RIKEN Regulations for Donations

January 25, 2007, Reg. 3
Latest revision: March 24, 2021, Reg. 381

This English translation is for information purposes only. Any questions regarding interpretation are to be resolved using the original Japanese document.

Article 1 Purpose

The purpose of these Regulations is to establish RIKEN's policies and standards concerning donations made to RIKEN, including such monetary donations as cash and securities, donations of goods, real estate including land and buildings, intellectual property rights, and the like.

Article 2 Standards for acceptance

RIKEN may accept donations that meet any of the criteria listed in the following items.

(1) The donation contributes to the achievement of the goals presented in Article 3 of the RIKEN Law (2002, Law No. 160).
(2) None of the following conditions are attached to the acceptance of the donation.
   (a) Provision of benefit or service in compensation for the donation.
   (b) Auditing of the donated accounts by the donor.
   (c) Option of the donor to cancel all or part of the donation after it has been made.
   (d) Gratuitous transfer to or use of the donation by the donor.
(3) The donor does not fall under the category of antisocial forces as stipulated in Article 2, Item 1 of the Regulations for handling anti-social forces (Regulation No. 179, July 2019).
(4) There is no excessive operational or financial burden or impediment to RIKENas a result of accepting the donation.

Article 3 Types of donations

RIKEN may accept the following types of donations.

(1) General donation: The donor does not specify how the donation is to be used, and RIKEN specifies how the donation is to be used.
(2) Specified donation: The donation is to be applied to one of the following predetermined uses.
   (a) Donation for specific use: The donor specifies how the donation is to be used.
   (b) Donation made in response to requests for funds: RIKEN initiates a fund-raising campaign for a specific undertaking or purpose, specifying amounts and how the donations are to be made as well as the duration of the campaign.

Article 4 Procedures for receiving a donation

1. A person or organization that wishes to make a donation to RIKEN must submit a separately provided Donation Application Form to RIKEN entering the donor's name and contact information, the purpose of the donation, the monetary amount or name of the goods donated, and other relevant information.
2. Upon receipt of the application form specified in the above clause, RIKEN must check that the donation meets the conditions of Article 2 and decide whether or not to accept the donation.
3. When it is decided to accept a donation, RIKEN will advise the donor of the

decision and send the donor the necessary documents, including a deposit form, for the donor to make the donation.

Article 4-2
If any one of the following items is applicable, the provisions of the preceding article shall be disregarded and RIKEN shall accept monetary donations

(1) When payment is received based on the cooperative agreement for the donation.
(2) When a donor places money into a donation box inscribed with the standards of acceptance stipulated in Article 2.
(3) When a monetary donation is remitted by a donor using a bank remittance form printed by RIKEN inscribed with the standards of acceptance stipulated in Article 2.

Article 5 Management of donations
Donations accepted by RIKEN shall be managed in accordance to RIKEN's rules and regulations.

Article 6 General expenses
1. Upon receipt of a donation as stipulated in Article 3, RIKEN shall receive a portion of the amount for general expenses.
2. The amount for general expenses shall be 10% of the amount donated.

Article 7 Period of use for donations
If there are no special requirements at the time of receiving a donation, the donation is to be used within the fiscal year in which the donation is received. This period may be extended, however, if RIKEN deems there is an appropriate and rational reason for the extension.

Article 8 Change in use
RIKEN may change how a donation is to be used for any one of the following reasons.

(1) The original purpose for the donation has been achieved and there is still a small amount of the donation left.
(2) The period of use for the donation as specified in the preceding Article has expired.
(3) It has been decided for appropriate and rational reasons to change theemployee or organization for which the donation was originally applied.

Article 9 Transferring of donations
RIKEN may transfer a donation for any of the following reasons.

(1) The employee making use of the donation for specific use transfers to another research or similar institution and the related donation is to be transferred to that institution. In this case, RIKEN will not, in principle, return the amount that was originally deducted for general expenses as stipulated in Article 6, Clause 2.
(2) The employee making use of the donation for specific use transfers to RIKEN from another research or similar institution. In this case, RIKEN will deduct from the donation general expenses as stipulated in Article 6.

Article 10 Exceptions

All or part of these Regulations may not apply to the donor if any one of the following items apply.

(1) It is possible to manage the donation in accordance with the provisions of other RIKEN rules and regulations.
(2) The donation is being made by the national government, an Independent Administrative Institution, a regional public or community organization or the like.
(3) RIKEN determines that there are special extenuating circumstances.

Article 11 Other matters

Additional matters concerning donations that are not covered by these Regulations may be decided separately as necessary.

Supplementary provisions

1. These Regulations are effective as of February 1, 2007.
2. The provisions of Articles 7 and 8 shall apply to donations received by RIKEN before these Regulations became effective. In the case of donations that were made to RIKEN more than three years ago as of March 31, 2007, however, such donations must be used by no later than March 31, 2008.

These regulations are effective as of April 1, 2021. However, the provisions in Article 7 shall also apply to donations received prior to this revision.

Excerpt: Regulations for Training Expenses for Human Resources Development Paid by Specific Donation

(Regulation No. 37, September 3, 2009)

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

Article 1 Purpose

The purpose of these Regulations is to set forth the handling standard for specific donations partially used for human resources development for RIKEN (hereinafter referred to as 'RIKEN'), in order to cover training expenses for human resources development of skills and quality improvement of young researchers, and to achieve the sound operation thereof.

(1) Specific donations refer to the specified donation defined in item 2, Article 3 of the RIKEN Regulations for Donations (Regulations, No. 3, 2007) and shall be partially used for human resources development.

Article 3 Training Expenses

Training expenses shall be the cost of holding the training, expendables for the operation, invitation compensation, travel expenses and printing for material, etc. as well as food and drink expenses served at the Training or at a social gathering held after the Training (hereinafter referred to as 'Social gathering').

Article 5 Providing Food and Drink

1. Snacks at Training or food and drink at Social gathering may be provided only in cases where contributors have agreed.
2. Location of Social gathering shall be within the RIKEN when the Training is held thereat, and may be held outside the RIKEN when the Training is held outside thereof.
3. The maximum amount of expenses pertaining to the Social gathering is as follow:
   (1) 2,000 Yen per person if held within the RIKEN.
   (2) 3,000 Yen per person if held outside the RIKEN.

Personal Information Protection Regulations

Kojin jyoho hogo kitei

March 10, 2005, Reg. 6

With revisions effective March 24, 2022

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 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, *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 Framework for the protection of personal information

Article 3 General Manager for Personal Information

1. There shall be a General Manager to oversee the management of personal information 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 measures to manage personal information.

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 of the RIKEN Organization Regulations (2018, Reg. No. 1), that handle personal information shall be appointed as Personal Information Manager.
2. The Personal Information Manager must be the manager or a person of higher rank of the office, section, or equivalent organization, such as a laboratory, and is responsible for all administrative matters concerning the management of personal information for the section or laboratory.

   When personal information 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 laboratory to be Personal Information Administrators. Personal Information Administrators shall assist

the Personal Information Manager in managing personal information.

4. The Personal Information Manager of the section or laboratory that handles designated personal information (personal information including personal identification numbers which are given to every person possessing a resident record) appoints staff to handle designated personal information and decides their duties.
5. The Personal Information Manager of the section or laboratory that handles designated personal information decides the scope of the designated personal information that may be handled by the appointed staff.
6. The Personal Information Manager of the section or laboratory that handles designated personal information must set up procedures for the following processes.
   (1) A process for employees to notify the Personal Information Manager when the appointed staff person has violated, or may violate, the regulations for handling designated personal information.
   (2) A process for employees to notify the Personal Information Manager when designated personal information has been leaked, lost, or corrupted, or there is a possibility that it will be leaked, lost or corrupted.
   (3) A process for designating and clarifying the tasks and responsibilities of each section or department when multiple sections or departments handle designated personal information.
   (4) A process for dealing with the leakage, loss, or corruption of designated personal information.

Article 6 Committee

1. In making decisions and notifications regarding important matters related to management of personal information, 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 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, regarding the appropriate management, operation, and security measures for personal information.
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 is properly managed in the workplace.
4. Personal Information Managers must ensure that the relevant employees in their section or organization have the opportunity to participate in training programs related to the management of personal information implemented by the General Manager for Personal Information.

Chapter 4 Handling of personal information

Article 8 Employee responsibilities

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

Article 9 Controlled access

1. The Personal Information Manager must determine, in accordance with the degree of sensitivity (including whether individuals can be identified with the information), 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 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.
3. Even employees with access rights must not access personal information 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 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 11-2 Prohibition of inappropriate use

Employees shall not use personal information in a manner that may encourage or induce illegal or inappropriate conduct.

Article 12 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.

3. Employees shall not collect personal information concerning ideology, religion, and beliefs, or personal information that may cause social discrimination. However, this provision shall not apply when required by law or when indispensable for judicial procedures.
4. Employees must acquire personal information directly from the individual concerned, in principle. However, personal information may be acquired by other means in the following circumstances.
   (1) Permission has been granted by the individual
   (2) Applicable legal provisions exist
   (3) The information is publicly available in publications or the media
   (4) The information is urgently required to protect human life or property or prevent bodily injury
   (5) The individual's whereabouts are unknown
   (6) The information is needed for administrative procedures related to a lawsuit, selection process, instruction or consultation, and it is recognized that the information acquired directly from the individual would not fulfil the required purpose or would hinder the normal performance of the administrative procedures due to the nature of the procedures.
   (7) When it is deemed unavoidable to obtain the information from a government agency, independent administrative institution, regional public organization, or regional independent administrative institution for administrative procedures, and it is clear that there will be no risk of infringement on the rights and interests of the individual.
   (8) When the information will be used exclusively in a compilation of statistics or for scholarly research and it is clear that there will be no risk of infringement on the rights and interests of the individual.

Article 12-2 Notification of purpose of use in obtaining personal information

1. When employees acquire personal information, 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 signing 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 the purpose of use has been changed, 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 the business operator handling the personal information.
   (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 13 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 14 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 shall, 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 15 Media management

Employees, under instruction from a Personal Information Manager, must store all media containing personal information in a specified place, and when deemed necessary, store such media in a locked or fireproof safe.

Article 16 Media disposal

When personal information or media containing personal information 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 17 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.
3. 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 having a person capable of appropriately handling personal data engage in the relevant work. The commission contract must specify the following items, and there must be a written itemized list of items requiring inspection such as the agent's management organization, responsible persons, and procedures and security measures for the handling of personal information.
   (1) Requirement of confidentiality and prohibition against unauthorized use
   (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 information
   (4) Procedures to be followed in the case of leakage, loss, or corruption of personal information
   (5) Procedures for erasing and returning media containing personal information at the end of the period of commission
   (6) Conditions for cancelling the contract when there is violation of any of the contract provisions, and conditions for compensation for damages
4. When all or some of the tasks related to personal identification numbers are commissioned to an agent outside of RIKEN, there must be prior confirmation that the agent can implement the same security measures as those required of RIKEN under the provisions of the preceding paragraph and the Numbers Act.
5. When all or some of the tasks which involve handling of personal information 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 of personal information, depending on the degree of the confidentiality and the volume of information.
   When all or some of the tasks related to personal identification numbers are commissioned to an agent outside of RIKEN, the agent must be properly supervised so that it can implement the same security measures as those required of RIKEN.

6. When the commissioned agent sub-contracts tasks concerning personal information, it must be ensured that the commissioned agent takes necessary measures as set forth in the provisions of paragraph 3, 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 information. The same applies when the sub-contracting agent sub-contracts related tasks to another party.
   When the agent handling all or some of the tasks related to personal identification numbers wishes to sub-contract related tasks to another party, in addition to the measures explained above, it must be confirmed whether the party can manage designated personal information securely in performing tasks related to personal identification numbers and whether confidentiality security measures are in place before approving recommissioning of the tasks to the party.
7. When a dispatch agency staff person is required to handle personal information, confidentiality and security provisions must be included in the dispatch agency contract.
8. When providing personal information or commissioning work requiring the handling of personal information to an agent outside of RIKEN, necessary measures including replacing individual names with identifying numbers should be taken based on the purposes of use, tasks to be commissioned to the agent, and the degree of confidentiality of personal information to minimize damage by leakage of personal information.

Article 18 Worker responsibility

1. The persons listed below must not give out personal information to which they have access in the process of their work to unauthorized third parties or use this information for inappropriate purposes.
   (1) All employees at RIKEN including former employees who handle or handled personal information in the course of their work.
   (2) All persons who are or were affiliated with the agent commissioned by RIKEN to handle personal information as per Article 17, paragraph 2 above.
2. 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 personal related information to the third party, employees shall not falsely report the matters that require confirmation to the third party.

Article 19 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 20, 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 20 Limitations on provision to third parties overseas

1. When employees provide 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 this clause. 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 23, 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.), the consent of the person concerned must be obtained 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 employees provide personal data to a third party overseas (limited to those who have established an appropriate system prescribed in paragraph 1), they 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 20-2 Preparation of records pertaining to provision to third parties

1. When employees provide 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 20-4, paragraph 2.), 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 shall be prepared, 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 19, paragraph 1 or paragraph 4 (any of the items of Article 19, 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 20-3 Confirmation before receiving personal data from third parties

1. When receiving 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 19, paragraph 1 or paragraph 4.
2. When confirming the matters pursuant to paragraph 1, 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 20-4 Limitations on provision of personal related information to third parties

1. When it is expected that a third party will acquire personal related information (limited to that which constitutes personal related information databases) as personal data, except in the cases listed in the items of paragraph 1, Article 19, employees shall not provide such personal related 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 personal related 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 20 shall apply mutatis mutandis to the case where a business operator handling personal related information provides personal related 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 20-5 Creating pseudonymously processed information

1. When creating pseudonymously processed information (limited to that which constitutes pseudonymously processed information databases and the like), 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), 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 12-2 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 14 shall not apply.
6. Notwithstanding the provisions of Article 19, paragraphs 1 and 2 and Article 20, paragraph 1, a business operator handling pseudonymously processed information 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 19, paragraph 4 shall be replaced with "Article 20-5, paragraph 6," and the phrase "notify the individual concerned…, or make such change easily accessible to the individual" in Article 19, paragraph 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 19, paragraph 5 shall be replaced with "must publicly announce such change."
   In the proviso of Article 20-2, paragraph 1, the phrase "any of the items of Article 19, paragraph 1 or paragraph 4 (any of the items of Article 19, paragraph 1, regarding provision of personal data pursuant to paragraph 1 of the preceding Article)" and the phrase "any of the items of Article 19, paragraph 1 or paragraph 4" in the proviso of Article 20-3, paragraph 1 shall be replaced with "in accordance with laws and regulations or any of the items of Article 19, 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 17-2 shall not apply to pseudonymously processed information, including personal information constituting personal information databases.

Article 20-6 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 19, 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 20-5, 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 17 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 17 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 21 Record on the handling of personal information

1. The Personal Information Manager shall, depending on the nature of personal information and the need for confidentiality, maintain a record book of the use, handling and storage of personal information.
2. The Personal Information Manager must implement procedures for the handling of designated personal information files and must maintain records of how the information is used and stored.

Article 21-2 Limits on the handling of personal identification numbers

The Personal Information Manager must limit the handling of personal identification numbers for tasks specified in the Numbers Act.

Article 21-3 Limits on requests for 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 Article 21-5.) 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 21-4 Limits on the compilation of designated personal information files

Employees must not compile designated personal information files except when handling administrative work using personal identification numbers and in the other limited cases stipulated by the Numbers Act.

Article 21-5 Limits on the collection and storage of designated personal information Employees must not provide designated personal information and must not collect or store designated personal information including others’ personal identification numbers with the exception of the cases stipulated in the paragraphs listed under Article 19 of the Numbers Act.

Article 21-6 Physical location

The Personal Information Manager must specify the physical location in which designated personal information will be handled and must take all necessary precautions to ensure the location is secure.

Article 22 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 should 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 should promptly have the information conveyed to the RIKEN President through the General Manager for Personal Information.

Likewise, the General Affairs Division Director should 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 22-2 Reporting of leakage

1. In the event of leakage, loss, corruption, or any other situation pertaining to the security of personal data or designated personal information 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 23 Information security

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

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

Article 24 Notices regarding possession of personal information files

1. When retaining personal information files, the Personal Information Manager for the section or division 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")
   (5)-2 Notation of recorded information when it includes sensitive personal information
   (6) When recorded information will be regularly supplied to a person or organization outside of RIKEN, the name of that person or organization
   (6)-2 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
   (7) 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

(8) Designation of the format of the personal information record (electronic or paper)
(9) 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
(10) Notation of any files that might be converted to pseudonymously processed information for calls for proposals regarding pseudonymously processed information

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 laboratory, the Personal Information Manager must notify in advance the General Affairs Division Director of the items stipulated in Article 28, paragraph 1 of the Number 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 Number Act.

Article 25 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 25-2 Exemptions

Personal Information (limited to those 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, etc.) 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 to Chapters 6 and 6-2.

Chapter 6 Disclosure, corrections, and termination of use

Article 26 Disclosure, corrections, and termination of use

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

Chapter 6-2 Pseudonymously processed information

Article 26-2 Provision of pseudonymously processed information

RIKEN shall provide pseudonymously processed information in accordance with Government Directive No. 33 (2017) on provision of pseudonymously processed information retained by independent administrative institutions.

Article 26-3 Prohibition to identification

1. In handling pseudonymously processed information, employees shall not, except as required by laws and regulations, collate said pseudonymously processed information with other information in order to identify the individual whose personal information that was used to create the pseudonymously processed information.
2. To prevent leakage of pseudonymously processed information, deleted information stipulated in Article 107, paragraph 4 of the Personal Information Protection Act, and information concerning the processing method prescribed in Article 114, paragraph 1 of the Personal Information Protection Act (hereinafter referred to as “pseudonymously processed information, etc.” 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 pseudonymously processed information, etc., 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 pseudonymously processed information, etc. (including entrustment over two or more stages) by RIKEN performs the entrusted operations.

Article 26-4 Obligations of the engaged employees

Employees or former employees who are or were engaged in the handling of pseudonymously processed information, etc., shall not disclose to others or use for unjust purposes the contents of pseudonymously processed information, etc. obtained in connection with their work without reason.

Chapter 7 Complaints

Article 27 Complaints

1. RIKEN must respond to and act promptly on complaints regarding the handling of personal information.
2. Complains 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 division concerned must respond promptly to investigate the problem 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 8 Special provisions concerning designated personal information

Article 27-2 Application
The application of these regulations to specified personal information shall be in accordance with the provisions of Articles 30 and 31 of the Numbers Act, in addition to the provisions of these regulations.

Chapter 9 Audits and inspections

Article 27-3 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.
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 28 Inspections
The Personal Information Manager should regularly and as necessary inspect personal information records, the procedures by which they are processed, and how they are stored. When deemed necessary, a report should be made through the General Affairs Division Director to the General Manager for Personal Information.

Article 28-2 Evaluations and reviews
The General Manager for Personal Information shall review and implement appropriate measures for the handling and management of personal information as deemed necessary following audit results and to the extent that implementation is possible. The General Manager for Personal Information, General Affairs Division Director, and Personal Information Managers shall review and implement appropriate measures for the handling and management of personal information as deemed necessary following inspection results and to the extent that implementation is possible.

Article 29 Collaboration with government agencies
RIKEN shall collaborate closely with MEXT regarding the appropriate management of retained personal information in accordance with the provisions of the Basic Policy on the Protection of Personal Information approved by the Cabinet on April 2, 2004.