or not.
(10) “Processor” means any entity that processes personal data on behalf of the Controller. In these Bylaws, this mainly refers to contractors that provide services.
(11) “SCC (Standard Contractual Clauses)” mean standard contractual clauses which form agreements adopted by the decision of the European Commission. SCC are one effective protection measure by the EU to legalize the transfer of data to countries which cannot certify the adequacy of EEA personal data, for transfers between Controllers or for transfers from Controllers to Processors.
(12) “Transfer/Access” means allowing the provision of personal data to a third party, including data transmission (including by email, CD/DVD, FTP server etc.), or data input into a system which can be accessed by other entities (including software, online systems, networks, shared servers, or Group-wide document management systems etc.). Transfer may include transfers to third parties within an EEA region, from an EEA region to a Non-EEA region, or from a Non-EEA region to Non-EEA region.
(13) “Personal Data Files” means aggregates consisting of personal data, which can be accessed according to specific criteria, whether aggregated functional or geographically, or whether dispersed or scattered. Managed similarly to “Personal Information Files” as provided under Article 2 paragraph 4.
(14) “Recipient” means natural persons or corporations, public organizations, departments or other organizations which receive the disclosure of personal data, whether third parties or not. However, public institutions that acquire personal data within the framework of special investigations in accordance with EU laws and the laws of Member nations shall not be deemed Recipients. The processing of such data by public institutions shall comply with applicable data protection regulations according to the purpose of processing. “Personal data disclosure” within this Chapter shall apply mutatis mutandis to the “Provision of personal information” in Chapter 4.

(15) “Representative” means a person acting as the representative of an Controller or Processor, as nominated in writing by the Controller or Processor in accordance with Article 27 of the GDPR, taking the various obligations of the Controller or Processor within the EU region.
(16) “International Organizations” means organizations, subsidiary organizations or other organizations prescribed by international law, or established by agreement between multiple countries or based on such agreement.

Article 41-5 (Data Protection Officers)
1. Data Protection Officers (hereinafter “DPO”) as prescribed under Article 37 of the GDPR shall assume the duties described in the following items and shall serve as the head of the department established as a contact for personal information consultations.
(1) Notify and advise Controllers and Processors, and JICA Members and Information Handling Official Workers that process EEA personal data of their duties through the Secretariat based on this Chapter and the GDPR.
(2) Monitor as necessary, through the Secretariat, compliance with the GDPR, compliance with other personal data protection regulations of the EU and member nations, and compliance with Controller and Processor protection policies related to personal data protection, including the assignment of responsibilities for processing activities to staff, raising awareness and providing training, and related monitoring.
(3) When requested by the Supervising Information Security Officer, the Chief Information Security Officer or the Information Security Officer, cooperate with and advise the Secretariat regarding data protection impact evaluations as prescribed by Article 41-11 paragraphs 3 and 4 (referring to the provisions of Article 35 of the GDPR, hereinafter “DPIA”), and shall monitor performance.
(4) Cooperate with supervisory authorities.
(5) Act as a point of contact for supervisory authorities on issues related to the processing of personal data. This shall include preliminary consultations with supervisory authorities in cases indicative of high DPIA risk, and consultations on other related matters.
2. When carrying out the duties under the preceding paragraph, the DPO shall take into consideration the nature, scope, processes and purposes of the processing, and shall carefully consider the processing activities and associated risks.

Article 41-6 (Basic Principles of EEA Personal Data Protection)
When JICA processes EEA personal data in the course of its activities, this shall be processed appropriately in accordance with the provisions of Chapters 4 through 10 and with the GDPR.

Article 41-7 (Responding to Requests from Data Entities to Exercise Rights)

1. In the event that a data entity exercises any of the rights indicated in the following items with regard to EEA personal data, JICA must respond to said exercise of rights within at least one month.

(1) The right to receive notification of data processing activities carried out by JICA

(2) The right to access the EEA personal data processed by JICA

(3) The right to correct the EEA personal data processed by JICA

(4) The right to delete the EEA personal data processed by JICA

(5) The right to restrict the processing of EEA personal data processed by JICA

(6) The right to data portability in the EEA personal data processed by JICA by having it in a systematic and commonly used form which is machine readable and able to be received or transferred to another entity

(7) The right to challenge the processing of EEA personal data processed by JICA

(8) Rights related to automated decision-making regarding individuals, including profiling carried out by JICA

2. When JICA Members or Information Handling Official Workers receive contact from a data entity, whether direct or indirect, which is interpreted to be a request to exercise rights prescribed under each item of the preceding paragraph, this shall be immediately reported to the Contact Point for Personal Information Consultation as prescribed under Article 7. Also, as with Article 26 paragraph 2, any necessary procedures shall be specified separately.

3. The JICA Member or Information Processing Officer shall follow the instructions of the Secretariat and DPO as necessary and shall cooperate with the Contact Point for Personal Information Consultation to facilitate the exercise of data entity rights acknowledged by the Contact Point for Personal Information Consultation.

Article 41-8 (Accountability for the Processing of EEA Personal Data)

1. The Information Security Officer shall follow the GDPR as the basis for the processing of EEA personal data, and shall save and keep current all policies, regulations and other decisions and documentary records.

2. When JICA Members or Information Processing Officers have concerns regarding the principles of these Bylaws or the GDPR, or regarding compliance with their obligations in the processing of EEA personal data, they shall seek advice from the Secretariat or the DPO. Related departments etc. shall also seek advice from the Secretariat or the DPO to ensure compliance with these regulations etc.

3. When the work of processing EEA personal data is consigned to a Processor, the Information Security Officer shall take measures necessary to ensure compliance with matters required under Article 28 of the GDPR, as well as the provisions of Article 23.

Article 41-9 (Data Protection in Design and Initialization for the Processing of EEA Personal Data)

The Information Security Officer shall take the steps and measures contained in the following items to ensure that there is no excessive, unnecessary or unauthorized processing of EEA personal data in information systems and processes at every stage of the EEA personal data processing activities.

(1) When developing or initializing new services, processes or information systems which process EEA personal data, privacy-conscious deign approaches shall be comprehensively incorporated into the design.

(2) The most privacy-conscious settings shall be applied as the default setting for all privacy data protection settings throughout the JICA information and communication network

(3) When JICA Members or Information Processing Officers cross-connect or access multiple databases, restrict unauthorized access to EEA personal data through pseudonymization or other measures

Article 41-10 (Implementation of Technical and Organizational Security Management Measures for the Processing of EEA Personal Data)

1. The Information Security Officer shall take the following technical and organizational security measures (security enhancement measures), depending on the risk of the EEA personal data processing, to ensure the appropriate security level is applied relative to the risk.

(1) The pseudonymization and encryption of personal data

(2) The ability to ensure the current levels of confidentiality, integrity, availability and recoverability of processing systems and processing services

(3) The ability to ensure the availability and restore access to personal data in the event of a physical or technical incident

(4) Procedures for the regular testing, evaluation and review of the effectiveness of technical and organizational measures to ensure the security of processing

2. When preparing non-identifying processing information from EEA personal data, in accordance with the provisions of Article 35, this shall only be processed as non-identifying processed information of incorporated administrative agencies etc. where it is impossible to re-identify anonymous individuals from descriptions or personal identifiers or other processes carried out under the same Article to delete information of personal information held by JICA

and used in the preparation of the non-identifying processed information of incorporated administrative agencies etc.

Article 41-11 (Restrictions etc. on the Processing of EEA Personal Data)

1. JICA Members and Information Processing Officers shall only process EEA personal data where there are books (hereinafter "Personal Information File Ledgers") organized as the foundation for personal information files as specified under Article 25, including the EEA personal data processing records specified in the following items, and shall not process EEA personal data where such EEA personal data processing records have not been organized.

(1) The following activity records related to processing performed by Controllers

A The name and contact information for the Controller and (if applicable) Joint-Controller or representative of the Controller, as well as the DPO

B Purpose of processing

C Description of the form of data entity and the type of personal data

D The type of Recipient to whom personal data was disclosed or will be disclosed, including Recipients that are third countries or international organizations

E (If applicable) in the case of the transfer of personal data to third countries or international organizations, including the identity of the third country or international organization, or the transfer of exceptional personal data where exceptions under the special circumstances prescribed under Article 49 (1) of the GDPR are not applicable, documents showing appropriate protective measures (SCC etc.)

F (Where possible) the deadline for the scheduled deletion of different types of data

G (Where possible) an outline of the technical and organizational security measures prescribed by Article 41-10

(2) The following activity records related to processing performed by Processors

A The names and contact information of Processors or individual Controllers on whose behalf Processors are acting, and (if applicable) the names and contact information of representatives of Controllers or Processors, and the DPO

B The types of processing performed on behalf of individual Controllers

C (If applicable) in the case of the transfer of personal data to a third country or international organization, including where the third country or international organization is identified, or for the exceptional transfer of personal data in circumstances where the exceptions in special circumstances set out in Article 49 (1) of the GDPR cannot be applied, a document showing appropriate protection measures (SCC etc.)

D (Where possible) an outline of the technical and organizational security measures prescribed by Article 41-10

2. Where the conditions listed in the following items apply to JICA Members or Information Processing Officers, they shall not be permitted to process EEA personal data.

(1) When EEA personal data is processed for a new purpose not specified in the prepared personal information file ledger

(2) When a new type of EEA personal data not specified in the prepared personal information file ledger is processed

3. When there is no EEA personal data processing record prepared in a department etc. that processes EEA personal data, the Information Security Officer shall have such a record created, and shall determine whether DPIA needs to be implemented, based on the matters set out in the following items.

(1) Consider the nature, scope, process and purpose of processing, and where there is a high risk with respect to the rights and freedoms of the data entity, particularly in the case of types using new technologies. The following cases are typical examples of cases with high risk.

A　Cases which lead to evaluations that have a legal effect or other similar serious effect on the data entity based on automatic processing, including profiling

B　When processing personal data as defined under Article 41-4 item 7 of these Bylaws in large amounts, which corresponds to “special types of personal data” under the same item.

C　When conducting large-scale monitoring on systems in locations which can be accessed by the public

(2) When processing activities requiring DPIA published by supervisory authorities, or when corresponding to personal data processing activities not requiring DPIA

4. The Information Security Officer shall immediately report to the Secretariat and DPO new EEA personal data processing records prepared in accordance with the preceding paragraph, and the results of DPIA decisions. In addition, in accordance with the preceding paragraph, when the Information Security Officer of the department that is the Controller of the EEA personal data implements a DPIA, the instructions and advice of the Secretariat and the DPO shall be followed, and the DPIA results shall be immediately reported to the Secretariat and the DPO. Depending on the content of the report, the Secretariat or the DPO may impose the conditions listed in the following items.

(1) The modification of the reported EEA personal data handing process

(2) The acquisition of consent from the data entity in accordance with the documents, guidance and instructions provided by the Secretariat, or the modification existing procedures for acquiring consent

(3) Notification or the modification of existing notifications in accordance with the documents, guidance and instructions provided by the Secretariat

(4) The addition of new processing processes or correction of existing processing necessary for the recording of existing EEA personal data processing

Article 41-12 (Restrictions of the Transfer of EEA Personal Data)

1. JICA Members and Information Handling Official Workers shall only transfer EEA personal data to third country entities (Non-EEA Region Offices or Processors) or international organizations which satisfy the conditions listed in the following items and shall not make transfers where such conditions are not satisfied.

(1) A personal information file ledger is maintained for the EEA personal data, including an EEA personal data processing record as prescribed by Article 41-11 paragraph 1

(2) There is no new purpose of processing or form or type of personal data in relation to the EEA personal data corresponding to Article 41-11 paragraph 1 item 1 B and C

(3) There is no new Recipient in relation to the EEA personal data corresponding to Article 41-11 paragraph 1 item 1 D

(4) The transfer of EEA personal data corresponds with Article 45 of the GDPR (transfer based on a recognition of adequacy) or corresponding to Article 49 paragraph 1 of the GDPR (exceptions in special circumstances), or documents (SCC etc.) showing appropriate protection measures for the data transfer have been prepared in accordance with the provisions of Article 41-11 paragraph 1 item 1 E and item 2 C.

2. When trying to transfer EEA personal data to a new third country entity (Non-EEA Region Office or Processor) or international organization, without satisfying the conditions of each item of the preceding paragraph, the Information Security Officer shall prepare a new personal information file ledger in accordance with the provisions of Article 41-11, and where said data transfer does not correspond with the provisions of Article 45 of the GDPR (transfer based on a recognition of adequacy) or Article 49 paragraph 1 of the GDPR (exceptions in special circumstances), shall report to the Secretariat and the DPO regarding the need to prepare documents (SCC etc.) showing appropriate protection measures for said data transfer. The matters listed in each of the following items shall be confirmed when preparing the personal information file ledger.

(1) A new transfer, new category of personal data or new purpose in relation to the transfer of EEA personal data

(2) The EEA personal data Recipient, the country in which the Recipient is located, and the country in which the EEA personal data is stored or processed

(3) Whether there are any agreements, outsourcing agreements or other documents provided or exchanges in relation to the transfer

3. When the Information Security Officer needs to prepare a new personal information file ledger or a document (SCC etc.) showing the appropriate protection measures for the transfer of EEA personal data in accordance with the preceding paragraph, they shall immediately report this to the Secretariat and the DPO and shall follow the advice and instructions of the Secretariat and the DPO. When concluding an SCC, consideration shall be given to the matters listed in the following items.
(1) Whether the data Recipient is suitable for concluding an SCC
(2) The EEA personal data Recipient, the country in which the Recipient is located, and the country in which the EEA personal data is stored or processed
(3) Whether there are any agreements, outsourcing agreements or other documents provided or exchanges in relation to the transfer

Article 41-13 (Personal Data Breaches in the Processing of EEA Personal Data)
1. In the event that the EEA personal data processed by JICA is infringed, JICA shall report this to the relevant supervisory authorities within 72 hours of recognizing the breach. JICA must also contact relevant data entities regarding said data breach. However, this shall exclude cases in which there is no risk of the personal data breach impacting rights and freedoms of a natural person.
2. JICA Members or Information Handling Official Workers that recognize or discover the fact or potential fact of a breach or security management issue (hereinafter "EEA personal data issue") in relation to EEA personal data processed by JICA shall immediately take necessary measures and report in accordance with the provisions of Article 41.
3. The JICA Member or Information Handling Official Workerrelated to the EEA personal data issue shall, according to the judgement of the Chief Information Security Officer, investigate the EEA personal data breach and, as necessary, follow the instructions of the Chief Information Security Officer and cooperate with the Secretariat and the DPO to execute all regulatory duties.

Chapter 11: Education and Training

Article 42 (Education and Training)
1. The CISO shall regularly provide JICA Members and Information Handling Official Workers who are engaged in the handling of personal or other information held by JICA with educational, training, and personnel development programs necessary to enhance their awareness concerning the protection of such information.

2. The CISO shall provide JICA Members and Information Handling Official Workers who are engaged in official work related to the management of information systems to handle personal or other information held by JICA with educational and training programs concerning the management, operation, and security measures of information systems in order to appropriately control such information.
3. The CISO shall provide the Information Security Officers and the Division/Office Information Security Officers with educational and training programs concerning the appropriate on-site management of personal or other information held by JICA.
4. The Information Security Officers shall take necessary measures such as providing JICA Members and Information Handling Official Workers of the departments or other units to which the Information Security Officers belong with opportunities for participating in educational and training programs that the CISO offers to appropriately control personal or other information held by JICA.

Chapter 12: Audits and Inspections

Article 43 (Inspections)
1. The Information Security Officers shall regularly, or from time to time, inspect the recording media, processing pathways, storage methods, and other aspects of the personal or other information held by JICA for which they are accountable for management.
2. The Information Security Officers shall report the results of inspections as specified in the preceding paragraph and propose improvement actions to the Head Information Security Officer.
3. The Head Information Security Officer must carry out the procedure to amend rules pertaining to the protection of personal information if he/she determines it necessary to do so based on a proposal as mentioned in the preceding paragraph. Regarding such rules recognized as having the potential to have an important influence on operations of JICA, proposed amendments shall be presented to the Committee for deliberation.

Article 44 (Audits)
The audit manager shall regularly, or at the time when the necessity to do so arises, implement audits (including external audits) of the management status of personal or other information held by JICA in order to check the appropriate management of such information and report the results to the CISO.

Article 45 (Assessment and Review)

Regarding measures for the appropriate management of personal or other information held by JICA, the CISO, the Head Information Security Officer, and the Information Security Officers shall assess measures for the appropriate management of such information from the viewpoint of effectiveness taking into account the results of audits and inspections, and take action including reviews if they consider it to be necessary.

Chapter 13: Cooperation with Administrative Agencies

Article 46 (Cooperation with Administrative Agencies)

Based on the "Basic Policy Concerning the Protection of Personal Information" (Cabinet decision dated April 2, 2004) 4, JICA shall cooperate closely with the Ministry of Foreign Affairs of Japan and appropriately manage personal or other information held by JICA.

Chapter 14: Miscellaneous

Article 47 (Implementation Details)

1. Procedures and other details necessary for the implementation of these Bylaws (excluding those matters defined in the next paragraph) shall be separately determined by the Director General of the Office of Information System.
2. Disclosure, amendment, and suspension of use pertaining to personal information protection, as well as procedures and other details concerning handling of specific personal information and provision of non-identifying processed information of incorporated administrative agencies, etc. shall be separately determined by the Director General of the General Affairs Department.

Supplementary Provisions

These Bylaws shall come into force from April 1, 2005.

Supplementary Provisions (Bylaws (Gen) No. 5 dated April 1, 2008)

1. These Bylaws shall come into force from April 1, 2008.
2. If a person (hereinafter referred to as an "Authorized Person") who has been authorized or entrusted by the President to determine details related to the implementation of these Bylaws is changed to another person by the provisions of these Bylaws that are amended by Articles 1 to 27 due to the enforcement of these Bylaws and any internal quasi-regulations or similar rules (hereinafter referred to as "Internal Quasi-Regulations") actually exist at the time of the enforcement of these Bylaws, the present Internal Quasi-Regulations shall be construed to have

been established by the new Authorized Person until new Internal Quasi-Regulations which are equivalent to the present ones are established by such a new Authorized Person.

Supplementary Provisions (Bylaws (Info) No. 51 dated November 14, 2008)
These Bylaws shall come into force from November 14, 2008 and shall apply from October 1, 2008.

Supplementary Provisions (Bylaws (Info) No. 8 dated March 16, 2009)
These Bylaws shall come into force from March 16, 2009.

Supplementary Provisions (Bylaws (Info) No. 33 dated June 28, 2010)
These Bylaws shall come into force from June 28, 2010.

Supplementary Provisions (Bylaws (Info) No. 9 dated March 31, 2011)
1. These Bylaws shall come into force from April 1, 2011.
2. If a person (hereinafter referred to as an "Authorized Person") who has been authorized or entrusted by the President to determine details related to the implementation of these Bylaws is changed to another person by these Bylaws and any internal quasi-regulations or similar rules (hereinafter referred to as "Internal Quasi-Regulations") actually exist at the time of the enforcement of these Bylaws, the present Internal Quasi-Regulations shall be construed to have been established by the new Authorized Person until new Internal Quasi-Regulations which are equivalent to the present ones are established by such a new Authorized Person.

Supplementary Provisions (Bylaws (Info) No. 49 dated December 12, 2011)
These Bylaws shall come into force from December 12, 2011.

Supplementary Provisions (Bylaws (Info) No. 13 dated June 12, 2015)
These Bylaws shall come into force from June 12, 2015.

Supplementary Provisions (Bylaws (Info) No. 20 dated September 30, 2015)
These Bylaws shall come into force from September 30, 2015.

Supplementary Provisions (Bylaws (Info) No. 12 dated May 2, 2017)
1. These Bylaws shall come into force from May 30, 2017.
2. If a person (hereinafter referred to as an "Authorized Person") who has been authorized or entrusted by the President to determine details related to the implementation of these Bylaws is

changed to another person by these Bylaws and any internal quasi-regulations or similar rules (hereinafter referred to as “Internal Quasi-Regulations”) actually exist at the time of enforcement of these Bylaws, the present Internal Quasi-Regulations shall be construed to have been established by the new Authorized Person until new Internal Quasi-Regulations which are equivalent to the present ones are established by such a new Authorized Person.

Supplementary Provisions (Bylaws (Info) No. 21 dated November 27, 2017)

These Bylaws shall come into effect from November 27, 2017.

Supplementary Provisions (Bylaws (Info) No. 26 dated December 12, 2018)

These Bylaws shall come into effect from December 12, 2018.