Provisional Translation

Regulations for the Protection of Personal Information at the National Research and Development Agency, National Institute for Environmental Studies (NIES)

April 1, 2005, Regulation No. 80 of 2005
Completely amended on December 1, 2015
Partially amended on December 21, 2016
Partially amended on September 20, 2017
Partially amended on January 4, 2019
Partially amended on April 20, 2022

Table of Contents

Chapter 1. General Provisions

(Purpose)

Article 1. These regulations set forth basis provisions for the handling of retained personal information and individual numbers (hereinafter "personal information") as prescribed in the Act on the Protection of Personal Information. (Act No. 57 of 2003. Hereinafter the "Protection Act") and the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 27 of 2013. Hereinafter the "Numbers Act.") at the National Research and Development Agency, National Institute for Environmental Studies (NIES) for the purpose of protecting the rights and interests of individuals while ensuring proper and smooth execution of NIES administration and activities.

(Definition of Terms)

Article 2. Terms used in these regulations are defined as follows pursuant to Articles 2, 16, and 60 of the Protection Act, Article 2 of the Numbers Act, and other sources:

(i) "Unit Director" refers to unit directors pursuant to Article 16 of the Regulations Related to the Authority of Officers of the National Research and Development Agency, National Institute for Environmental Studies (NIES).
(ii) "Units" refer to the administrative departments and/or research centers overseen by Unit Directors.
(iii) "Executives and Employees etc." refers to executives, employees, fixed term employees, or contract employees.
(iv) "Members" refer to executives, employees and all other individuals engaged in NIES work.
(v) "Personal information" refers to personal information pursuant to Article 2, paragraph 1 of the Protection Act.
(vi) "Personal information database or the equivalent" refers to a personal information database or the equivalent pursuant to Article 16, paragraph 1 of the Protection Act.
(vii) "Personal data" means personal information compiled in a personal information database or the equivalent.
(viii) "Personal information the administrative entity holds" refers to personal information retained by NIES pursuant to Article 60, paragraph 1 of the Protection Act.

(ix) "Personal information file" refers to a personal information file pursuant to Article 60, paragraph 2 of the Protection Act.
(x) "Sensitive personal information" refers to personal information requiring special care in handling pursuant to Article 2, paragraph 3 of the Protection Act.
(xi) "Identifiable person" refers to a specific individual identified by personal information.
(xii) "Pseudonymized personal information" is pseudonymized information pursuant to Article 2, paragraph 5 of the Protection Act.
(xiii) "Anonymized personal information" refers to anonymized information pursuant to Article 2, paragraph 6 of the Protection Act.
(xiv) "Information related to personal information" refers to personally referable information pursuant to Article 2, paragraph 7 of the Protection Act those compiled in a database or the equivalent of information related to personal information pursuant to Article 16, paragraph 7 of the Protection Act.
(xv) "Anonymized personal information the administrative entity holds" refers to anonymized personal information that can be processed by the administrative entity pursuant to Article 60, paragraph 3 of the Protection Act.
(xvi) "Individual number" refers to the individual number pursuant to Article 2, paragraph 5 of the Numbers Act.
(xvii) "Specific personal information" refers to the specific personal information pursuant to Article 2, paragraph 8 of the Numbers Act.
(xviii) "Specific personal information file" those compiled in a database or the equivalent of information related to personal information of the Numbers Act.
(xix) "Process using individual numbers" refers to a Process using individual numbers pursuant to Article 2, paragraph 10 of the Numbers Act.
(xx) "Process related to an individual number" refers to a process related to an individual number pursuant to Article 2, paragraph 11 of the Numbers Act.

Chapter 2. Management Structure

(General Personal Information Protection Manager)
Article 3. A General Personal Information Protection Manager shall be appointed at NIES by the Vice President (Planning and General Affairs).
2. The General Personal Information Protection Manager shall be responsible for administering all matters related to the management of personal information held by NIES.

(Personal Information Protection Manager)
Article 4. A personal information protection manager shall be appointed for each unit by the Unit Director.
2. Personal information protection managers shall be responsible for ensuring the appropriate management of personal information. held by their respective Units.
3. If personal information is handled using an information system, the personal information protection manager shall work with the information system administrator to carry out his or her responsibilities.
4. Personal information protection managers shall appoint executives and employees etc. (hereinafter "Personal Information Handler") to handle identification numbers and other specific personal information (hereinafter, "specific personal information") and define his or her duties.
5. Personal information protection managers shall define the scope of specific personal information to be handled by each personal information handler.
6. Personal information protection managers shall establish the following mechanisms:
(i) A mechanism for notifying the personal information protection manager if a personal information handler is found to be acting in violation of relevant laws or regulations or evidence thereof is found.
(ii) A mechanism for members to notify personal information protection managers if a case of specific personal information leaking, disappearing, or otherwise being damaged (hereinafter "information leak etc.") or evidence thereof is discovered.
(iii) When specific personal information is jointly handled by multiple units/divisions, a mechanism for clarifying the portion of specific personal information to be managed by each unit/division and the responsibilities of each unit/division.
(iv) Mechanisms and procedures for responding when an information leak etc. occurs or if evidence thereof is found.

(Person in charge of Personal Information Protection)
Article 5. Person in charge of Personal Information Protection shall appoint a person (or persons) responsible for protecting personal information in their respective units.
2. A person (or persons) in charge of protecting personal information shall assist the personal information protection manager and carry out duties related to the management of personal information etc. held by their unit.

(Personal Information Protection Auditor)
Article 6. The General Manager of the Audit Office shall be appointed as the Personal Information Protection Auditor.
2. The Personal Information Protection Auditor shall be responsible for investigating the issues related to the management of personal information etc. held by NIES.

(Committee to Ensure Appropriate Management of Personal Information)
Article 7. When it is deemed necessary to decide, report, or coordinate important matters related to the management of personal information or when it is deemed necessary to respond etc. to a serious incident related to personal information, the General Personal Information Protection Manager shall establish a committee consisting of personal information protection managers and other relevant staff members and shall convene the committee on a regular or ad hoc basis.

Chapter 3. Education and Training

(Implementation of Education and Training)
Article 8. The General Personal Information Protection Manager shall provide instruction and implement other necessary education and training for all members who handle personal information to deepen understanding related to the handling of personal information and to increase awareness related to the protection of personal information and specific personal information.
2. The General Personal Information Protection Manager shall implement necessary education and training for members who manage information systems that handle personal information regarding the management, operation, and security measures required for appropriate management of information systems.
3. The General Personal Information Protection Manager shall implement education and training for personal information protection managers and persons in charge of personal information protection regarding the appropriate management of personal information held by their respective units.
4. Personal information protection managers shall take necessary steps to ensure appropriate management of personal information such as providing opportunities for members in their respective units to participate in education and training implemented by the General Personal Information Protection Manager.
5. The General Personal Information Protection Manager and personal information protection managers shall deal strictly with individuals who are found to have violated laws or regulations.

Chapter 4. Responsibility of Members

(Handling of Personal information the administrative entity holds)
Article 9. Members must handle personal information in a manner consistent with the spirit of the Protection Act and the Numbers Act and must comply with provisions of relevant laws and regulations and follow the instructions of the General Personal Information Protection Manager, personal information protection managers, and others responsible for personal information protection.
2. Members must not disclose to others personal information or specific personal information acquired through their work without just cause or use such information for invalid purposes. The same prohibitions apply after members has left NIES.
3. Members who discovers that an information leak etc. of specific personal information has occurred (or evidence thereof) or discovers that a personal information handler is acting in violation of relevant laws or regulations (or evidence thereof), he or she must promptly notify the personal information protection manager.

Chapter 5. Handling of Personal information the administrative entity holds

(Specifying the Purpose of use)

Article 10. In handling personal information, personal information must specify as much as possible the purpose for which it uses that information (hereinafter referred to as the "purpose of use").

2. When altering the purpose of use, personal information must not alter it beyond the extent that can be appreciably linked to what it was before the alteration.

(Restrictions Due to Purpose of use)

Article 11. Personal information that exceeds the necessary scope to achieve the purpose of use specified pursuant to the immediately preceding Article must not be handled without obtaining the identifiable person's consent in advance.

2. The provisions of the preceding two paragraphs do not apply in the following cases:
   (i) Cases based on laws and regulations.
   (ii) Cases in which there is a need to protect the life, wellbeing, or property of an individual, and it is difficult to obtain the consent of the identifiable person.
   (iii) Cases in which there is a special need to improve public wellbeing or promote healthy child development, and it is difficult to obtain the consent of the identifiable person.
   (iv) Cases in which there is a need to cooperate with a national government organ, local government, or person entrusted thereby with performing the functions prescribed by laws and regulations, and obtaining the consent of the identifiable person is likely to interfere with the performance of those functions.
   (v) Cases in which the business handling personal information is an academic research institution or the equivalent, and needs to handle the personal information for the purpose of using it in academic research (hereinafter referred to as "academic research purposes" in this Chapter) (including cases in which a part of the purpose of handling the personal information is for academic research purposes, and excluding cases in which there is a risk of unjustly infringing on individual rights and interests).
   (vi) Cases in which personal data is provided to an academic research institution or the equivalent, and they need to handle the personal data for academic research purposes (including cases in which a part of the purpose of handling the personal data is for academic research purposes, and excluding cases in which there is a risk of unjustly infringing on individual rights and interests).

(Prohibition of Inappropriate Use)

Article 12. Personal information shall not be used in a manner that encourages or induces illegal or wrongful acts.

(Proper Acquisition)

Article 13. Personal information shall not be acquired through deception or other wrongful means.

2. Except in those cases set forth in the following, sensitive personal information shall not be acquired without obtaining the identifiable person's consent in advance.
   (i) Cases based on laws and regulations.
   (ii) Cases in which there is need to protect the life, wellbeing, or property of an individual, and it is difficult to obtain the consent of the identifiable person.
   (iii) Cases in which there is a special need to improve public wellbeing or promote healthy child development, and it is difficult to obtain the consent of the identifiable person.
   (iv) Cases in which there is a need to cooperate with a national government organ, local government, or person entrusted thereby with performing the functions prescribed by laws and regulations, and the consent of the identifiable person is likely to interfere with the performance of those functions.
   (v) Cases in which there is a need to handle the sensitive personal information for academic research purposes (including cases in which a part of the purpose of handling the sensitive personal information is for academic research purposes, and excluding cases in which there is a risk for unjustly infringing on individual rights and interests
   (vi) Cases of acquiring the sensitive personal information from an academic research institution or the equivalent and it is necessary to acquire that information for academic research purpose (including cases in which a part of the purpose of acquiring the sensitive personal information is for academic research purposes, excluding cases in which there is a risk of unjustly infringing on individual rights and interests) (limited to cases in which academic research is conducted jointly with the academic research institution or the equivalent).
   (vii) Cases in which the sensitive personal information is open to public by a person identifiable by that information, a national government organ, a local government, an academic research institution or the

equivalent, a person set forth in each item of Article 57, paragraph (1), or other person prescribed by Order of the Personal Information Protection Commission.

(viii) Other cases prescribed by Cabinet Order as equivalent to the cases set forth in each preceding item.

(Notification of a Purpose of Use when Acquiring Personal Information)

Article 14. When acquiring personal information, the purpose of use shall be announced in advance or communicated to the identifiable person or disclose this to the public promptly after acquisition.

2. Notwithstanding the provision of the preceding paragraph, the purpose of the identifiable person must be explicitly specified, before acquiring their personal information which appears in a written agreement or other document (this includes an electronic or magnetic record; hereinafter the same applies in this paragraph) as a result of concluding an agreement with that person; or acquiring their personal information which appears in a document, directly from the person in question; provided, however that this does not apply if there is an urgent necessity to dispense with this requirement in order to protect the life, wellbeing, or property of individual.
3. If the purpose of use is altered, it must notify identifiable persons of the altered purpose of use or disclose this to the public.
4. The provisions of the preceding three paragraphs do not apply in the following cases:
   (i) Cases in which there is a possibility that notifying the identifiable person of or publicly disclosing the purpose of use would harm the life, welfare, property, or other rights and interests of the identifiable person or a third party.
   (ii) Cases in which there is a possibility that notifying the identifiable person of or disclosing the purpose of use would harm the rights or legitimate interests of NIES.
   (iii) Cases in which there is a need to cooperate with the execution of a process prescribed by laws and regulations set forth by a national government organ or local government, and there is a possibility that notifying the identifiable person of or disclosing the purpose of use would hinder the execution of the said process.
   (iv) Cases in which the purpose of use is recognized as being clear from the circumstances of acquisition.

(Maintaining Accuracy of Data)

Article 15. Personal information must endeavor to keep the content of personal data accurate and up to date, within the scope necessary for achieving the purpose of use, and delete the personal data without delay if they no longer require it.

(Restricting Access)

Article 16. Personal information protection managers shall, depending on the confidentiality and content of the personal information, limit access to members with authority to access the personal information in question and the scope of that authority to the extent that is needed for the members to conduct their work.

2. Members who do not have authority to access personal information must not access such information.
3. Even if members has authority to access personal information, he or she must not access personal information for purposes other than those required for work.

(Restrictions on Copying etc.)

Article 17. Even when members handle personal information as part of their professional duties, depending on the confidentiality and content of the personal information in question, personal information protection managers shall restrict cases in which the following actions are permitted. Members shall follow the instructions of personal information protection managers.

(i) Making copies of personal information
(ii) Sending of personal information
(iii) Sending or taking outside of NIES media on which personal information is recorded (including information stored internally on personal computers or servers. The same applies hereinafter).
(iv) Other acts that might impede proper management personal information.

(Management of Media etc.)

Article 18. Members shall comply with the instructions of personal information protection managers and store media containing Personal information the administrative entity holds in the specified location, and when deemed necessary, protect said media in a fire-proof safe or by means of locked storage etc. If media containing Personal information the administrative entity holds is sent or taken outside NIES, in principle, necessary access control measures that function to identify users and access rights (hereinafter “verification function”) shall be put in place by using passwords etc. (= passwords, IC cards, biometric data, etc. The same applies

hereinafter).

(Prevention of Mistaken Transmission etc.)

Article 19. Members shall implement necessary measures such as confirmation by multiple employees and the use of checklists etc. depending on the confidentiality of personal information handled in individual process and operations to prevent the mistaken transmission, mis-delivery, accidental conveyance, or mistaken disclosure on websites etc. of electronic or magnetic records or media containing personal information the administrative entity holds (including additional information such as property information).

(Disposal etc.)

Article 20. When personal information the administrative entity holds or media containing personal information the administrative entity holds (including information stored on computers and servers) is no longer needed, members shall comply with the instructions of personal information protection managers and delete the relevant information or dispose of the relevant media in a manner that prevents restoration or identification of the relevant personal information the administrative entity holds. In particular, when the deletion of personal information the administrative entity holds or disposal of media containing personal information the administrative entity holds is outsourced to a third party (including multi-tiered contracting arrangements), deletion or disposal by the contracted party shall be confirmed by having an employee present at the deletion or disposal or through the receipt of documentation containing photographic verification etc. of deletion or disposal.

(Record of the Status of Handling of Personal Information)

Article 21. Depending on the confidentiality or content of personal information, personal information protection managers shall establish mechanisms for confirming the status of handling of information and keep a record of the status of handling (use and storage) of the personal information in question.

(Restriction on Provision of Information to a Third Party)

Article 22. When providing personal data to a third party, except in those cases set forth in the following cases, it is necessary to obtain the identifiable person’s consent in advance.

(i) Cases based on laws and regulations.
(ii) Cases in which there is a need to protect the life, wellbeing or property of an individual it is difficult to obtain the identifiable person’s consent.
(iii) Cases in which there is a special need to improve public wellbeing or promote healthy child development, and when it is difficult to obtain the identifiable person's consent.
(iv) Cases in which there is a need to cooperate with a national government organ, local government, or person entrusted thereby with performing the functions prescribed by laws and regulations, and the consent of the identifiable person is likely to interfere with the performance of those functions.
(v) Cases in which providing the personal data for the purpose of publication of academic research results or teaching is unavoidable (excluding cases in which there is a risk of unjustly infringing on individual rights and interests).
(vi) Cases in which providing the personal data for the academic research purpose (including cases in which a part of the purpose of handling the personal data is for academic research purposes, and excluding cases in which there is a risk of unjustly infringing on individual rights and interests) (limited to cases in which academic research is conducted the jointly third party).
(vii) Cases in which the third party is an academic research institution or the equivalent, and the third party needs to handle the personal data for academic research purposes (including cases in which a part of the purpose of handling the personal data is for academic research purposes, and excluding cases in which there is a risk of unjustly infringing on individual rights and interests).

2. Notwithstanding the provisions of the preceding paragraph, personal data can be provided a third party which can be used to identify the identifiable person, at the request of that person; NIES notifies that person of the following information in advance or makes that information readily accessible to that person in advance, as provided for by Order of the Personal Information Protection Commission; and NIES files a notification of this to the Commission, NIES may provide that personal data to a third party; provided, however, that this does not apply to cases in which personal data which is to be provided to a third party is sensitive personal information, has been acquired in violation of the provisions of Article 21, paragraph (1), or has been provided by another handing personal information pursuant to the provisions of the main clause of this paragraph (including personal data all or part of which has been reproduced or processed):

(i) Name and address of the research institute, name of the President.
(ii) The fact that providing the data to the third party constitutes the purpose of use.
(iii) The details of the personal data it will provide to the third party.
(iv) The means or manner in which it will acquire the data it provides to the third party.

(v) The means or manner in which it will provide the data to the third party.
(vi) The fact that it will cease to provide personal data that can be used to identify the identifiable person to a third party at the request of the identifiable person.
(vii) The means of receiving the identifiable person's request.
(viii) Other matters following as those necessary to protect individual rights and interests:
(a) Method for updating personal data provided to the third party
(b) The date that personal data that is the subject of relevant notification will start being provided to the third party

3. If there has been an alteration to the details set forth in item (i) of the preceding paragraph, or providing personal data pursuant have been ceased to personal data pursuant to the provisions of the preceding paragraph, NIES must notify the identifiable person of this or make this readily accessible to the person, and notify the Personal Information Protection Commission of this, pursuant to Order of the Personal Information Protection Commission, without delay; and if NIES seek to alter the details set forth in items (iii) through (v), item (vii), or item (viii) of that paragraph, NIES must do so beforehand.
4. In the following cases, a person receiving personal data is not to fall under a third party regarding applying the provisions of each preceding paragraph:
(i) Cases in which the relevant personal data is provided as the result of outsourcing all or part of the handling of personal data within the scope of achieving the purpose of use.
(ii) The personal data is provided when a person succeeds to the business due to a merger or other such circumstances.
(iii) The personal data is provided to specific persons who have joint use of that data, and NIES notifies the person identifiable by that data of this in advance as well as the details of that data, the extent of the joint users, the users' purpose of use, and the name and address of the person responsible for managing the personal data, and, if the user is corporation, the name of its representative; or NIES makes the foregoing information readily accessible to the person identifiable by that data in advance.
5. If there has been an alteration to the name and address of the person responsible for managing the personal data or, in cases of a corporation, to the name of the representative, as provided for in item (iii) of the preceding paragraph, the person identifiable by that data of this must be notified, or make this readily accessible to the person identifiable by that data, without delay; and if NIES intends to alter a user's purpose of use or the person responsible for the management as provided for in that item, NIES must do so beforehand.

(Restrictions on the Provision of Personal Data to Third Parties in Foreign Countries)
Article 23. When providing personal data to a third party (except for a party establishing a system that falls under any of the items set forth below) in a foreign country (meaning a country or region located outside the territory of Japan, excluding foreign countries establishing a personal information protection system recognized pursuant to the Order of the Personal Information Protection Commission as having equivalent standards to that of Japan in regard to the protection of individual rights and interests), except in those cases falling under Item 1 of the immediately preceding paragraph, consent from the identifiable person to the effect that he or she approves the provision to a third party in a foreign country must be obtained in advance. In this case, the provisions of the immediately preceding Article do not apply.
(i) The handling of the relevant personal data between NIES and the party receiving the provision of the relevant personal data shall implement appropriate and reasonable measures regarding the handling of the relevant personal data in line with the purpose of the provisions in Chapter 5.
(ii) The party receiving the provision of the relevant personal data must have obtained certification based on an international framework concerning the handling of personal information.
2. When obtaining consent from the identifiable person pursuant to the immediately preceding paragraph, in advance, information regarding the personal information protection system of the foreign country, the personal information protection measures of the relevant third party, and other information that would serve as reference information to the identifiable person must be provided to the identifiable person through the provision of electronic or magnetic records, delivery of written documents, or other appropriate means.
3. When personal data has been provided to a third party in a foreign country (limited to parties establishing systems pursuant paragraph 1), measures must be put into place to ensure the continuous implementation of corresponding measures by the third party and information regarding the relevant necessary measures must be provided to the identifiable person upon request of the identifiable person.
(i) The implementation status of the third party’s corresponding measures and any national systems of the foreign country that might influence the implementation of the corresponding measures must be periodically verified using appropriate and reasonable means.
(ii) When implementation of the corresponding measures by the relevant party is hindered, appropriate and necessary measures shall be implemented. When the continuous implementation of the corresponding measures is difficult, provision of personal data to the third party shall be stopped.

(Preparing of Records on Provision of Personal Data to Third Parties)
Article 24. When personal data is provided to a third party (excluding national government organs, local governments, an incorporated administrative agency or other prescribed corporation, and a local

incorporated administrative agency) pursuant to the immediately preceding Article, a record shall be created for each item listed for the relevant category listed in the category column of Table 1 based on Article 20 of the Order of the Personal Information Protection Committee. This, however, shall not apply when the provision of personal data falls under any of the items in paragraph 1 or 4 of Article 22 (in the case of provision of personal data pursuant to paragraph 1 of the immediately preceding Article, any of the items in paragraph 1 of Article 22).

<Table 1: Matters to be recorded upon provision>

Category	Provision date	Name etc. of the third party	Name etc. of the identifiable person	Personal information items etc.	Consent from the identifiable person
Provision of information to a third party pursuant to Article 22, paragraph 2	○	○	○	○	—
Provision of information to a third party based on consent from the identifiable person	—	○	○	○	○

2. The record created pursuant to the immediately preceding paragraph must be kept for a period of time from the date when it prepared the record listed in the following items:
   (i) In cases where personal data relating to the identifiable person is provided to a third party in connection with supplying the identifiable person with goods or services pursuant to Article 22, paragraph 1 or paragraph 1 of the immediately preceding Article, a period one year from the last day that personal data relating to the relevant record was last provided.
   (ii) In cases where personal data is provided to the third party continuously or repeatedly (excluding provision pursuant to Article 27, paragraph 2 of the Protection Act; hereinafter the same shall apply in this paragraph) or in cases where it is expected with high degree of certainty that personal data will be provided to the third party continuously or repeatedly, a period three years from the last day that personal data relating to the relevant record was last provided.
   (iii) In cases other than those listed in preceding two items, a period of three years.

(Confirmation on Receiving Personal Data from a Third Party)

Article 25. When a personal information protection manager receives personal data provided by a third party, he or she shall confirm and create a record for each item listed for the relevant category in the category column of Table 2 based on Article 24 of the Order of the Personal Information Protection Committee. This, however, shall not apply if any item in Article 22, paragraph 1 or any item in paragraph 4 of the Article applies to the provision of relevant personal data.

<Table 2: Matters to be recorded upon receipt>

Category	Date of receipt	Third party name etc.	Acquisition process	The identifiable person's name etc.	Personal information items	Public disclosure by the Personal Information Protection Committee	Consent from the identifiable person etc.
Receipt of a third party provision pursuant to Article 22, paragraph 2	○	○	○	○	○	○	—
Receipt of a third-party provision based on consent from the identifiable person	—	○	○	○	○	—	○

2. The record created pursuant to the immediately preceding paragraph shall be stored from the day that the relevant record was created for a period of time listed in the following items:
   (i) In cases where the provision of personal data relating to the identifiable person is received in connection

with supplying the identifiable person with goods or services, a period of one year from the last day that personal data relating to the relevant record was last received.

(ii) In cases where personal data provided by the third party is received continuously or repeatedly (excluding provision pursuant to Article 22, paragraph 2) or in cases where it is expected with a high degree of certainty that personal data will be provided by the third party will be received continuously or repeatedly, a period three years from the last day that the personal data relating to the relevant record was last received.

(iii) In cases other than those listed in preceding two items, a period of three years.

(Restrictions on the Provision of Information Related to Personal Information to Third Parties)

Article 26. When information related to personal information constituting an information related to a personal information database is provided to a third party and there is an expectation that relevant third party will add the information related to personal information to personal data and otherwise utilize it as personal data, except for those cases that fall under any item in Article 22, paragraph 1, the matters set forth in the following items shall be confirmed in advance by a reasonable method such as receiving a written declaration from the third party receiving the information related to personal information.

(i) Consent has been obtained from the identifiable person to the effect that he or she agrees to the acquisition of information related to personal data that can identify the identifiable person and that will be provided by NIES to the third party.

(ii) In the case of provision to a third party in a foreign country, when attempting to obtain consent from the identifiable person pursuant to the immediately preceding item, the identifiable person has been informed by a reasonable method such as receiving a written document that the information stipulated in the same item is being provided and has in advance been provided information regarding the personal information protection system of the foreign country, the personal information protection measures of the third party, and other information that would serve as reference information to the identifiable person.

2. When information related to personal information has been provided to a third party in a foreign country (limited to parties establishing systems pursuant to Article 23, paragraph 1), pursuant to the items in Article 23, paragraph 3, measures must be put into place to ensure the continuous implementation of corresponding measures by the third party.

3. When information related to personal information has been provided to a third party pursuant to paragraph 1, a record shall be created for each item listed for the relevant category in the category column of Table 2 in paragraph 1 of the immediately preceding Article.

4. The record created pursuant to the immediately preceding paragraph shall be stored from the day that the record was created for a period of time set forth in the applicable item of paragraph 2 of the immediately preceding Article.

(Handling of Pseudonymized Information)

Article 27. Pseudonymized information shall be handled pursuant to Chapter 4, Section 3 of the Protection Act.

(Handling of Anonymized Information)

Article 28. Anonymized information (except for anonymized information of administrative organs) shall be handled pursuant to Article 121 of the Protection Act.

(Restrictions on Use of Individual Numbers)

Article 29. Personal information protection managers shall ensure that use of individual numbers is limited to processes specified in the Numbers Act.

(Restrictions on Requests for Specific Personal Information)

Article 30. Requests for provision of individual numbers are prohibited except in cases where individual numbers are needed for processes using individual numbers or processes related to individual numbers (hereinafter “Processes Using Individual Numbers etc.”) or other cases specified in the Numbers Act.

(Restrictions on Collection and Retention of Specific Personal Information)

Article 31. The collection and retention of specific personal information including another person’s individual number is prohibited except in the cases specified in Article 19 of the Numbers Act.

(Scope of Handling)

Article 32. Personal information protection managers shall clearly define the scope of administrative processes that handle specific personal information and shall take steps to ensure the physical safety of the information in question.

Chapter 6. Handling Personal Information Files

(Advance Notification Regarding the Retention of Personal Information Files)

Article 33. If a Unit is planning to retain personal information files, the personal information protection manager of the Unit in question shall give prior notice to the General Personal Information Protection Manager of the following items. The same applies when changing an item about which the General Personal Information Protection Manager has already been notified.

(i) Title/name of the personal information file
(ii) The name of the Unit and the name of the section or office that will primarily be using the personal information file
(iii) Purpose of use for the personal information file
(iv) Matters (hereinafter "recorded items") and scope of individuals (hereinafter "scope of record") to be recorded as relevant persons (limited to those who can be identified through a search without another individual's name, date of birth, or other identifiers or their equivalent) in the personal information file
(v) Means of collecting the personal information recorded in the personal information file (hereinafter "recorded information")
(vi) If sensitive personal information is included in the recorded information, an indication to that effect.
(vii) If recorded information will be provided routinely to a party outside of NIES, the name of the receiving party.
(viii) The Name and address of the organizational that accepts requests for disclosure, correction, or suspension of use.
(ix) If the personal information the administrative entity holds is subject to correction, suspension of use, deletion, or prohibition of provision, an indication to that effect.
(x) A personal information file subject to government ordinances pertaining to Article 74, paragraph 1, item 11 of the Protection Act.

2. The provisions of the immediately preceding paragraph shall not apply to the personal information files set forth in the following cases:

(i) A personal information file that contains information relating to national security, diplomatic secrets, and other important national interests.
(ii) A personal information file prepared or obtained for criminal investigation, investigation of tax crimes based on the provisions of laws related to tax, or instituting or keeping a legal proceeding.
(iii) A personal information file relating to executives and employees or former executives and employees that exclusively contains information concerning their affairs, wages or welfare benefits, or any equivalent matters (including a personal information file concerning the employment exam of executives and employees).
(iv) A personal information file to be exclusively used for the purpose of experimental computer processing.
(v) A personal information file that contains in whole or in part recorded information relating to a notification pursuant to the immediately preceding paragraph whose purpose of use, record items, and scope of record fall within the scope of the matters relating to the relevant notification.
(vi) A personal information file that exclusively contains recorded information that is scheduled to be deleted within 1 year.
(vii) A personal information file that contains recorded information that is utilized for the purpose of sending materials or any goods or money needed for business communications that only contains the names, addresses, and other necessary details concerning the recipients.
(viii) A personal information file that is created or obtained by executives and employees based on that person's idea for an academic research purpose and whose recorded information will be exclusively utilized for that academic research purpose.
(ix) A personal information file containing information for less than 1000 individuals.
(x) A personal Information file by Cabinet Order relating to Article 74, paragraph 2, item 10 of the Protection Act.

(Advance Notification Regarding Use or Provision of Personal Information Files for Purposes Other than the Purpose of Use)

Article 34. If a personal information protection manager plans to use or provide personal information files held by their unit for purposes other than the purpose of use, he or she shall provide prior notice to the General Personal Information Protection Manager of the following items in advance.

(i) Title/name of the personal information file
(ii) Name of the Unit and the name of the section or office responsible for the process in which the personal information file will be used.
(iii) Purpose of use for the personal information file
(iv) Details regarding use or provision for purposes other than the purpose of use
(v) If the files will be provided to a third party, the name of the party

(vi) Reason for use or provision

(Personal information file register)
Article 35. NIES shall prepare and publish a personal information file register according to detailed regulations specified elsewhere.

(Restrictions on the Preparation of Specific Personal Information Files)
Article 36. The preparation of specific personal information files is prohibited except in cases where such a file is needed for handling processes using individual numbers etc. or other cases specified in the Numbers Act.
2. If a specific personal information file is to be prepared, it shall be prepared according to provisions provided elsewhere.

Chapter 7. Ensuring the Security of Information Systems etc.

(Access Control)
Article 37. Depending on the confidentiality and content of personal information (limited to information handled by information systems. The same applies to rest of this Chapter and the next Chapter with the exception of Article 51), personal information protection managers (limited to sections or offices that set up or manage information systems. The same applies to the rest of this Chapter and the next Chapter) shall take necessary steps to control access by using passwords etc. (passwords, IC cards, biometric information, etc., this applies below) to differentiate levels of authorization (hereinafter authentication function).
2. When taking steps pursuant to the previous paragraph, personal information protection managers shall establish rules for managing passwords etc. (including periodic or as-needed reexamination thereof) and take necessary steps to prevent passwords etc. from being stolen.

(Record of Access)
Article 38. Depending on the confidentiality and content of personal information, personal information protection managers shall record accesses to the personal information in question and retain this record (hereinafter "access record[s]") for a specified period and takes steps to analyze access records either periodically or on an as-needed basis.
2. Personal information protection managers shall take necessary steps to prevent falsification, theft, or unauthorized erasure of access records.

(Monitoring of Access)
Article 39. Depending on the confidentiality, content, and quantity of personal information, to monitor improper access of the personal information in question, personal information protection managers shall specify settings so that a warning is displayed when data containing or suspected of containing personal information over a certain size threshold is downloaded from the information system and shall take steps to periodically check these settings.

(Setting of System Administrator Privileges)
Article 40. Depending on the confidentiality and content of personal information, personal information protection managers must take necessary steps to minimize system administrator privileges to minimize the potential damage caused when administrator privileges are stolen and to prevent improper manipulation of data in the information system.

(Prevention of Unauthorized External Access)
Article 41. Personal information protection managers shall take necessary steps such as setting up firewalls to control routing etc. to prevent unauthorized external access to information systems that handle personal information.
2. Regarding information systems that are used in processes using individual numbers, personal information protection managers shall ensure that operating protocols and systems are designed for high security, such as by isolating systems from the internet.

(Prevention of Information Leaks etc. by Unauthorized Programs)
Article 42. To prevent leaks etc. of personal information, personal information protection managers shall take steps necessary (including continuously updating installed software) to address/eliminate known software vulnerabilities and to prevent infection by unauthorized programs that are detected.

(Processing of Personal Information in Information Systems)
Article 43. If members must temporarily copy personal information for processing, the scope of information copied shall be kept to a minimum, and information that is no longer needed after processing shall be promptly erased. Depending on the confidentiality and content of the personal information in question, personal information protection managers shall make it a priority to check, as needed, that the information has been erased etc.

(Encryption)
Article 44. Depending on the confidentiality and content of the personal information, personal information protection managers shall take necessary steps to encrypt the personal information in question.
2. Pursuant to provisions of the previous paragraph, depending on the confidentiality and content of the personal information, members shall appropriately encrypt (including selection of appropriate passwords, measures to prevent their disclosure, etc.) personal information that they will process.

(Restrictions on the Connection of Devices and Media with Recording Function)
Article 45. Depending on the confidentiality and content of the personal information, to prevent leaks etc. of the personal information in question, personal information protection managers shall take steps necessary to restrict (including upgrade of such devices) the connection of devices or media with recording function such as smartphones, USB memory drives, and other devices and media with recording functions to information system terminals.

(Restriction of Terminals)
Article 46. Depending on the confidentiality and content of the personal information, personal information protection managers shall take steps necessary to restrict the terminals on which the personal information in question can be processed.

(Prevention of Theft etc. of Terminals)
Article 47. To prevent the theft or loss of terminals, personal information protection managers shall take steps necessary such as locking down terminals and locking offices.
2. Except in cases where there is deemed necessary by a personal information protection manager, members must not take a terminal outside NIES or bring a terminal in from outside NIES.

(Prevention of Viewing by Third Parties)
Article 48. Regarding the use of terminals, members shall take necessary steps to prevent third parties from viewing personal information such as by making sure to log off from the information system depending on circumstances of use.

(Checking of Entered Data)
Article 49. Depending on the importance of the personal information to be handled by the information system, members shall check the entered data against the source data, compare the personal information in question before and after processing, and confirm the data against existing personal information.

(Backup of Personal Information)
Article 50. Depending on the importance of the personal information, personal information protection managers shall create backups of the information and take other necessary steps regarding backups.

(Storage of Information System Design Specifications etc.)
Article 51. Personal information protection managers shall take necessary steps to store, copy, and dispose of, etc. design specifications, configuration diagrams, and other documents related to information systems related to personal information in a manner so that they cannot be viewed by anyone outside NIES.

Chapter 8. Secure Management of Rooms etc. Housing Information Systems

(Management of Entry and Departure)
Article 52. Personal information protection managers shall specify individuals who are authorized to enter rooms or other areas where the main server and other equipment for handling personal information are installed (hereinafter “Information System Rooms etc.”) and shall take steps such as checking the reason for entry;

recording entry and departure; establishing a method to differentiate outsiders from NIES employees; having member accompany outsiders or otherwise monitor outsiders when they enter such spaces; and restricting the carrying in, use, and carrying out of outside electromagnetic media, etc. If a storage facility for storing media containing personal information exists, similar measures should be implemented if deemed necessary.

2. If deemed necessary, personal information protection managers shall take steps such as simplifying entry and departure management by designating different doors for entry and departure from information system rooms etc. and limiting signage indicating the location of such rooms.
3. With regard to management of entry and departure from information system rooms etc. and media storage rooms, if deemed necessary, personal information protection managers shall take necessary steps such as setting up an authentication function related to entry, establishing rules regarding the management of passwords etc. (including periodic or as-needed reexamination), and preventing passwords etc. from being stolen.

(Management of Information System Rooms etc.)

Article 53. Protection managers shall take steps to prevent unauthorized entry into Information System Rooms etc. by outsiders by installing locking devices, alarms, and other warning equipment, and monitoring facilities.

2. To prepare for natural disasters, personal information protection managers shall take steps to deploy earthquake proofing as well as fire prevention, smoke protection, and water protection measures for Information System Rooms etc. and to secure backup power for servers etc., and establish measures to prevent damage to wiring.

Chapter 9. Provision and Outsourcing of Administrative Tasks Related to Personal Information

(Provision of personal information)

Article 54. When providing personal information to parties other than administrative organs or incorporated administrative agencies etc. pursuant to Article 69, paragraph 2, items 3 and 4 of the Protection Act, personal information protection managers shall exchange written documents (including electronic or magnetic records) that, in principle, include the purpose of use by the receiving party, laws and regulations serving as the legal basis for the process in which the information is to be used, the scope of information or recorded particulars that are to be used, and the method of use, etc.

2. When providing personal information to parties other than administrative organs or incorporated administrative agencies etc. pursuant to Article 69, paragraph 2, items 3 and 4 of the Protection Act , personal information protection managers shall, in addition to requesting that the security of the information be protected, if deemed necessary, perform an investigation(s) etc. before the information is provided or on an as-needed basis to confirm that necessary measures are in place, keep a record of the investigation(s), and, based on the results of the investigations etc. take the necessary steps to request improvements etc.
3. When providing personal information to an administrative organ or incorporated administrative agency etc. pursuant to Article 69, paragraph 2, item 3 of the Protection Act, if deemed necessary, personal information protection managers shall take steps specified in the two previous paragraphs.
4. Except in cases that are clearly specified in the Numbers Act, personal information protection managers must not provide specific personal information.

(Outsourcing of Operations etc.)

Article 55. If an operation relating to the handling of personal data (including the preparation of anonymized information. The same applies below) is outsourced to an external party, necessary measures shall be implemented to prevent the selection of a party that does not have the ability to appropriately manage personal information. In addition to clearly indicating in the contract the matters set forth in the items below, necessary items shall be confirmed in writing including matters relating to the party to whom the relevant operation is outsourced such as the person in charge, management and implementation system of persons involved in the operation, and matters relating to the monitoring of the management status of personal information.

(i) Obligations to protect the confidentiality of personal information and prohibit it from being used for any purpose other than that intended.
(ii) Matters relating to restrictions and conditions such as advanced notification relating to multi-tiered contracting arrangements (including cases in which the subcontracted party is a subsidiary (as defined in Article 2, item 3 of the Companies Act (law no. 86 of 2005) of the contracted party. The same applies to this item and paragraph 5).

(iii) Matters relating to restrictions on the reproduction of personal information.
(iv) Matters relating to measures for the secure management of personal information.
(v) Matters relating to response when a problem such as leakage of personal information occurs.
(vi) Matters relating to the deletion of personal information and return of media when the contracted arrangement ends.
(vii) Matters relating to contract cancellation and liability for damages etc. in the case of violation of a law or the contract.
(viii) Matters relating to periodic reporting on contract compliance and matters relating to audits etc. to monitor the handling status of personal information by the contracted party (including matters relating to the audit of subcontracted parties).

2. When a process using individual numbers etc. is outsourced in whole or in part, it shall be confirmed in advance whether the contracted party has established measures for the secure management of personal information that are equivalent in effect to measures that NIES is obligated to establish pursuant to the Numbers Act.
3. When a process using Personal information the administrative entity holds is outsourced to an external party, in accordance with the confidentiality, content, volume, etc. of the Personal information the administrative entity holds relating to the outsourced process, the management and implementation systems established by the contracted party and the management status of personal information shall be confirmed by performing an onsite inspection at least once a year.
4. When a process using individual numbers etc. is outsourced in whole or in part, necessary and appropriate supervision shall be provided to ensure that the contracted party establishes measures for the secure management of personal information that are equivalent in effect to those that NIES is obligated to establish.
5. When a process involving the handling of Personal information the administrative entity holds is subcontracted by the contracted party, in addition to ensuring that the subcontracted party establishes the measures stipulated in paragraph 1, depending on the confidentiality and content of the process involving Personal information the administrative entity holds that is further subcontracted, NIES shall perform the supervision stipulated in paragraph 3 either directly or through the contracted party. The same applies when a process involving the handling of Personal information the administrative entity holds is subcontracted by contracted parties beyond the initial contracted party.
6. When a process using individual numbers etc. is subcontracted by the contracted party in whole or in part, acceptance or refusal of the subcontracting shall be decided after confirming whether the security of the specific personal information handled as part of the contracted process using individual numbers etc. will be appropriately managed.
7. When a process that involves the handling of Personal information the administrative entity holds is to be performed by a temporary worker, clearly indicate the duty of confidentiality and other matters related to the handling of personal information in the contract with the relevant temporary worker.
8. When Personal information the administrative entity holds is provided or when a process involving the handling of Personal information the administrative entity holds is outsourced, consider the purpose of use of the party provided with the relevant information, the nature of the contracted process, and the confidentiality and content of the Personal information the administrative entity holds and, as necessary, implement measures to anonymize the data by replacing names with numbers etc. from the standpoint of reducing the risk of damage due to leakage.

Chapter 10. Disclosure, Corrections, Ceasing to Use, and Appeals for Review

(Disclosure, Corrections, Ceasing to Use, and Appeals for Review)
Article 56. NIES shall process requests for disclosure, revision, cessation of use, and review of personal information according to detailed provisions based on law prescribed elsewhere.

Chapter 11. Processing of Complaints

(Processing of Complaints)
Article 57. NIES shall endeavor to deal appropriately and promptly with complaints regarding the handling of personal information.
2. NIES shall establish a contact point for receiving consultations and handling complaints in the General Affairs Office.

Chapter 12. Addressing Security-related Problems

(Reporting Leaks)

Article 58. In the occurrence of a circumstance relating to the security of personal information the administrative entity holds such as leakage, loss or damage wherein damage to the rights and interests of an individual or individuals is highly likely, executives and employees who confirms the circumstance etc. set forth in the items below shall immediately report the circumstance to the personal information protection manager responsible for managing the relevant personal information the administrative entity holds.

(i) The occurrence or suspected occurrence of leakage, loss, or damage (hereinafter in this Article, "leakage etc.") of personal data containing sensitive personal information (except for personal information to which a necessary measure to ensure the protection of individual rights and interests such as advanced encryption has been applied. The same applies below in this Article).

(ii) The occurrence or suspected occurrence of leakage etc. wherein property damage due to misuse of the relevant information is likely.

(iii) The occurrence or suspected occurrence of leakage etc. of personal information for a wrongful purpose.

(iv) The occurrence of suspected occurrence of leakage etc. involving the data of more than 1000 individuals.

2. The personal information protection manager shall promptly implement measures necessary to prevent the expansion of damage and incident recovery. However, for measures to prevent the further spread of damage that can be implemented immediately, such as disconnecting the LAN cable from a computer terminal for which unauthorized access from outside NIES or infection with malware is suspected, the personal information protection manager shall perform such measures immediately (including making members take these measures).

3. The personal information protection manager shall identify the chain-of-events leading to the incident and the extent of damage, etc. and report in a timely manner to the general personal information protection manager. However, incidents deemed particularly serious shall be immediately reported to the general personal information protection manager.

4. A general personal information protection manager who receives a report pursuant to the immediately preceding paragraph shall, depending on the nature of the case, promptly report the nature of, circumstances leading up to, and state of damage caused by the case to the President of the Institute.

5. The general personal information protection manager shall, depending on the nature of the case, promptly provide information to the Ministry of the Environment regarding the nature of, circumstances leading up to, and state of damage caused by the case.

6. The personal information protection manager shall determine the cause of the occurrence and implement necessary measures to prevent further recurrence.

(Public Announcements etc.)

Article 59. Depending on the content and influence of the incident, NIES shall take necessary step such as making a public announcement regarding the facts of the case and measures to prevent recurrence and dealing with the individual(s) whose personal information is at the center of the incident in question,

2. For incidents that will be publicly announced, NIES shall promptly provide information regarding the particulars, steps leading up to the incident, and the extent of damage to the Personal Information Protection Commission.

Chapter 13. Audits and Inspections

(Audits)

Article 60. The Personal Information Protection Auditor shall conduct audits (including external audits), either periodically or on an as-needed basis, to verify that personal information is being managed properly and the management status of personal information at NIES, including the status of measures prescribed in Chapters 2 to 12 of these regulations. The results of audits will be reported to the general personal information protection manager.

(Inspections)

Article 61. Personal information protection managers shall conduct inspections, either periodically or on an as-needed basis, of storage media, processing pathways, storage methods, etc. for personal information for which he or she is responsible and shall report the results of inspections to the general personal information protection manager.

(Evaluations and Reviews)

Article 62. Taking the audit and inspection results into consideration, the Chief Personal Information Protection Officer, personal information protection managers, etc. shall evaluate measures for appropriately managing personal information from the perspective of their effectiveness based on audit or inspection findings and shall review such measures when deemed necessary.

Chapter 14. Cooperation with Ministry of the Environment

Article 63. NIES shall carry out appropriate management of the personal information in its possession in close with Ministry of Environment personal information in question based on Paragraph 4 of the *Basic Policy on the Protection of Personal Information* (Cabinet decision on April 2, 2004).

Supplementary provisions. These regulations shall come into force on April 1, 2005.

Amended provisions. These regulations shall come into force on June 1, 2007.

Amended provisions. These regulations shall come into force on April 1, 2011.

Amended provisions. These regulations shall come into force on April 1, 2015.

Amended provisions. These regulations shall come into force on December 1, 2015.

Amended provisions. These regulations shall come into force on December 21, 2016.

Amended provisions. These regulations shall come into force on September 20, 2017.

Amended provisions. These regulations shall come into force on January 4, 2019.

Amended provisions. These regulations shall come into force on April 20, 2022.