Radiation Effects Research Foundation
Regulations for Protection of Personal Information

Section 1 – General provisions

(Objective)

Article 1 – Based on the provisions of Article 65-2, Articles of Incorporation of the Radiation Effects Research Foundation (hereafter referred to as "this foundation") and in accord with the idea that personal information should be handled carefully to respect each individual, the objective of these regulations is to define necessary matters for the proper handling of personal information at this foundation.

(Definitions)

Article 2 – The terms used in these regulations are defined as follows:

(1) "Employees" mean individuals stipulated in Article 2 of the Rules of Employment as well as all individuals engaged in activities at this foundation by direction and order of this foundation.

(2) "Personal information" means information relating to a living individual that can identify a specific individual by name, date of birth, or other description (meaning records in a document, drawing, or electromagnetic form) contained in such information (including any information that can be easily collated with other information and thereby enables the identification of that specific individual).

(3) "Sensitive personal information" means personal information as to an identifiable person's race, creed, social status, medical history, criminal record, history of being a crime victim, or other identifiers that require special care to prevent unlawful discrimination, prejudice, or other disadvantages to the identifiable person.

(4) "Personal information database" means a collective body of information including personal information, as set forth in the following (excluding those prescribed by Cabinet Order as having little possibility of harming individual rights and interests in light of how the information is used):

1) Those systematically organized so as to be searchable for particular personal information using a computer.

2) Beyond what is set forth in the preceding item, those prescribed by Cabinet Order as having been systematically organized so as to be easily searchable for particular personal information.

(5) "Business handling personal information" means an entity that uses a personal information database for business.

(6) "Personal data" means personal information compiled in a personal information database managed by this foundation.

(7) "Retained personal data" means personal data which this foundation has the authority to disclose; to correct, add, or delete content from; to cease to use; to erase; or to cease to provide to a third party, other than those set forth as follows, which would harm the public interest or other interests if their existence were made known:

1) Personal data for which there is a possibility that an identifiable person's or

third party's life, body, or property might be harmed if its existence were made known.

2) Personal data for which there is a possibility that an illegal or unjust act might be encouraged or induced if its existence were made known.

3) Personal data for which there is a possibility that national security might be undermined, a relationship of trust with another country or an international organization might be damaged, or negotiations with another country or an international organization might be disadvantaged if its existence were made known.

4) Personal data for which there is a possibility that the maintenance of public safety and order, such as the prevention, suppression, or investigation of a crime, would be hindered if its existence were made known.

(Employee responsibilities)

Article 3 – In handling personal information, employees pledge to comply with the Act on the Protection of Personal Information (Act No. 57 of 2003: hereafter referred to as the "Personal Information Protection Act") and relevant laws and regulations.

2. In conducting research and studies, employees pledge to comply with the Personal Information Protection Act, relevant laws and regulations, and the government-issued Ethical Guidelines for Life-Science and Medical Research Involving Human Subjects (Ministry of Education, Culture, Sports, Science and Technology/Ministry of Health, Labour and Welfare/Ministry of Economy, Trade and Industry) (hereafter referred to as the "national ethical guidelines"), as well as the following items, and intend to properly handle personal information:

(1) Having the Institutional Review Board (IRB) review research protocols concerned prior to conducting research and studies, including the security management of personal information, and not to initiate the research and studies concerned without approval from the IRB.

(2) Informing the individuals of the purpose of use of the personal information in advance when obtaining personal information from individuals.

(3) Not providing personal information to any third party without consent from the individuals from whom information was obtained.

(4) Choosing reliable organizations and concluding work contracts with the other parties to ensure proper handling of personal information when outsourcing activities to other institutions.

(5) Disclosing personal information in the custody of this foundation when requested by the individual from whom information was obtained.

3. Notwithstanding the provisions of the preceding items 2 and 3, as well as Articles 5, 7, 10, 11, 12, and 13, when handling personal information for the purpose of using it in academic research based on laws and regulations, restrictions according to the purpose of use (Article 18, Paragraph 3 of the Personal Information Protection Act), restrictions on the acquisition of sensitive personal information (Article 20, Paragraph 2 of the Personal Information Protection Act), restrictions on the provision of personal data to third parties (Article 27 of the Personal Information Protection Act), restrictions on the provision of personal data to third parties in foreign countries (Article 28 of the Personal Information Protection Act), and obligations to confirm and record when providing personal data to third parties (Articles 29 and 30 of the Personal Information Protection Act) are not applicable,

excluding cases in which there is a risk of unjust infringement of the rights and interests of individuals.

Section 2 – Basic items requiring attention from employees in compliance with the Personal Information Protection Act

(Specification of purpose of use)

Article 4 – In handling personal information, employees must specify to the extent possible the purpose of using such information.

2. Employees must not alter the purpose of use beyond a reasonable scope that can be appreciably linked to the original purpose of use.

(Restrictions on use for other purposes)

Article 5 – Employees must not handle personal information beyond the scope of the purpose of use, except as provided by laws and regulations.

(Notification of purpose of use)

Article 6 – In acquiring personal information, employees must notify the relevant individual of, or make public, the purpose of use, except as provided by laws and regulations.

(Proper acquisition)

Article 7 – Employees must not acquire personal information through falsification or other fraudulent means.

2. Employees must not acquire sensitive personal information without obtaining the identifiable person's consent in advance, except as provided by laws and regulations.

(Ensured accuracy of personal data)

Article 8 – Employees must strive to keep personal data accurate and current within the scope necessary for achieving the purpose of use and to delete the personal data without delay when it becomes unnecessary.

(Security management of personal data)

Article 9 – Employees must adopt necessary and proper measures for the prevention of leakage of, loss of, or damage to personal data.

(Restrictions on provision of personal data to third parties)

Article 10 – Employees must not provide personal data to third parties without obtaining the identifiable person's consent in advance, except as provided by laws and regulations.

2. Those who receive the personal data in question will not fall under the category of a third party concerning the application of the provision stipulated in the previous paragraph when any of the following circumstances are applicable:
   (1) When this foundation provides personal data in connection with the entrustment of all or part of the handling of personal data within the scope necessary for achieving the purpose of use.
   (2) When this foundation jointly uses personal data with specified individuals or

groups (provided that the parties from whom the data were derived are informed in advance of this matter, items of the data to be used jointly, the extent of the individuals or groups using the data jointly, the objective of the users, and the name and address of person/others responsible for supervising the personal data concerned, and if it is a corporation, the name of its representative, or that the parties are allowed ready access to the above-mentioned information).

(Restrictions on provision of personal data to third parties in foreign countries)

Article 11 – Except in cases set forth in Paragraph 1 of the preceding article, before employees provide personal data to a third party (excluding an entity that establishes a system that conforms to the standards prescribed by the Enforcement Rules for the Act on the Protection of Personal Information [Rules of the Personal Information Protection Commission No. 3 of 2016. Hereafter, referred to as "Rules of the Personal Information Protection Commission"] necessary for continuously taking measures concerning the handling of personal data equivalent to those required of a business handling personal information, pursuant to Chapter 4, Section 2 of the Personal Information Protection Act [referred to as "equivalent measures" in Paragraph 3]. The same applies hereafter in this and the following paragraphs) in a foreign country (excluding those prescribed by Rules of the Personal Information Protection Commission as a foreign country that has established a personal information protection system recognized to have equivalent standards to that in Japan regarding the protection of individual rights and interests. The same applies hereafter in this article), they must obtain the identifiable person's consent to the provision.

2. Before seeking the identifiable person's consent pursuant to the provisions of the preceding paragraph, employees must provide that person with information on the personal information protection system of the foreign country, the measures the third party takes for the protection of personal information, and other information that is to serve as a reference.

3 When having provided personal data to a third party (limited to a person establishing a system prescribed in Paragraph 1) in a foreign country, employees must take necessary measures to ensure continuous implementation of the equivalent measures by the third party, and provide information on the necessary measures to the identifiable person when requested.

(Preparation of records on provision of personal data to third parties)

Article 12 – When having provided personal data to a third party, employees must prepare a record pursuant to the Rules of the Personal Information Protection Commission on the date of the provision of the personal data, the name of the third party, and other matters prescribed by the Rules of the Personal Information Protection Commission.

(Confirmation on receiving personal data from a third party)

Article 13 – When receiving personal data from a third party, employees must confirm matters set forth in the following, pursuant to the Rules of the Personal Information Protection Commission:

(1) The name and address of the third party and, if the third party is a corporation, the name of its representative.

(2) Background of the acquisition of the personal data by the third party.

Section 3 – Basic items concerning disclosure of information in accordance with the Personal Information Protection Act

(Disclosure of retained personal data)

Article 14 – This foundation must disclose without delay an individual's retained personal data to the individual when the individual requests disclosure of such information, except as provided by laws and regulations.

(Correction of retained personal data)

Article 15 – When an individual, based on the justification that his/her retained personal data of this foundation are incorrect, requests correction, addition, or deletion (hereafter referred to as "corrections") of the personal data in question, this foundation must investigate without delay the personal data within the scope necessary for achieving the purpose of use, and make corrections to the personal data in question based on the investigation results.

(Suspension of use)

Article 16 – This foundation must suspend the use of the retained personal data, delete it, or suspend the provision of such data to third parties , pursuant to the provisions of laws and regulations.

(Handling of complaints)

Article 17 – This foundation must take appropriate and prompt action upon receipt of complaints regarding the handling of personal information.

2. The General Affairs Section of the Secretariat conducts the administrative work stipulated in the preceding paragraph.

Section 4 – Organization and system

(General privacy officer)

Article 18 – The Chair will appoint a general personal information privacy protection officer (hereafter referred to as "general privacy officer") for the comprehensive handling of personal information at this foundation.

2. The general privacy officer must conduct regular or ad-hoc inspections on the management status of the retained personal data.
3. Based on the results of the inspections mentioned in the previous paragraph, the general privacy officer must evaluate, review, and improve the security management measures.

(Privacy officers and personal information custodians)

Article 19 – The Chair will appoint personal information privacy protection officers (hereafter referred to as "privacy officers") and personal information custodians (hereafter referred to as "information custodians") for supervising the proper handling of personal information in this foundation's departments and Secretariat.

2. The responsibilities of privacy officers and information custodians will be prescribed separately.

(Committee for promoting personal information protection)

Article 20 – A committee for promoting personal information protection (hereafter referred to as the "committee") will be established to deliberate the necessary issues for the proper handling of personal information at this foundation.

2. The committee will consist of a general privacy officer, privacy officers, and others whom the general privacy officer deems necessary.
3. The general privacy officer will supervise the committee.
4. The General Affairs Section of the Secretariat will carry out administrative work related to the operation of the committee.

Section 5 – Other

(Disciplinary action)

Article 21 – This foundation may take disciplinary action based on the Rules of Employment or Regulations Concerning Disciplinary Action against employees who violate any of these regulations.

(Ensuring information system security)

Article 22 – This foundation will give due consideration to the necessity of security management of personal data and will strive to ensure information system security.

(Supervision of the party entrusted)

Article 23 – When entrusting the handling of personal data to another party, this foundation will conduct necessary and due supervision of the entrusted party in order to ensure the security management of the personal data concerned.

(Understanding of overseas conditions)

Article 24 – When handling personal data in a foreign country, this foundation must acquire and maintain a comprehensive understanding of the personal information protection systems and other measures of such country, and implement necessary and appropriate measures to ensure the security management of the personal data.

(Revision and abolition)

Article 25 – Revision and abolition of these regulations will be implemented only through decisions made by the Board of Directors.

(Miscellaneous provision)

Article 26 – For matters not stipulated in these regulations, the Personal Information Protection Act, other relevant laws and regulations, and this foundation's Detailed Regulations on Handling of Personal Information will apply.

Supplementary Provision

(Effective date)

These regulations will take effect from October 11, 2005.

Supplementary Provision

(Effective Date)

These regulations will take effect from the date of registration of the establishment as a public interest corporation, as stipulated in Paragraph 1 of Article 106 of the Act Serving as a Complement to Related Laws that Accompany Enactment of the Act on Authorization of Public Interest Incorporated Associations and Public Interest Incorporated Foundations and the Act on General Incorporated Associations and General Incorporated Foundations.

Supplementary Provision

(Effective Date)

These regulations will take effect on the date of approval by the Board of Directors (June 4, 2014).

Supplementary Provision

(Effective Date)

Based on the procedure in Article 8-3 of the Regulations on Management Authority of Directors, these regulations will take effect on the date of approval by the Executive Committee (August 2, 2016) and be applied retroactively to April 1, 2015. The revised provision in Article 3-2-1, however, will be applied from April 1, 2016.

Supplementary Provision

(Effective Date)

These regulations will take effect on the date of approval by the Board of Directors (June 4, 2019).

Supplementary Provision

(Effective Date)

These regulations will take effect on the date of approval by the Board of Directors (June 3, 2021) and be implemented from June 30, 2021.

Supplementary Provision

(Effective Date)

These regulations will take effect on the date of approval by the Board of Directors (March 13, 2025).