RIKEN Regulations for Donations

January 25, 2007, Reg. 3
Latest revision: November 22, 2019, Reg. 212

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 all of the following criteria.

(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 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) Donor must not be a member of or associated with any antisocial forces stipulated in Article 2, paragraph 1 of the Regulations for handling antisocial forces (July 2019, Reg. 179).
(4) There is no excessive operational or financial burden or impediment to RIKEN as 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 a donor makes a donation using RIKEN's public website screen for donation by credit card, and the donor has indicated agreement with the standards of acceptance stipulated in Article 2 above.
(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 3 years. 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 the employee 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 may deduct from the donation general expenses as stipulated in Article 6.

Article 10 Exceptions

All or part of these Regulations may not apply in the event of any one of the following.

(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.

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 June 11, 2020

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 based on Article 2 of the Act on the Protection of Personal Information Held by Independent Administrative Agencies (2003, Act No. 59; hereafter "Personal Information Protection Act") and Article 2 of the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (2013, Act No. 27; hereafter "Numbers Act").
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).
3. Notwithstanding the provisions of paragraph 1, in these Regulations, *retained personal information* is personal information retained by RIKEN that is systematically acquired and recorded in the line of work and used institutionally by RIKEN employees, but which is limited to personal information recorded in the *corporate documents* stipulated in Article 2, paragraph 2 of the Act on Access to Information Held by Independent Administrative Agencies (2001, Act. No. 140).

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 retained personal information and individual numbers at RIKEN (hereinafter collectively referred to as "retained personal information").
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 retained 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 retained 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 retained personal information for the section or laboratory.

   When personal information is retained or 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 retained personal information.
4. The Personal Information Manager appoints staff to handle individual numbers and other designated personal information (hereafter "designated personal information") and decides their duties.
5. The Personal Information Manager decides the scope of the designated personal information that may be handled by the appointed staff persons.
6. The Personal Information Manager 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 retained personal information, the General Manager for Personal Information may call regular or periodic meetings of a 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 retained personal information of the importance of protecting personal information including designated personal information.
2. The General Manager for Personal Information shall carry out educational activities and training of employees involved in managing online information systems, regarding the appropriate management, operation, and security measures for retained personal information.
3. The General Manager for Personal Information shall carry out educational activities and training of Personal Information Managers and Personal Information Administrators.

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.
2. Employees must promptly report to 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, and when an appointed staff person who handles personal information has violated, or may violate, the regulations for handling personal information.

Article 9 Controlled access

1. The Personal Information Manager must, in accordance with the degree of privacy (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, keep to a minimum the number of employees with access rights to retained personal information and the extent of their access.
2. Employees without access rights must not access retained personal information.
3. Even employees with access rights must not access retained personal information for purposes other than those required by RIKEN business.

Article 10 Limits on retaining personal information including designated personal information

1. Employees may retain personal information including designated personal information only for purposes required by law and must specify those purposes to the extent possible.
2. Employees must not retain personal information including designated personal information for purposes that go beyond the requirements noted above.
3. When employees change the purpose for which personal information will be used, they should not do so beyond the extent to which such change is relevant to the original purpose.
4. Employees must not collect personal information including designated personal information that may lead to discrimination such as information related to ideology, religious faith or belief. This does not apply, however, when there are legal provisions or when required for legal procedures.

Article 11 Statement of reasons for use

When acquiring written personal information (including personal information recorded on electronic or magnetic media that cannot be confirmed by human sensory perception; hereinafter referred to as “electronic data”) from an individual, employees must explain in advance the purposes for which the personal information will be used, except in the following cases:

(1) When the information is urgently required to protect human life or assets or prevent bodily injury
(2) When explaining the purpose for which the personal information will be used is likely to harm the life, body, property, or other rights or interests of the person or a third party
(3) When explaining the purpose for which the personal information will be used is likely to harm the operation or activities of government agencies, independent administrative institutions, regional public organizations or regional independent administrative institutions
(4) When the purpose for which the personal information will be used is obvious from the circumstances in which the information is provided

Article 12 Appropriate acquisition

1. Employees must not acquire personal information including designated personal information under false pretenses or by other inappropriate means.
2. Employees must acquire personal information including designated personal information directly from the individual concerned, expect in the following circumstances:
   (1) Permission has been granted by the individual
   (2) There are applicable legal provisions
   (3) The information is publicly available in publications or the media
   (4) The information is urgently required to protect human life or assets or prevent bodily injury
   (5) The individual's whereabouts are unknown
   (6) The information is needed for a lawsuit, selection process, instruction or consultation and would not serve the required purpose, or would hinder the normal execution of duties, if it were acquired directly from the individual
   (7) When the normal conduct of business requires that the information be acquired from a government agency, other independent administrative institution, regional public organization, or regional independent administrative institution, and it is clear that there will be no disadvantage to the individual
   (8) When the information will be used in a compilation of statistics or for scholarly research and it is clear that there will be no disadvantage to the individual

Article 13 Copy restrictions

Employees must follow instructions from their Personal Information Manager for any of the following actions related to retained personal information.

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

Article 14 Ensuring accuracy

1. Employees must, to the extent necessary for the purpose for which the information will be used, ensure that retained personal information (excluding non-identifiable processed information limited to non-identifiable processed information files, and deleted information as defined by Article 44-2, paragraph 3 and Article 24, paragraph 3, item 3, of the Personal Information Protection Act) is accurate for both past and current information.
2. Employees must, in accordance with the level of importance of the retained personal information 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 retained personal information after processing is accurate; and check against already retained personal information.
3. When employees discover an error in retained personal information, 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 retained personal information in a specified place, and when deemed necessary, store such media in a locked or fireproof safe.

Article 16 Media disposal

When retained personal information or media containing retained 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 retained personal information cannot be read or reproduced.

Article 17 Safety measures

1. RIKEN must take every precaution to prevent the leakage, loss or corruption of retained personal information and otherwise ensure that such information is appropriately stored.
2. The above provision applies equally to those outside of RIKEN who have been commissioned to handle RIKEN's retained personal information.
3. When commissioning work requiring the handling of personal information to an agent outside of RIKEN, care must be taken to ensure that the agent is capable of appropriately managing the personal information and ensuring its security. 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 retained individual 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 commissioning work requires the handling of personal information by an agent outside RIKEN, the Personal Information Manager must conduct an on-site inspection at least once a year of the agent's manner of handling commissioned tasks and management of retained personal information including designated personal information, the degree of confidentiality and security measures taken depending on the degree of the confidentiality and the volume of information.
   When all or some of the tasks related to retained individual 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 retained personal information, it must be ensured that the provisions listed under paragraph 3 above are applied to the sub-contracting agent, as well as the provisions of the preceding paragraph. 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 retained individual numbers wishes to sub-contract related tasks to another party, it must be confirmed whether the party can manage retained designated personal information securely and has security measures for confidentiality before approving recommissioning of the tasks to the party.
7. When a dispatch agency staff person is required to handle retained personal information, confidentiality and security provisions must be included in the dispatch agency contract.
8. When providing retained 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 retained personal information to minimize damage by leakage of personal information.

Article 18 Worker responsibility

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.

Article 19 Limitations on use and provision

1. Employees must not, except when provided for by law, use or provide retained personal information for other than the intended purposes.
2. When RIKEN conducts research specified as activities in its annual plan jointly with other organizations (including those in the private sector), the provision of retained personal information to the other organizations shall be considered one of the activities' intended purposes. However, the President must approve the provision of information.
3. Regardless of the paragraph 1, employees may use or provide retained personal information (excluding unidentifiable processed information and deleted information; the same hereafter) for other than the intended purposes in any of the cases listed below. This does not apply, however, if the use or provision of personal information may curtail the rights and benefits of the individual concerned or of a third party.
    (1) Permission has been granted by the individual or the individual is being provided his or her own personal information.
    (2) When the personal information will be used within RIKEN for legally defined purposes and there is good reason for this use of personal information.
    (3) When the personal information will be provided to a government agency, an independent administrative institution, a regional public organization, or a regional independent administrative institution, and it is clear that the recipient of the information will be using it for legally defined purposes, and when there are good reasons for this use of personal information, including items (a) and (b) shown below.
        (a) When RIKEN provides retained personal information to a government agency in response to a request for provision of retained personal information for the agency's own research.
        (b) When RIKEN provides retained personal information to independent administrative institutions in order for them to use such information for their research conducted under their annual plans that are created in accordance with the Act on General Rules for Independent Administrative Agencies (1999, Act. No.103), the National University Corporation Act (2003, Act. No. 112), or other acts that define the scope of business of the relevant agencies.
    (4) In addition to the conditions stipulated in paragraph 3 above, when the information will be used in a compilation of statistics or for scholarly research, it is clear that providing information to a person other than the individual is to the individual's advantage, and whenever there are other extenuating circumstances for providing personal information.
4. The above provisions do not preclude limitations on the use and supply of retained personal information imposed by other laws and regulations.
5. When deemed necessary for the protection of individual rights and benefits, the internal use of personal information for purposes other than the original purpose for which the information was gathered must be limited to certain, designated employees.

Article 20 Requirements to receive retained personal information

1. The Personal Information Manager shall, when providing retained personal information to a party other than government agencies and independent administrative institutions, in accordance with the provisions stipulated in paragraphs 3, items 3 and 4 of the above article, as a general rule, exchange a written memorandum with the party that will be using the information that stipulates the purpose, legal rationale, and extent of the information that will be recorded, and includes a listing of the items to be recorded, and the format in which the information will be used.
2. The Personal Information Manager shall, when providing retained personal information to a

party other than government agencies and independent administrative institutions, , in accordance with the provisions stipulated in paragraphs 3, items 3 and 4 of the above article, request security measures and, when deemed necessary, shall conduct on-site investigations prior to providing the information and periodically thereafter, to ensure that security measures are in place. The Personal Information Manager shall maintain a record of these investigations and require improvements of security measures as necessary.

3. The Personal Information Manager shall, when providing retained personal information to a government agencies and independent administrative institutions, in accordance with the provisions stipulated in paragraphs 3, item 3 of the above article, implement as deemed necessary the measures outlined in paragraph 2 above.
4. The Personal Information Manager shall, when providing retained personal information to other organizations, in accordance with the provisions stipulated in paragraph 2 of the above article, request security measures in writing. The written document shall include clarification of the scope of retained personal information to be handled, such as encryption of retained personal information, prohibition of secondary use of retained personal information and provision to third parties (unless the consent of the concerned individual is obtained), and procedures for discarding retained information at the end of the collaborative research. The Personal Information Manager shall check the implementation status of the security measures through written reports.
5. If a record book of personal information files is required to be created and disclosed, pursuant to Article 25, paragraph 1, when providing retained personal information to other organizations, in accordance with the provisions stipulated in paragraph 2 of the above article, the record book shall include descriptions of the personal information that is used for collaborative research, the purpose of use for collaborative research, the categories of retained personal information provided for the collaborative research, the scope of users of the retained personal information in the collaborative research, and whether or not an opt-out is applied (application of the opt-out from the concerned individual will suspend the provision of personal information for the collaborative research).
6. The Personal Information Manager may not provide designated personal information other than in the limited cases specified by the Numbers Act.

Article 21 Record on the handling of retained personal information

1. The Personal Information Manager shall, depending on the nature of the retained 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 use of individual numbers

The Personal Information Manager must limit the use of individual numbers for tasks specified in the Numbers Act.

Article 21-3 Limits on requests for designated personal information

Designated personal information must not be requested except when carrying out procedures related to individual numbers and in the other limited cases stipulated by the Numbers Act..

Article 21-4 Limits on the compilation of designated personal information files

Designated personal information must not be compiled in files except when carrying out procedures related to individual 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

Designated personal information may not be collected or stored 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 damage 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 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.
   In the event that a case is made public, information on the case, its background, and the extent of damage must be promptly reported to the Ministry of Internal Affairs and Communications.

Article 23 Information security

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

Chapter 5 Notices regarding possession of personal information files

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 (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 any personal information requiring special care in handling
   (6) When personal information will be regularly supplied to a person or organization outside of RIKEN, the name of that person or organization
   (7) The names of the relevant laws and regulations that require special procedures to change or stop the use of personal information files
   (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 non-identifiable 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
   (3)-2 Personal information files equivalent to non-identifiable processed information files
   (3)-3 Personal information files containing deleted information
   (4) Personal information files that only contain recorded information that will be erased within one year
   (5) A personal information file containing data on fewer than 1,000 persons
   (6) 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.
   (7) 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
   (8) Any personal information files equivalent to those noted in the above items and for which Article 4 of the Order for Enforcement of the Act on the Protection of Personal Information Retained by Independent Administrative Institutions applies (2003, Ordinance 549)
3. Regardless of the provisions of paragraph 1 above, if recording any of the recorded items and the information cited in paragraph 1, items 5 and 6 may significantly hinder the appropriate carrying out of procedures related to the uses for which the personal information is required, a part or all of such information may be left unrecorded.
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 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 Government Directive No. 3 (2005) on disclosure and corrections of personal information files and retained personal information.

Chapter 6 Disclosure, corrections, and termination of use

Article 26 Disclosure, corrections, and termination of use

RIKEN shall disclose, correct, and terminate retained personal information as stipulated in the relevant government directive mentioned in the preceding article.

Article 26-2 Provision of non-identifiable processed information files

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

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 Miscellaneous provisions

Article 27-2

1. The provisions of Article 19, paragraph 3, items 2 through 4 do not apply when the provisions of Article 30, paragraph 2 of the Numbers Act apply.
2. When the provisions of Article 30, paragraph 2 of the Numbers Act apply, the provisions of these Regulations are to be read as follows.

Reg. Article	Relevant section	To be replaced with
Article 19, paragraph 1	"…,except when provided for by law,..."	"…,except when provided for by Article 9, paragraph 4 of the Numbers Act,..."
	"must not,…,use or provide retained personal information...	"must not,…,use…"
Article 19, paragraph 3	"…must not use or provide…"	"…must not use…"
Article 19, paragraph 3, item 1	"Permission has been granted by the individual or the individual is being provided his or her own personal information."	"When the information is necessary for the preservation of human life or to physically protect the person or the person's assets and when the person has given permission, or when it is difficult to acquire the person's permission."

Article 27-3

1. The provisions of Article 19, paragraph 3 to paragraph 5, and Article 20 do not apply when the provisions of Article 31, paragraph 3 of the Numbers Act apply.
2. When the provisions of Article 31, paragraph 3 apply, the provisions of these Regulations are to be read as follows.

Reg. Article	Relevant section	To be replaced with
Article 19, paragraph 1	"1. Employees must not, except when provided for by law, use…for other than the intended purposes."	"Employees must not use…for other than the intended purposes."

Chapter 9 Audits and inspections

Article 27-4 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 retained 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 retained 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 retained 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 retained 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.