Personal Information Protection Regulations
Kojin jyoho hogo kitei
March 10, 2005, Reg. 6
With revisions effective May 30, 2017

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"). Additional terms are defined as follows.
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. 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 56, paragraph 1 of the RIKEN Organization Regulations (2013, Reg. No. 2), 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 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 a staff person has violated, or may violate, the regulations for handling personal information.
   (2) A process for designating and clarifying the tasks and responsibilities of each section or department when multiple sections or departments handle designated personal information.
   (3) 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.
   (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 Review Committee.
2. Provisions for the Disclosure and Personal Information Review Committee are set forth in the RIKEN Regulations for the Establishment of a Disclosure and Personal Information Review Committee (2003, Reg. 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 staff 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 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 designated staff responsible for tasks related to protecting personal information.
4. Personal Information Managers must ensure that the employees and designated staff in their

section or organization have the opportunity to participate in training programs related to the management of personal information.

Chapter 4 Handling of personal information

Article 8 Employee responsibilities

(1) Employees must handle personal information in accordance with the instructions of Personal Information Managers, the General Affairs Division Director, and the General Manager for Personal Information, and in accordance with the provisions 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 a staff person 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 required, keep to a minimum the number of employees with access rights to retained personal information.
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

1. Employees may retain personal information only for purposes required by law and must specify those purposes to the extent possible.
2. Employees must not retain 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 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 under false pretenses or by other inappropriate means.
2. Employees must acquire 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 notice
    (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 personal information 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 relevant personal information laws and regulations.
5. An inspection must be made at least once a year of the agent's management of retained personal information and confidentiality and security measures.
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.
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.

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 who handle personal information in the course of their work
(2) All persons 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 purpose.
2. Regardless of the above paragraph, employees may use or provide retained personal information (excluding unidentifiable processed information and deleted information; the same hereafter) for other than the intended purpose 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, other 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 is good reason for this use of personal information.
    (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.

3. The above provisions do not preclude limitations on the use and supply of retained personal information imposed by other laws and regulations.
4. 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 government agency, other independent administrative institution, regional public organization, or a regional independent administrative institution, in accordance with the provisions stipulated in paragraphs 2 and 3 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 government agency, other independent administrative institution, regional public organization, or a regional independent administrative institution, in accordance with the provisions stipulated in paragraphs 2 and 3 of the above article, request security measures and, when deemed necessary, shall conduct 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 agency, other independent administrative institution, regional public organization, or a regional independent administrative institution, in accordance with the provisions stipulated in paragraphs 2 and 3 of the above article, implement as deemed necessary the measures outlined in paragraph 2 above.
4. The Personal Information Manager may not provide specific personal information other than in the limited cases specified by the Numbers Act.

Article 21 Personal information record book

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 specified 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 to those uses specified in the Numbers Act.

Article 21-3 Limits on requests for specified personal information

Specified personal information must not be requested except in the limited cases stipulated by the Numbers Act, such as when carrying out procedures related to individual numbers.

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

Specified personal information must not be compiled in files except in the limited cases stipulated by the Numbers Act, such as when carrying out procedures related to individual numbers.

Article 21-5 Limits on the collection and storage of specified personal information

Specified 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 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 there is a leak or the suspicion of a leak or other breach of security regarding personal information, the person who first discovers or suspects the security breach 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 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 used to digital processing of data
(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 clauses 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 items specified as follows will 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. This applies to the recorded items to be included in the personal information files or the recording limitations on the personal information cited in paragraph 1, clause (4) and the information cited in paragraph 1, clauses (5) and (6).

4.

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 cited above.
2. The conditions for the creation and public release of the record book of personal information files noted above are stipulated in a 2005 government directive.

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 directives.

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 Affairs 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 2, 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 2	"…must not use or provide…"	"…must not use…"
Article 19, paragraph 2, 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 2 to paragraph 4, 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 purpose."	"Employees must not use…for other than the intended purpose."

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 Manger for Personal Affairs, 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 audit results and to the extent that implementation is possible. The General Manger for Personal Affairs, 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.