Personal Information Protection Regulations

Kojin jyoho hogo kitei

March 10, 2005, Reg. 6

With revisions effective April 1, 2023

This is an English translation of the regulations written in Japanese and is for information purposes only.

Table of Contents

Chapter 1 General provisions

Article 1 Purpose

These Regulations establish the basic criteria for the handling of personal information or equivalent at National Research and Development Institute RIKEN for the appropriate and smooth conduct of its business and to protect the rights and interests of the individual.

Article 2 Definitions

1. The terms used in these Regulations are prescribed in these Regulations and also based on the Act on the Protection of Personal Information (2003, Act No. 57; hereafter “Personal Information Protection Act”), the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (2013, Act No. 27; hereafter “Numbers Act”) and the government ordinances and rules, etc. delegated by these laws.
2. In these Regulations, “personal information” means information concerning a living individual that falls under any of the following items.
   (1) Information that can be used to identify a specific individual (including information that can be easily cross-checked with other information and thereby used to identify a specific individual), such as name, date of birth, or other descriptions, that are posted or recorded in documents, drawings, or electromagnetic records created using electromagnetic methods (electronic, magnetic, or other methods that cannot be recognized by human perception; the same shall apply in item 2 of the following paragraph), or expressed by means of voice, motion, or other methods (excluding personal identification codes).
   (2) Items that contain personal identification codes.
3. The term "personal identification code" in these Regulations means a character, number, symbol, or other code that falls under any of the following items and is specified by a government ordinance.
   (1) Characters, numbers, symbols, or other codes that are converted from the physical characteristics of a specific individual for use in computers and that can identify said specific individual
   (2) Characters, numbers, symbols, or other codes that are assigned in connection with the use of services provided to an individual or the purchase of goods sold to an individual, or that are described on a card or other documents issued to an individual or recorded by an electromagnetic method, so that they can be used to identify each user, purchaser, or person to whom they are issued.
4. The term “sensitive personal information” as used in these Regulations means personal information that includes the individual's race, creed, social status, medical history, criminal record, the fact that the person has been harmed by a crime, or any other description specified by a government ordinance as requiring special consideration in its handling so as not to cause unjust discrimination, prejudice, or other disadvantage to the individual.
5. The term "personal data" in these Regulations means personal information that constitutes personal information databases or equivalent.
6. The term “personal information databases or equivalent” in these Regulations means a collection of

information that contains personal information and is listed below (excluding those specified by a government ordinance as being unlikely to harm the rights and interests of individuals in light of the method of use).

(1) Information that is systematically organized so that specific personal information can be retrieved using a computer

(2) In addition to the information described in the preceding paragraph, information that is specified by a government ordinance as being systematically organized so that specific personal information can be easily retrieved.

7. The term “pseudonymously processed information” in these Regulations means information on individuals obtained by processing personal information using the measures stipulated in the items below in accordance with the categories of personal information so that specific individuals cannot be identified unless it is cross-checked with other information.

(1) Personal information falling under paragraph 2, item 1: Deletion of a part of descriptions, etc. included in the personal information (including replacing such part of descriptions, etc. with other descriptions, etc. by a method that does not have regularity with which such descriptions can be restored, etc.).

(2) Personal information falling under Paragraph 2, Item 2: Deletion of all of the personal identification code contained in the personal information (including replacement of the personal identification code with another description, etc. by a method that does not have regularity with which the personal identification code can be restored).

8. The term “anonymized personal information” in these Regulations means information on individuals obtained by processing personal information using the measures stipulated in the items below in accordance with the categories of personal information so that specific individuals cannot be identified, and their personal information is unrecoverable.

(1) Personal information falling under paragraph 2, item 1: Deletion of a part of descriptions, etc. contained in the personal information (including replacing such part of descriptions, etc. with other descriptions, etc. by a method that does not have regularity with which such descriptions can be restored, etc.).

(2) Personal information falling under paragraph 2, item 2: Deletion of all of the personal identification code contained in the personal information (including replacing the personal identification code with another description, etc. by a method that does not have regularity with which the personal identification code can be restored).

9. The term “personally relevant information” in these Regulations means information on living individuals that does not fall under any of the categories of personal information, anonymized personal information, or pseudonymously processed information.

10. The term "retained personal information" in these Regulations means personal information created or obtained by employees in the course of their duties, and retained by RIKEN for organizational use by its employees. However, it shall be limited to information recorded in corporate documents prescribed in the items of Article 2, paragraph 2 (including those described in item 4 of the same paragraph) of the “Act on Access to Information Held by Independent Administrative Agencies” (Act No. 140 of 2001).

11. The term “personal information file” in these Regulations means a collection of information containing retained personal information, which includes the following.

(1) A file that is systematically organized so that specific retained personal information can be retrieved using a computer in order to achieve a certain business purpose

(2) In addition to the file described in the preceding item, information that is systematically organized so that specific retained personal information can be easily retrieved by name, date of birth, or other descriptions in order to achieve a certain business purpose

12. The term “anonymized personal information retained by administrative organizations” as used in these Regulations means all or part of the retained personal information that constitutes a personal information file that falls under any of the following items (except for information that is subject to the Non-Disclosure of Information prescribed in Article 5 of the Act on Access to Information Held by Independent Administrative Agencies (Act No. 140 of 2001, hereinafter referred to as the "Incorporated Administrative Agency Information Access Act"), which excludes the information listed in item 2 of the same Article and includes the information prescribed in the proviso of item 2 of the same Article).

(1) The information shall fall under any of the items of Article 75, paragraph 2 of the Personal Information Protection Act or shall be exempted from being listed in the personal information file book prescribed in paragraph 1 of the same Article pursuant to paragraph 3 of the same Article.

(2) If Incorporated Administrative Agencies, which are prescribed in Article 2, paragraph 1 of the Incorporated Administrative Agency Information Access Act, receive a request for disclosure of the corporate documents in which the retained personal information constituting the relevant personal information file is recorded (meaning a request for disclosure pursuant to the provisions of Article 3 of the Incorporated Administrative Agency Information Access Act), they shall conduct any of the following matters.
(a) Decide to disclose all or part of the retained personal information recorded in their administrative documents.
(b) Give an opportunity to submit a written opinion pursuant to the provisions of Article 14, paragraph 1 or paragraph 2 of the Incorporated Administrative Agency Information Access Act.

(3) To the extent that it does not hinder the proper and smooth operation of the affairs and business of the Incorporated Administrative Agencies, anonymized personal information may be created by processing the retained personal information that constitutes the personal information file in accordance with the standards of Article 114, paragraph 1 of the Personal Information Protection Act.

13. The term "anonymized personal information file retained by administrative organizations" as used in this Chapter means a collection of information containing anonymized personal information and refers to as the following.
(1) A file that is systematically structured so that anonymized personal information retained by a specific administrative organization can be retrieved using a computer.
(2) In addition to what is listed in the preceding item, information specified by a government ordinance as information that is systematically organized so that anonymized personal information retained by administrative organizations can be easily retrieved.
14. In these Regulations, "personal information or equivalent" means personal information, pseudonymously processed information, anonymized personal information, personally relevant information, and other information defined by the Personal Information Protection Act and subject to said Act, and information defined by the Numbers Act and subject to said Act.
15. In these Regulations, "designated personal Information or equivalent" means personal identification numbers and other designated personal information.
16. In these Regulations, "employees*"* refers to RIKEN executive officers, permanent and indefinite-term employees, fixed-term employees, and all others primarily engaged in conducting RIKEN business (including dispatched agency staff).

Chapter 2 Management framework for the protection of personal information or equivalent

Article 3 General Manager for Personal Information

1. There shall be a General Manager to oversee the management of personal information or equivalent at RIKEN
2. The Executive Director in charge of general affairs shall be the General Manager for Personal Information.

Article 4 General Affairs Division Director

The General Affairs Division Director shall assist the General Manager for Personal Information and shall supervise administrative work that handles personal information or equivalent.

Article 5 Personal Information Managers

1. One person in each office and section of RIKEN's administrative divisions and equivalent research organizations, as stipulated in Article 35, paragraph 1 and Article 36, paragraph 1 of the RIKEN Organization Regulations (2018, Reg. No. 1) and equivalent organizations (hereinafter referred to as "section or equivalent organization") that handle personal information or equivalent shall be appointed as Personal Information Manager.
2. The Personal Information Manager must be the manager or a person of higher rank of the section, or equivalent organization, and is responsible for all administrative matters concerning the management of personal information or equivalent for the section or laboratory.
When personal information or equivalent is used through the online information system, the Personal Information Manager must work with the system administrator to ensure appropriate use and management.
3. The Personal Information Manager may appoint one or more people from among the people in the section or equivalent organization to be Personal Information Administrators. Personal Information

Administrators shall assist the Personal Information Manager and engage in administrative work related to management of personal information or equivalent.

4. In cases where personal information is handled directly by an organization other than a section or equivalent organization, said organization shall be deemed to be a section or equivalent organization, and these Regulations shall apply.

Article 6 Committee

1. In making decisions and notifications regarding important matters related to management of personal information or equivalent, the General Manager for Personal Information may call regular or periodic meetings of the Disclosure and Personal Information Protection Committee.
2. Provisions for the Disclosure and Personal Information Protection Committee are set forth in the RIKEN Regulations for the Establishment of a Disclosure and Personal Information Protection Committee (2003, Reg. No. 23).

Chapter 3 Education and training

Article 7 Education and training

1. The General Manager for Personal Information shall carry out educational activities and training as necessary to increase understanding and raise awareness among designated employees who handle personal information or equivalent of the importance of protecting personal information.
2. The General Manager for Personal Information shall carry out educational activities and training of employees involved in managing information systems that handle personal information or equivalent, regarding the appropriate management, operation, and security measures for personal information or equivalent to ensure that personal information or equivalent is properly managed. However, when education and training concerning information system management, operation, and security measures are provided by other organizations within RIKEN, if the General Manager for Personal Information approves that that education and training meet the standards necessary for the education and training under this paragraph, the implementation of the education and training under this paragraph shall be deemed to be fulfilled with the completion of said education and training.
3. The General Manager for Personal Information shall carry out educational activities and training for Personal Information Managers and Personal Information Administrators to ensure that personal information or equivalent is properly managed in the workplace.
4. Personal Information Managers must ensure that the relevant employees in their section or equivalent organization have the opportunity to participate in training programs related to the management of personal information or equivalent that are implemented by the General Manager for Personal Information.

Chapter 4 Handling of personal information or equivalent

Article 8 Employee responsibilities

1. Employees must handle personal information or equivalent in accordance with the Personal Information Protection Act, the Numbers Act, and the relevant ordinances and regulations, under the instructions of the General Manager for Personal Information, the General Affairs Division Director, and the Personal Information Managers.

Article 9 Controlled access

1. The Personal Information Manager must determine, in accordance with the confidentiality of personal information or equivalent (including whether individuals can be easily identified (such as degree of anonymization), whether extra care is necessary for specific information, and the degree and characteristics of damage that would be caused by leakage of personal information), and keep the number of employees with access rights to personal information or equivalent and the extent of their access to the minimum necessary for the employees with access rights to perform their duties.
2. Employees without access rights must not access personal information or equivalent.
3. Even employees with access rights must not access personal information or equivalent for purposes other than those required by RIKEN business.

Article 10 Specification of purpose of use

1. In handling personal information, employees shall specify the purpose of use as much as possible.

2. When employees change the purpose of use, an amended purpose of use shall not go beyond the scope that is reasonably considered to be relevant to the original purpose of use.

Article 11 Limitation to access depending on the purpose of use

1. Employees shall not handle personal information beyond the scope necessary for the purpose of use specified in the preceding Article without obtaining prior consent of the individual concerned.
2. In the event that RIKEN has acquired personal information as a result of succession of business from a business operator handling the personal information due to a merger or otherwise, employees shall not, except in the following cases, handle said personal information beyond the scope necessary for the original purpose of use before the business succession without obtaining the prior consent of the individual concerned.
3. The provision in the preceding two paragraphs shall not apply to the following cases.
   (1) When applicable legal provisions exist.
   (2) When it is necessary to protect the life, body, or property of the individual and it is difficult to obtain the consent of the individual.
   (3) When it is necessary to improve public health or ensure the health of children and it is difficult to obtain the consent of the individual.
   (4) When it is necessary to cooperate with a national agency, a local government, or an individual or entity entrusted by either of the former two authorities to execute affairs prescribed by law, and obtaining the consent of the individual is likely to impede such cooperation.
   (5) When said personal information is to be used for academic research purposes, including cases where part of the purpose of handling said personal information is for academic research. Cases where there is a risk of unreasonable infringement on the rights and interests of the individual are excluded.
   (6) When personal data (personal information constituting personal information databases, etc.) is provided to an academic research organization and the like, and the academic research organization needs to handle the personal data for academic research purposes, including cases where part of the purpose of handling the personal information is for academic research. Cases where there is a risk of unreasonable infringement on the rights and interests of the individual are excluded.

Article 12 Prohibition of inappropriate use

1. Employees shall not use personal information in a manner that may encourage or induce illegal or inappropriate conduct.
2. Employees must not inform others of the contents of personal information acquired in the course of business or use that information for unreasonable purposes.

Article 13 Appropriate acquisition

1. Employees must not acquire personal information under false pretenses or by other inappropriate means.
2. Employees shall not acquire sensitive personal information without obtaining the prior consent of the individual, expect in the following circumstances:
   (1) When applicable legal provisions exist.
   (2) When it is necessary to protect the life, body, or property of the individual and it is difficult to obtain the consent of the individual.
   (3) When it is necessary to improve public health or ensure the health of children and it is difficult to obtain the consent of the individual.
   (4) When it is necessary to cooperate with a national agency, a local government, or an individual or entity entrusted by either of the former two in executing affairs prescribed by law, and obtaining the consent of the individual is likely to impede such cooperation.
   (5) When the sensitive personal information is to be used for academic research purposes, including cases where part of the purposes of obtaining the personal information is for academic research. Cases where there is a risk of unreasonable infringement on the rights and interests of the individual are excluded.
   (6) When sensitive personal information is obtained from an academic research organization and the like, and the personal information is required for academic research purposes, including cases where part of the purposes of obtaining the personal information is for academic research. Cases where there is a risk of unreasonable infringement on the rights and interests of the individual are excluded. (This applies only when RIKEN and the academic research organization jointly conduct academic research.)
   (7) When the sensitive personal information has been disclosed by any of the persons listed in the items of Article 57, paragraph 1 of the Personal Information Protection Act or any other persons specified in

the rules of the Personal Information Protection Commission, including the individual, national agency, local government, and academic research institution concerned.

(8) Other cases specified by a government ordinance as equivalent to the cases listed in the preceding items.

Article 14 Notification of purpose of use in obtaining personal information

1. When employees acquire personal information for a business purpose, they shall promptly notify the individual concerned of the purpose of use, or publicly announce such purpose of use, except in cases where the purpose of use has been publicly announced in advance.
2. Notwithstanding the provisions of the preceding paragraph, when employees, in order for RIKEN to sign a contract with the individual, acquire personal information from the individual as described in the contract or other documents (including electromagnetic records; hereinafter the same shall apply in this paragraph) or acquire personal information concerning the individual directly from the individual in writing, the employees shall clearly indicate the purpose of use to the individual in advance. However, this shall not apply in cases where it is urgently necessary for the protection of the life, body or property of the individual.
3. In the event that RIKEN changes the purpose of use, employees shall notify the individual concerned of the changed purpose of use or publicly announce it.
4. The provisions of the preceding three paragraphs shall not apply to the following cases.
   (1) When notifying the individual concerned of the purpose of use or publicly announcing it may harm the life, body, property, or other rights or interests of the individual or third parties.
   (2) When notifying the individual concerned of the purpose of use or publicly announcing it is likely to harm the rights or legitimate interests of RIKEN.
   (3) When it is necessary to cooperate with government organizations or local public entities in performing administrative procedures prescribed by law, and notifying the individual concerned of the purpose of use or publicly announce it is likely to impede the performance of such procedures.
   (4) When it is recognized that the purpose of use of personal information is clear in view of the circumstances under which the personal information was acquired.

Article 15 Copy restrictions

Employees must follow instructions from their Personal Information Manager for any of the following actions related to personal information. Even when employees handle personal information for business purposes, the following actions shall be limited according to the confidentiality of the personal information and the contents, and employees shall follow the instructions of the Personal Information Manager.

(1) Copying of personal information
(2) Transmitting of personal information
(3) Transmitting or otherwise taking out of RIKEN media on which personal information is recorded
(4) Any other action that might affect the management of personal information

Article 16 Ensuring accuracy of data

1. Employees shall keep personal data accurate and updated to the extent necessary to fulfil the purpose of use, and shall endeavor to delete the personal data without delay when there is no longer a need to use it.
2. Employees must, in accordance with the level of importance of the personal data in the information system, verify that the information on the original data entry form and that entered into the system are the same; check that the personal data after processing is accurate; and check the data against previously retained personal data.
3. When employees discover an error in personal data, they must correct the error under instruction from the Personal Information Manager.

Article 17 Media management

Employees, under instruction from a Personal Information Manager, must store all media containing personal information or equivalent (including those stored in the terminals and servers. The same shall apply in the following Article.) in a specified place, and when deemed necessary, store such media in a locked or fireproof safe.

Article 18 Media disposal

When personal information or equivalent, or media containing personal information or equivalent is no longer needed, employees must, under instruction from a Personal Information Manager, erase the information or destroy the media so that the personal information cannot be read or reproduced.

Article 19 Safety management measures

1. RIKEN must take necessary and appropriate measures to prevent the leakage, loss or corruption of personal data and otherwise ensure that such data is appropriately managed.
2. When employees handle personal data, they must follow the measures in the preceding paragraph and RIKEN's supervision to ensure the safe management of such personal data.

Article 20 Supervision of commissioned agents

1. When commissioning all or some of the tasks which involve handling of personal data to an agent outside of RIKEN, necessary measures must be taken for the secure management of personal data, such as selecting a person capable of appropriately handling personal data to engage in the relevant work.
   The commission contract must specify the following items, and necessary matters must be confirmed in writing, such as the responsible person and the management and implementation system of business operators at the commissioned agent, and matters concerning inspections of the state of personal data management.
   (1) Obligations regarding personal data, including confidentiality and prohibition of use for other purposes
   (2) Limitations and conditions for sub-contracting, such as requirement of prior approval—possible subcontractors may include a subsidiary of the contractor as defined in Article 2, item 3 in the Companies Act (2005, Act. No. 86); this applies to the rest of the items below and to paragraph 6
   (3) Limitations on copying of personal data
   (4) Procedures to be followed in the case of leakage, loss, or corruption of personal data
   (5) Procedures for erasing and returning media containing personal data at the end of the period of commission
   (6) Conditions for cancelling the contract if there is violation of any of the contract provisions, and conditions for compensation for damages
2. When all or some of the tasks which involve handling of personal data are commissioned to an agent outside RIKEN, the Personal Information Manager must conduct an on-site inspection at least once a year concerning the agent's manner of handling and managing commissioned tasks and managing personal data, depending on the degree of the confidentiality and the volume of information.
3. When a commissioned agent sub-contracts tasks concerning personal data, it must be ensured that the commissioned agent takes necessary measures as set forth in the provisions of paragraph 1, and the measures described in the preceding paragraph shall be taken by RIKEN or through the commissioned agent, depending on the degree of the confidentiality of the personal data. The same applies when a sub-contracting agent sub-contracts related tasks to another party.
4. When a dispatch agency staff person is required to handle personal data, provisions for handling of personal data including confidentiality obligations must be specified in the dispatch agency contract.
5. When providing personal data or commissioning tasks that require handling of personal data to an agent outside of RIKEN, necessary measures should be taken to minimize damage from potential leakage of personal data in accordance with the purposes of use, tasks to be commissioned to the agent, and the degree of confidentiality of personal data, such as replacing individuals' names with identifying numbers.
6. When all or some of the tasks which involve handling of personal information that is not considered personal data are commissioned to an agent outside RIKEN, paragraph 5 shall apply only if RIKEN considers it necessary.

Article 21 Limitation on provision of personal data to third parties

1. Employees shall not provide personal data to a third party without obtaining the prior consent of the individual concerned, expect in the following circumstances:
   (1) Applicable legal provisions exist
   (2) When it is necessary to protect the life, body, or property of the individual and it is difficult to obtain the consent of the individual.
   (3) When it is necessary to improve public health or ensure the health of children and it is difficult to obtain the consent of the individual.
   (4) When it is necessary to cooperate with a national agency, a local government, or an individual or entity entrusted by either of the former two in executing affairs prescribed by law, and obtaining the consent of the individual is likely to impede such cooperation.
   (5) When said personal data must be provided for the publication of the results of academic research or for educational purposes. Cases where there is a risk of unreasonable infringement on the rights and interests of the individual are excluded.
   (6) When the personal data is to be used for academic research purposes, including cases where part of the purposes of providing the personal data is for academic research. Cases where there is a risk of

unreasonable infringement on the rights and interests of the individual are excluded. (This applies only when RIKEN and the academic research organization jointly conduct academic research.)

(7) When the third party is an academic research organization and the like, and the third party needs to use the personal data for academic research purposes, including cases where part of the purposes of using the personal information is for academic research. Cases where there is a risk of unreasonable infringement on the rights and interests of the individual are excluded.

2. With respect to personal data to be provided to a third party, where the provision to the third party of personal data that can identify the individual concerned is being suspended at the request of the individual, if employees notify the individual or make the personal data easily accessible to the individual in advance in accordance with the rules of the Personal Information Protection Commission, and report on the notification to the Personal Information Protection Commission, they may provide the personal data to the third party, notwithstanding the provisions of the preceding paragraph. However, if the personal data to be provided to the third party is sensitive personal information, acquired in violation of Article 13, paragraph 1 or obtained from a business operator handling personal information pursuant to the provision of this paragraph (including those copied or processed in whole or in part), the personal data may not be provided to the third party.
   (1) Name and address of RIKEN and the name of its representative
   (2) Purpose of use of personal data is to provide personal data to third parties
   (3) Items of personal data to be provided to third parties
   (4) Means to acquire personal data to be provided to third parties
   (5) Means to provide personal data to third parties
   (6) Provision to third parties of personal data that identifies the individual concerned may be suspended at the request of the individual
   (7) Means to accept the request of the individual
   (8) Other matters prescribed by the rules of the Personal Information Protection Commission as necessary to protect the rights and interests of individual
3. When there has been a change in the matters listed in item 1 of the preceding paragraph, or when the provision of personal data pursuant to the provisions of the preceding paragraph has been cancelled, RIKEN shall, without delay, notify the individual concerned of such change, or make such change easily accessible to the individual, as provided for in the rules of the Personal Information Protection Commission. When intending to change the matters listed in items 3, 4, 5, 7 and 8 of the preceding paragraph, RIKEN must, in the same manner, in accordance with the rules of the Personal Information Protection Commission, notify the individual concerned of such change or make such changes readily accessible to the individual, and notify the Personal Information Protection Commission of such changes in advance.
4. In the following circumstances, the person to whom the personal data concerned is provided shall not be considered a third party with respect to the application of the provisions in the preceding paragraphs.
   (1) When said personal data is provided in conjunction with the entrustment of all or part of the handling of personal data within the scope necessary to fulfil the purpose of use
   (2) When personal data is provided as a result of the succession of business due to merger or other reasons
   (3) When personal data that will be used jointly with a specific person is provided to said specific person, and RIKEN has, in advance, notified the individual concerned or made readily accessible to the individual the items of personal data to be jointly used, the scope of the joint users, the purpose of use by the users, the name and address of the person (or corporation) responsible for the management of said personal data, and the name of the representative, in the case that a corporation is the joint user.
5. When there has been a change in the name or address of the person (or corporation) responsible for the management of personal data, as prescribed in item 3 of the preceding paragraph, RIKEN must, without delay, notify the individual concerned of such change, or make such change easily accessible to the individual, and when RIKEN intends to change the purpose of use by the users, the person (or corporation) responsible for the management of said personal data, RIKEN must, in advance, notify the individual concerned of such change, or make such change easily accessible to the individual.

Article 22 Limitations on provision to third parties overseas

1. When RIKEN provides personal data to third parties (excluding those who have established an appropriate system that conforms to the standards prescribed by the rules of the Personal Information Protection Commission to continuously take measures, hereinafter referred to as "equivalent measures" in paragraph 3, required for business operators handling personal information regarding handling of personal data in accordance with the provisions in Chapter 4, clause 2 of the Personal Information Protection Act. The same shall apply hereinafter in this paragraph, the next paragraph and items.) in countries overseas (meaning

countries or regions outside Japan; hereinafter the same shall apply in this Article and Article 25, paragraph 1, item 2) (excluding countries overseas that have a system to protect personal information, which is recognized to be at the same level as that of Japan in protecting the rights and interests of individuals, as defined by the rules of the Personal Information Protection Commission. The same shall apply hereinafter in this Article and the same item.), employees must obtain the consent of the person concerned in advance regarding the provision of personal data to a third party located in a foreign country, except in the cases listed in the items of paragraph 1 of the preceding Article. In this case, the provisions of the preceding Article shall not apply.

2. When employees intend to obtain the consent of the individual pursuant to the provision of the preceding paragraph, they must, pursuant to the rules of the Personal Information Protection Commission, provide the individual in advance with information on systems concerning the protection of personal information in the relevant foreign country, measures taken by the relevant third party for the protection of personal information, and other reference information to the individual.
3. After RIKEN provides personal data to a third party overseas (limited to those who have established an appropriate system prescribed in paragraph 1), employees must, pursuant to the rules of the Personal Information Protection Commission, take necessary measures to ensure the continuous implementation of the corresponding measures by the third party, and provide information concerning such necessary measures to the individual concerned upon request of the individual.

Article 23 Preparation of records pertaining to provision to third parties

1. When RIKEN provides personal data to a third party (excluding those listed in the items of Article 16, paragraph 2 of the Personal Information Protection Act. The same shall apply hereinafter in this Article and the following Article, including cases where it is applied mutatis mutandis by replacing the terms and phrases in Article 25, paragraph 3.), employees must prepare a record of the date of provision of said personal data, the name of said third party, and other matters specified by the rules of the Personal Information Protection Commission, pursuant to the rules of the Personal Information Protection Commission. However, this shall not apply where the provision of said personal data falls under any of the items of Article 21, paragraph 1 or paragraph 4 (any of the items of Article 21, paragraph 1, regarding provision of personal data pursuant to paragraph 1 of the preceding Article).
2. Employees shall retain the records described in the preceding paragraph for the period of time in accordance with the rules of the Personal Information Protection Commission from the date of creation of said records.

Article 24 Confirmation before receiving personal data from third parties

1. When RIKEN receives personal data from a third party, employees shall confirm the following matters as prescribed by the rules of the Personal Information Protection Commission.
   (1) The name and address of the third party and, the name of its representative in the case that a corporation is the third party.
   (2) History of acquisition of said personal data by said third party

   However, this shall not apply where the provision of the personal data falls under any of the items of Article 21, paragraph 1 or paragraph 4.
2. When confirming the matters pursuant to the preceding paragraph, employees shall, in accordance with the rules of the Personal Information Protection Commission, keep a record of the date the personal data received, the matters required to be confirmed, and other matters prescribed by the rules of the Personal Information Protection Commission.
3. Employees shall retain the records set forth in the preceding paragraph for the period of time prescribed by the rules of the Personal Information Protection Commission from the date of creation of said records.

Article 25 Limitations on provision of personally relevant information to third parties

1. When it is expected that a third party will acquire personally relevant information (limited to that which constitutes personally relevant information databases, and the same shall apply in this Article) as personal data, except in the cases listed in the items of paragraph 1, Article 21, employees shall not provide such personally relevant information to the third party without confirming the following matters in accordance with the rules of the Personal Information Protection Commission.
   (1) The consent of the individual concerned has been obtained to allow the third party to receive personal data as personally identifiable information from RIKEN through the provision of personally relevant information to the third party.
   (2) In the case of provision to a third party in a foreign country, when the consent of the individual set forth in the preceding item is to be obtained, prior to such provision, in accordance with the rules of the Personal Information Protection Commission, the individual concerned shall receive the information about the system concerning protection of personal information in the foreign country,

measures taken for protection of personal information by the third party, and other reference information to the individual.

2. The provisions of paragraph 3, Article 22 shall apply mutatis mutandis to the case where a business operator handling personally relevant information provides personally relevant information pursuant to the preceding paragraph. In this case, the phrase “take necessary measures to ensure the continuous implementation of the corresponding measures by the third party, and provide information concerning such necessary measures to the individual concerned upon request of the individual concerned” in Paragraph 3 of the same article shall be replaced with “take necessary measures to ensure the continuous implementation of the corresponding measures by the third party.”
3. The provisions of paragraphs 2 and 3 of the preceding Article shall apply mutatis mutandis to the case where RIKEN confirms the matters pursuant to the provisions of paragraph 1. In this case, the phrase “data received” in paragraph 3 of the same Article shall be replaced with “data provided.”

Article 26 Worker responsibility regarding provision of personal data or personally relevant information

When RIKEN is requested by a third party to confirm the items of Article 30, paragraph 1 or those of Article 31, paragraph 1 of the Personal Information Protection Act in providing personal data or personally relevant information to the third party, employees shall not falsely report the matters that require confirmation to the third party.

Article 27 Creating pseudonymously processed information

1. When creating pseudonymously processed information (limited to that which constitutes pseudonymously processed information databases and the like. The same shall apply in this Article and the following Article.), personal information shall be processed in accordance with the standards prescribed by the rules of the Personal Information Protection Commission to make it impossible to identify a specific individual unless it is collated with other information.
2. When creating pseudonymously processed information, or when obtaining pseudonymously processed information and deleted information generated (meaning descriptions and personal identification codes deleted from personal information in the course of creating the pseudonymously processed information, as well as information on the method of processing pursuant to the preceding paragraph. The same shall apply hereinafter in this Article and in paragraph 3 of the following Article and in paragraph 7 as applied mutatis mutandis by replacing the terms and phrases.), employees shall take measures for secure management of the deleted information in accordance with the standards prescribed in the rules of the Personal Information Protection Commission as necessary to prevent leaks of the deleted information.
3. Notwithstanding the provisions of Article 11, except as required by laws and regulations, employees shall not handle pseudonymously processed information (limited to personal information) beyond the scope necessary to achieve the purpose of use specified pursuant to the provisions of Article 10, paragraph 1.
4. With respect to the application of the provisions of Article 14 regarding pseudonymously processed information, the phrase “notify the individual concerned… or publicly announce” in paragraphs 1 and 3 of Article 12-2 shall be replaced with "publicly announce" and the phrase “notifying the individual concerned… or publicly announcing” in items 1 through 3 of paragraph 4 of the same Article shall be replaced with “publicly announcing.”
5. When there is no longer a need to use personal data that is pseudonymously processed information and deleted information, employees shall endeavor to delete the personal data and deleted information without delay. In this case, the provisions of Article 16 shall not apply.
6. Notwithstanding the provisions of Article 21, paragraphs 1 and 2 and Article 22, paragraph 1, employees shall not provide pseudonymously processed information to a third party since it is personal data, except as required by law. In this case, the phrase “the preceding paragraphs” in Article 21, paragraph 4 shall be replaced with “Article 27, paragraph 5,” and the phrase “notify the individual concerned…, or make such change easily accessible to the individual” in Article 21, paragraph 4, item 3 shall be replaced with “publicly announce such change.” The phrase “must notify the individual concerned of such change, or make such change easily accessible to the individual” in the Article 21, paragraph 5 shall be replaced with “must publicly announce such change.”
   In the proviso of Article 23, paragraph 1, the phrase “any of the items of Article 21, paragraph 1 or paragraph 4 (any of the items of Article 21, paragraph 1, regarding provision of personal data pursuant to paragraph 1 of the preceding Article)” and the phrase “any of the items of Article 21, paragraph 1 or paragraph 4” in the proviso of Article 24, paragraph 1 shall be replaced with “in accordance with laws and regulations or any of the items of Article 21, paragraph 4”.
7. In handling pseudonymously processed information, employees shall not collate said pseudonymously

processed information with other information in order to identify individuals with respect to personal information used to create said pseudonymously processed information.

8. In handling the pseudonymously processed information, employees shall not use information included in the said pseudonymously processed information, such as contact information, to make telephone calls, send letters by mail or by general delivery service operators prescribed in "Article 2, paragraph 6 of the Act on Correspondence Delivery by Private Business Operators (Act, No. 99 of 2002)" or by specified delivery service operators prescribed in paragraph 9 of the same article, send telegrams, send messages using a facsimile device or electromagnetic method (a method using an electronic data processing system or other information communication technology, which is prescribed by the rules of the Personal Information Protection Commission), or visit the residence of the individual.
9. The provisions of Article 10, paragraph 2 and Article 20 shall not apply to pseudonymously processed information, including personal information constituting personal information databases.

Article 28 Limits on the provision of pseudonymously processed information to third parties

1. Employees shall not provide pseudonymously processed information (excluding personal information; the same shall apply in paragraphs 2 and 3) to any third parties except in accordance with laws and regulations.
2. The provisions of Article 21, paragraphs 4 and 5 shall apply mutatis mutandis to a person who receives pseudonymously processed information. In this case, the phrase “the preceding paragraphs” in paragraph 4 of the same article shall be replaced with “Article 27, paragraph 1,” and the phrase “notified the individual or made readily accessible to the individual” in item 3 of the same paragraph shall be replaced with “publicly announced,” and the phrase “notify the individual concerned of such change, or make such change easily accessible to the individual” in paragraph 5 of the same article shall be replaced with “publicly announce”.
3. The provisions of Article 19 and paragraphs 7 and 8 of the preceding Article shall apply mutatis mutandis to the handling of pseudonymously processed information by employees. In this case, the phrase “leakage, loss or corruption” in Article 19 shall be replaced with “leakage,” and the phrase “in order to” in paragraph 7 of the preceding Article shall be replaced with “obtain deleted information in order to.”

Article 29 Reporting of security violations and preventive measures

1. When employees notice or suspect that there is a breach of security regarding personal information, such as a leak, loss, or corruption of personal information or find or suspect that the staff handling personal information are breaking the law and regulations related personal information, they must promptly report it to the relevant Personal Information Manager.
2. The Personal Information Manager must promptly implement measures to contain the damage and restore security. Prior to this, however, in cases where there may have been unauthorized access or a computer virus is suspected, those on site must take immediate action, such as by detaching the LAN cable.
3. The Personal Information Manager must investigate the cause of the problem and extent of damage and report to the General Affairs Division Director. In the event of a major breach or leak of personal information, the Personal Information Manager must immediately report on the occurrence to the General Affairs Division Director.
4. Upon receipt of the report cited above, and depending on the extent of the damage incurred, the General Affairs Division Director must promptly have the information conveyed to the RIKEN President through the General Manager for Personal Information. Likewise, the General Affairs Division Director shall promptly provide information to the Ministry of Education, Culture, Sports, Science and Technology (MEXT) through the General Manager for Personal Information on the nature of the breach, what led up to it, and the extent of the damage.
5. The Personal Information Manager must investigate the cause of the problem and implement the necessary measures to prevent a reoccurrence.
6. The General Affairs Division Manager must, depending on the extent and repercussions resulting from the problem, implement measures to make public the nature of the damage and the measures implemented to contain it and prevent a reoccurrence, and must implement countermeasures for the persons whose personal information has been compromised.

Article 30 Reporting of leakage

1. In the event of leakage, loss, corruption, or any other situation pertaining to the security of personal data handled by RIKEN, which is specified by the rules of the Personal Information Protection Commission as being highly likely to cause damage to the rights and interests of individuals, RIKEN shall report to the Personal Information Protection Commission to the effect that such a situation has occurred, as provided for in the rules of the Personal

Information Protection Commission. However, this shall not apply where the handling of said personal data has been entrusted in whole or in part by a business operator handling personal information or an administrative organization, etc. and they have been notified of the occurrence of said situation pursuant to the provisions of the rules of the Personal Information Protection Commission.

2. In the case prescribed in the clause of the preceding paragraph, RIKEN shall notify the individual concerned of the occurrence of such a situation pursuant to the provisions of the rules of the Personal Information Protection Commission. However, this shall not apply when it is difficult to notify the individual, and alternative measures are taken to protect the rights and interests of the individual.

Article 31 Information security

RIKEN shall implement measures to prevent the leak or other security breach of personal data, in accordance with the Supplementary Regulations for the Security of Personal Data (2005, Supp. Reg. 8) and other internal regulations related to information security as well as these Regulations.

Chapter 5 Creation and public release of record book on personal information files, etc.

Article 32 Notices regarding possession of personal information files

1. When retaining personal information files, the Personal Information Manager for the section or equivalent organization must give advance notice to the General Affairs Division Director of the following items. This also applies when making changes.
   (1) Names of personal information files
   (2) Name of the group or organization in charge of the procedures that make use of the information in the files
   (3) Purpose for which the personal information files will be used
   (4) Items to be included in the personal information files (hereinafter, "recorded items") and the limitations on the personal information to be recorded in the personal information files, which is limited to information that can be retrieved without using the name, date of birth, or other description. The same shall apply in the item 9 of the following paragraph. (hereinafter, "recording limits"), and the estimated number of individuals whose information will be in the files
   (5) The personal information to be recorded in the personal information file (hereinafter, "recorded information")
   (6) Notation of recorded information when it includes sensitive personal information
   (7) When recorded information will be regularly supplied to a person or organization outside of RIKEN, the name of that person or organization
   (8) Name and address of the organization that accepts disclosure requests pursuant to Article 76, paragraph 1 of the Personal Information Protection Act, correction requests pursuant to Article 90, paragraph 1 of the Personal Information Protection Act, or suspension of use requests pursuant to Article 98, paragraph 1 of the Personal Information Protection Act
   (9) The names of the relevant laws and regulations that require special procedures regarding the correction requests and suspension of use requests described in the preceding item
   (10) Designation of the format of the personal information record (electronic or paper)
   (11) In the case of an electronic file, indicate whether there is also a paper file stipulating the use and recording limits of the personal information
   (12) Notation of any files that might be converted to anonymized personal information retained by administrative organizations for calls for proposals regarding anonymized personal information retained by administrative organizations.
2. The above items do not apply to the following types of personal information files.
   (1) Personal information files of employees or equivalent persons that are to be used for recording personnel appointments, salary, social security matters and equivalent information (including test results at the time of hire)
   (2) Personal information files to be exclusively used for experimental computer processing
   (3) A personal information file that contains all or part of the recorded information requiring the advanced notice referred to in the preceding paragraph, and for which the use, recorded items, and recording limits are within the same range as those stipulated for the file requiring advanced notification
   (4) Personal information files that only contain recorded information that will be erased within one year
   (5) A personal information file containing necessary contact information for the sending of documents,

goods, or money or for contacting regarding work-related matters, matters related to work, and which contact information is limited to the person's name, address and other information necessary for contacting the person or sending the person items.

(6) A personal information file created or acquired at the initiative of employees for the purpose of scientific research that contains information to be used for the scientific research in question

(7) A personal information file containing data on fewer than 1,000 persons

(8) Any personal information files specified by government ordinances as equivalent to those listed in the preceding items

(9) Any personal information files containing all or part of data recorded in personal information files pertaining to the public release pursuant to Article 25, preceding paragraph 1, whose purpose of use, recorded items, and recorded limitation are within the scope of these items pertaining to the public release.

(10) Any personal information files specified by the government ordinances as equivalent to those listed in the preceding item

(11) Any personal information files that are systematically structured so that specific personal information can be easily retrieved by name, date of birth, or other descriptions for a certain administrative purpose (excluding, however, information that can be retrieved by using a computer).

3. Regardless of the provisions of paragraph 1 above, if recording any of the recorded items, the information cited in paragraph 1, items 5 and 6 or listing any of personal information files in a record book of personal information files may significantly hinder the appropriate carrying out of administrative work and business operation pertaining to the purpose of use due to the nature of such administrative work and business operation, a part or all of the recorded items may be left unrecorded or the personal information file may not be included in the record book of personal information files.
4. When maintaining designated personal information files within a section or equivalent organization, the Personal Information Manager must notify in advance the General Affairs Division Director of the items stipulated in Article 28, paragraph 1 of the Numbers Act. The same procedures will be applied when there are changes to the designated personal information files.
5. After receiving the notice on the items mentioned above, the General Affairs Division Director shall take necessary procedures to obtain approval from the Personal Information Protection Commission, based on the Article 28 of the Numbers Act.

Article 33 Creation and public release of a record book of personal information files

1. The General Affairs Division Director shall create and announce publicly a record book of personal information files based on the notices provided in accordance with paragraph 1 of the article above.
2. The conditions for the creation and public release of the record book of personal information files noted in the paragraph above are stipulated in the relevant laws, regulations and the Government Directive No. 3 (2005) on disclosure and corrections of a record book of personal information files and retained personal information.

Article 34 Exemptions

Retained personal information (limited to information recorded in corporate documents that exclusively contain non-disclosed information as prescribed in Article 5 of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies) of which classification or other arrangement has not yet been made, and from which it is extremely difficult to retrieve specific personal information from the extremely large amount of information pertaining to the same purpose of use, shall be deemed not to be retained by RIKEN with respect to the application of the provisions of this Chapter. The same shall apply in the following Chapter.

Chapter 6 Disclosure, corrections, and termination of use

Article 35 Disclosure, corrections, and termination of use

RIKEN shall disclose, correct, and terminate retained personal information as stipulated in these Regulations, the relevant laws, regulations, and directives of disclosure, etc.

Chapter 7 Anonymized personal information

Article 36 Provision of anonymized personal information retained by administrative organizations

RIKEN shall create and provide anonymized personal information retained by administrative organizations in accordance with Government Directive No. 33 (2017) on provision of anonymized personal information retained by administrative institutions.

Article 37 Prohibition to identification

1. In handling anonymized personal information retained by administrative organizations, employees shall not, except as required by laws and regulations, collate said anonymized personal information retained by administrative organizations with other information in order to identify the individual whose personal information that was used to create the anonymized personal information retained by administrative organizations.
2. To prevent leakage of anonymized personal information retained by administrative organizations, deleted information stipulated in Article 109, paragraph 4 of the Personal Information Protection Act, and information concerning the processing method prescribed in Article 116, paragraph 1 of the Personal Information Protection Act (hereinafter referred to as "anonymized personal information retained by administrative organizations" in this Article and the following Article), RIKEN shall comply with the standards established by the rules of the Personal Information Protection Commission and take necessary measures for appropriate management of anonymized personal information retained by administrative organizations, and employees shall follow the measures.
3. The provisions of the preceding two paragraphs shall apply mutatis mutandis to the case where a person or entity who has been entrusted with the handling of anonymized personal information retained by administrative organizations (including entrustment over two or more stages) by RIKEN performs the entrusted operations.

Article 38 Obligations of the engaged employees

Employees or former employees who are or were engaged in the handling of anonymized personal information retained by administrative organizations, shall not disclose to others without reason, or use for unjust purposes, the contents of anonymized personal information retained by administrative organizations that are obtained in the course of their work.

Article 39 Obligations when handling anonymized personal information

1. If RIKEN provides anonymized personal information (excluding anonymized personal information retained by administrative organizations, and the same shall apply in this Article) to a third party, RIKEN shall, except as required by laws and regulations, publicly announce in advance the items of information concerning individuals contained in the anonymized personal information to be provided to the third party and the method of provision, in accordance with the rules of the Personal Information Protection Commission, and clearly indicate to the third party that the information to be provided is anonymized personal information.
2. In handling anonymized personal information, RIKEN must not, except as required by laws and regulations, obtain descriptions deleted from personal information, personal identification codes, or information on the processing method used pursuant to the provisions of Article 43, paragraph 1 of the Personal Information Protection Act, and collate said anonymized personal information with other information in order to identify the individual whose personal information that was used to create the anonymized personal information.
3. To prevent leakage of anonymized personal information, RIKEN shall comply with the standards established by the rules of the Personal Information Protection Commission and take necessary measures for appropriate management of anonymized personal information.
4. The provisions of the preceding two paragraphs shall apply mutatis mutandis to cases where a person or entity who has been entrusted with the handling of anonymized personal information (including entrustment over two or more stages) by RIKEN performs the entrusted operations.

Chapter 8 Complaints

Article 40 Complaints

1. RIKEN must respond to and act promptly on complaints regarding the handling of personal information, pseudonymously processed information or anonymized personal information.
2. Complaints regarding personal information should be directed to the General Administration Section of the General Affairs Division.
3. When there is a complaint, the section or equivalent organization concerned must respond promptly to investigate the status of the handling of pseudonymously processed information or anonymized personal information relevant to the complaint and take appropriate measures to correct the situation upon consultation with the General Affairs Division Director.
4. When deemed appropriate, the General Manger for Personal Information should oversee the measures undertaken in response to a complaint.
5. When deemed appropriate and necessary, the results of the actions undertaken in response to a complaint

should be reported in writing to the person who made the complaint.

Chapter 9 Special provisions concerning handling of designated personal information or equivalent

Article 41 Special provisions concerning handling of designated personal information or equivalent

This Chapter sets forth special provisions concerning the handling of designated personal information or equivalent. Matters not provided for in this Chapter shall be in accordance with the provisions of the Numbers Act and other related laws and regulations, including government ordinances and regulations entrusted by the Numbers Act.

Article 42 Personal Information Manager of a section or equivalent organization that handles designated personal information or equivalent

1. The Personal Information Manager of a section or equivalent organization that handles designated personal information or equivalent shall designate the employees who handle the designated personal information or equivalent (hereinafter referred to as "staff handling designated personal information") and assign them the relevant roles.
2. Personal Information Manager of a section or equivalent organization that handles designated personal information or equivalent shall specify the scope of designated personal information or equivalent handled by the staff handling designated personal information.
3. Personal Information Manager of a section or equivalent organization that handles designated personal information or equivalent shall develop the following systems.
   (1) Reporting system to the Personal Information Manager if staff handling the designated personal information are found to be in violation of the rules and regulations in handling the designated personal information or equivalent.
   (2) Reporting system from employees to the Personal Information Manager in the event of the occurrence or signs of leakage, loss, damage, etc. of designated personal information or equivalent.
   (3) Clarification of duties and responsibilities of each division when designated personal information or equivalent is handled by multiple divisions
   (4) Response system for if the occurrence or signs of leakage, loss, or damage of designated personal information or equivalent are detected
4. When designated personal information or equivalent is directly handled by an organization other than the section or equivalent organization, said organization shall be deemed to be the section or equivalent organization within RIKEN and these Regulations in this Chapter shall apply.

Article 43 Limitation on use of personal identification numbers

Employees must use personal identification numbers within the scope of the personal identification number-related administrative work that is limited by the Numbers Act, and only to the extent necessary for the performance of RIKEN's business affairs.

Article 44 Limitation on requests to provide personal identification numbers

Employees must not request others (i.e., other than those who belong to the same household as themselves. The same shall apply in the parentheses of the following Article, paragraph 2.) to provide their personal identification numbers except when handling administrative work using personal identification numbers and in the other limited cases stipulated by the Numbers Act.

Article 45 Limitation on provision, collection and retention of designated personal information or equivalent

1. Employees must not provide designated personal information except in the cases that fall under any of the items, Article 19 in the Numbers Act.
2. Employees must not collect or retain designated personal information (limited to the information containing others' personal identification numbers), except in the cases that fall under any of the items, Article 19 in the Numbers Act.

Article 46 Limitation on creation of designated personal information files

1. Employees must not create designated personal information files except when handling administrative work using personal identification numbers and in the other limited cases stipulated by the Numbers Act.
2. When intending to retain a designated personal information file (excluding those which record matters concerning personnel affairs, salaries, or welfare of employees or former employees of RIKEN, or those otherwise provided for by the rules of the Personal Information Protection Commission; hereinafter the same shall apply in this Article), the Personal Information Manager of the section or equivalent organization concerned shall, prior to retaining the designated personal information file, notify the Director of the General Affairs Division of the matters listed in each item of Article 28, paragraph 1 of the Numbers Act. The same shall apply when a significant change is to be made to said designated personal information file as prescribed by the rules of the Personal Information Protection Commission.
3. Upon receiving the notification set forth in the preceding paragraph, the Director of the General Affairs Division shall, if necessary, perform the procedures necessary for approval by the Personal Information Protection Commission in accordance with Article 28 of the Numbers Act.

Article 47 Records on the handling of designated personal information or equivalent

The Personal Information Manager must develop the procedures to check the status of handling designated personal information or equivalent and maintain records of how the information is used and stored. Designated personal information shall not be entered in the record book for checking the status.

Article 48 Scope of handling and security measures for personal identification numbers

1. The Personal Information Manager must clarify the scope of administrative work using designated personal information and take physical security measures.
2. The Personal Information Manager shall take necessary and appropriate measures, in addition to the preceding paragraph, to prevent leakage, loss, or damage of the personal identification numbers handled and for security of other personal data.
3. In handling personal data, employees must comply with the measures prescribed in the preceding two paragraphs and RIKEN's supervision for security control of the personal data concerned.

Article 49 Commissioning administrative work using personal identification numbers

1. When a section or equivalent organization outsources all or part of the personal identification numbers-related administrative work, the Personal Information Manager of the section or equivalent organization shall confirm in advance whether or not the commissioned agent will be able to take measures equivalent to the security control measures taken by RIKEN based on the Numbers Act.
2. The Personal Information Manager of a section or equivalent organization that handles designated personal information or equivalent shall, when commissioning all or part of the personal identification number-related administrative work, exercise necessary and appropriate supervision to ensure that the commissioned agent takes measures equivalent to the security control measures taken by RIKEN.
3. The Personal Information Manager of a section or equivalent organization that handles designated personal information or equivalent must, when a commissioned agent subcontracts all or part of the personal identification number-related administrative work to a subcontractor, determine whether to accept or reject the subcontract after confirming that the subcontractor will ensure appropriate security control of the designated personal information handled in the commissioned personal identification number-related administrative work. The same shall apply in the case of re-consignment by the subcontractor and thereafter.

Article 50 Implementation of training

When retaining or intending to retain a designated personal information file, the General Manager for Personal Information, pursuant to the provisions of a government ordinance, must provide the staff handing designated personal information with training related to ensuring "cyber security," which means cyber security as prescribed in Article 2 of the "Cyber Security Basic Act" (2014, Act, No. 104), and the relevant matters, in order to ensure that designated personal information is handled appropriately. However, if another organization within RIKEN provides training related to ensuring cyber security and the relevant matters, and the General Manager for Personal Information finds that such training meets the level required for the training under this Article, then the implementation of such training may be deemed as the implementation of the training under this Article.

Article 51 Reports on leakage of designated personal information

1. In the event of leakage, loss, or damage of designated personal information recorded in a designated personal information file, or other incidents pertaining to the security of designated personal information that are specified by the rules of the Personal Information Protection Commission as being highly likely to cause damage to the rights and interests of individuals, RIKEN must, pursuant to the rules of the Personal Information Protection Commission, report to the Commission that such an incident has occurred. However, this shall not apply where RIKEN has been commissioned to handle all or part of said personal identification number-related administrative work by another party and has notified the party of the occurrence of said incident, pursuant to the rules of the Personal Information Protection Commission.
2. In the case prescribed in the preceding paragraph (excluding cases where notification has been given pursuant to the proviso of the same paragraph), RIKEN must notify the individual concerned of the occurrence of such an incident in accordance with the rules of the Personal Information Protection Commission. However, this shall not apply in cases where it is difficult to notify the individual concerned and alternative measures necessary to protect the rights and interests of the individual concerned are taken.

Article 52 Special provisions of the Personal Information Protection Act

1. The provisions of Article 11, paragraph 3, items 3 through 6; Article 13, paragraph 2; Articles 21 through 24; and Article 26 of these Regulations shall not apply to the designated personal information retained or to be retained by RIKEN.
2. In cases where provisions of these Regulations, except those listed in the preceding paragraph, are applied by replacing the terms and phrases pursuant to the provisions of Article 30, paragraph 2 of the Numbers Act, the terms and phrases shall be replaced as shown in the following table.

Provisions	Terms and phrases to be replaced	Replaced with
Article 11, paragraph 1	"in the preceding Article without obtaining prior consent of the individual concerned."	in the preceding Article
Article 11, paragraph 2	"before the business succession without obtaining the prior consent of the individual concerned."	before the business succession
Article 11, paragraph 3, item 1	"When applicable legal provisions exist."	When the provision of Article 9, paragraph 5 applies
Article 11, paragraph 3, item 2	"it is difficult to obtain the consent of the individual."	the consent of the individual has already been obtained or it is difficult to obtain the consent of the individual.

3. With respect to personal identification numbers, these Regulations shall apply even after the death of the individual concerned.

Chapter 10 Audits and inspections

Article 53 Audits

1. There shall be a person responsible for audits at RIKEN.
2. The person responsible for audits shall be the director of the Auditing Office.
3. The person responsible for audits must make regular, and as necessary, audits of the management of personal information or equivalent.
4. The General Affairs Division Director, Personal Information Managers, and Personal Information Administrators must cooperate with the carrying out of audits.
5. The person responsible for audits must report the results to the General Manager for Personal Information.

Article 54 Inspections

The Personal Information Manager of a section or equivalent organization should regularly and as necessary inspect recording media of personal information or equivalent, the procedures by which they are processed, and how they are stored. When deemed necessary, a report must be made through the General Affairs Division Director to the General Manager for Personal Information.

Article 55 Evaluations and reviews

The General Manager for Personal Information must evaluate the effectiveness, etc. of measures for appropriate management of personal information or equivalent, based on audit results, and if deemed necessary, review and modify the measures. In addition, the General Manager for Personal Information, General Affairs Division Director, and Personal Information Managers must evaluate the effectiveness, etc. of measures for appropriate management of personal information or equivalent, based on inspection results, and if deemed necessary, review and modify the measures.

Article 56 Collaboration with government agencies

RIKEN shall collaborate closely with the Personal Information Protection Commission and Ministry of Education, Culture, Sports, Science and Technology (MEXT) regarding the appropriate management of personal information or equivalent in accordance with the provisions of the Basic Policy on the Protection of Personal Information approved by the Cabinet on April 2, 2004.