Regulations on the Management of Personal Information of Nagasaki University

Table of Contents

Chapter 1　General Provisions

(Purpose)

Article 1　These Regulations set forth the matters necessary for appropriate management of the Personal Information and Anonymized Personal Information and Other Related Information Held by an Administrative Organ, etc. (hereinafter referred to as "Personal Information, etc.") that Nagasaki University (hereinafter referred to as the "University") retains, in accordance with the provisions of Article 58 of the Rules and Regulations on Personal Information Protection of Nagasaki University (Rule No. 6 of 2005; hereinafter referred to as the "Rules and Regulations").

2　The appropriate management of Personal Information, etc. retained by the University shall be as provided for in these Regulations, in addition to the Act on the Protection of Personal Information (Act No. 57 of 2003; hereinafter referred to as the “Act”), the Act on the Use of Numbers to Identify a Specific Individual in

Administrative Procedures (Act No. 27 of 2013), the Regulations on the Management of Specific Personal Information of Nagasaki University (Regulation No. 51 of 2015), and other laws, regulations, etc. that specifically provide for in this regard.

(Definitions)

Article 2　In these Regulations, "Personal Information," "Subject Person," “Aliased Personal Information,” “Personal Data,” “Retained Personal Information,” “Anonymized Personal Information Held by an Administrative Organ, etc.,” and "Department, etc." mean the Personal Information, Subject Person, Aliased Personal Information, Personal Data, Retained Personal Information, Anonymized Personal Information Held by an Administrative Organ, etc., and Department, etc. prescribed in Article 2 of the Rules and Regulations.

2　In these Regulations, "Deleted Information" means the deleted information prescribed in Article 38, paragraphs 3 and 4 of the Rules and Regulations.

3　In these Regulations, "Anonymized Personal Information and Other Related Information Held by an Administrative Organ, etc." means the Anonymized Personal Information and Other Related Information Held by an Administrative Organ, etc. as prescribed in Article 50, paragraph 2 of the Rules and Regulations.

Chapter 2　Management System

(General Protection Administrator)

Article 3　The University shall have a general protection administrator, and this role shall be assumed by the Trustee or Vice President appointed by the President.

2　The general protection administrator shall oversee affairs related to the management of Retained Personal Information, Aliased Personal Information and Anonymized Personal Information and Other Related Information Held by an Administrative Organ, etc. (hereinafter referred to as “Retained Personal Information, etc.”) at the University.

(Protection Administrator)

Article 4　A protection administrator shall be placed in the administrative department of each Department, etc. that deals with Retained Personal Information, etc. (if a division or office is set up, the division or office; hereinafter referred to as a “Division/Office, etc.”), and this role shall be assumed by the director of the

Division/Office, etc.

2 The protection administrator shall ensure appropriate management of Retained Personal Information, etc. in his/her Division/Office, etc. ; provided, however, that if Retained Personal Information, etc. is handled on an information system, relevant operations shall be performed in cooperation with the administrator of the information system.

3 Notwithstanding the provisions of the preceding two paragraphs, for the management of Retained Personal Information, etc. related to education, research, or medical care, the director of the relevant Department, etc. shall serve as protection administrator.

(Person in Charge of Protection)

Article 5 A person in charge of protection shall be placed in each Division/Office, etc. that handles Retained Personal Information, etc., and this role shall be assumed by the person appointed by the protection administrator of the Division/Office, etc.

2 The person in charge of protection shall assist the protection administrator and take charge of affairs related to the management of Retained Personal Information, etc. in his/her Division/Office, etc.

3 Notwithstanding the provisions of the preceding two paragraphs, for affairs concerning the management of Retained Personal Information, etc. related to education, research, or medical care, the person appointed by the director of the relevant Department, etc. shall serve as the person in charge of protection.

(Audit Controller)

Article 6 The University shall have an audit controller, and this role shall be assumed by the Auditor appointed by the President.

2 The audit controller shall audit the status of management of Retained Personal Information, etc. at the University.

(Committee for Appropriate Management of Retained Personal Information, etc.)

Article 7 The Nagasaki University Personal Information Protection Committee (hereinafter referred to as the “Committee”) decides, communicates, and makes adjustments to important matters concerning the management of Retained Personal Information, etc. at the University.

Chapter 3　Education and Training

(Education and Training)

Article 8　The general protection administrator shall enlighten employees who are involved in the handling of Retained Personal Information, etc. (including dispatched workers; the same applies hereinafter) and provide them with other necessary education and training in order to deepen their understanding of the handling of Retained Personal Information, etc. and raise their awareness of the protection of Personal Information and the appropriate management of Anonymized Personal Information and Other Related Information Held by an Administrative Organ, etc.

2　The general protection administrator shall provide employees engaged in affairs related to the management of information systems handling Retained Personal Information, etc. with necessary education and training regarding the management, operation, and security measures of information systems in order to ensure appropriate management of Retained Personal Information, etc.

3　The general protection administrator shall provide protection administrators and persons in charge of protection with education and training for appropriate management of Retained Personal Information, etc. on such sites as Divisions/Offices, etc.

4　The protection administrator of a Department, etc. or Division/Office, etc. shall take necessary measures to ensure appropriate management of Retained Personal Information, etc., such as providing the employees of the Department, etc. or Division/Office, etc. with opportunities to participate in education and training provided by the general protection administrator.

Chapter 4　Responsibilities, etc. of Employees

(Responsibilities of Employees)

Article 9　Employees shall handle Retained Personal Information, etc. in the spirit of the Act, in accordance with the provisions of relevant laws, regulations, etc., and in conformity with the instructions of the general protection administrator, protection administrators, and persons in charge of protection.

2　Employees shall receive the education and training that pertain to Personal Information protection and are designated by the general protection administrator.

(Restrictions on Handling Work)

Article 9-2　Protection administrators may choose not to assign any work involving the handling of Retained Personal Information, etc. to those employees who have not received the education and training set forth in paragraph 2 of the preceding Article.

Chapter 5　Handling of Retained Personal Information, etc.

(Access Restrictions)

Article 10　According to the confidentiality and contents of Retained Personal Information, etc., the protection administrator shall limit the scope of employees who are to have the authority to access such Retained Personal Information, etc. and the contents of the authority to the minimum necessary scope for such employees' work.

2　Employees without access authority must not access Retained Personal Information, etc.

3　Even if employees have access authority, such employees must not access Retained Personal Information, etc. for purposes other than business purposes.

(Restrictions on Reproduction, etc.)

Article 11　Even when an employee handles Retained Personal Information, etc. for a business purpose, the protection administrator shall, in accordance with the confidentiality and contents of the Retained Personal Information, etc., limit the cases in which the employee may engage in any of the following acts, and the employee shall conduct the applicable act in conformity with the instructions of the protection administrator:

(1) Reproduction of the Retained Personal Information, etc.;

(2) Transmission of the Retained Personal Information, etc.;

(3) Sending or taking out the medium on which the Retained Personal Information, etc. is recorded; or

(4) Other acts that may hinder appropriate management of the Retained Personal Information, etc.

(Correction of Errors, etc.)

Article 12　If employees find any errors, etc. in the contents of Retained Personal Information, etc., they shall make corrections, etc. in accordance with the instructions of their protection administrators.

(Media Management, etc.)

Article 13　In accordance with the instructions of their protection administrators, employees shall store media on which Retained Personal Information, etc. is recorded at the designated places and, when it is found necessary, store them in a fireproof safe and lock it or take other necessary action.

(Disposal, etc.)

Article 14　When any Retained Personal Information, etc., or any medium on which Retained Personal Information, etc. is recorded (including any media embedded on terminals or servers), is no longer required, employees shall follow the instructions of their protection administrators and erase the information, etc. or dispose of the medium in a manner that makes it impossible to restore or decipher the Retained Personal Information, etc.

(Recording of the Status of Handling of Retained Personal Information, etc.)

Article 15　Protection administrators shall, according to the confidentiality and contents of Retained Personal Information, etc., maintain registers, etc. and record the statuses of use, storage, and other manners of handling of the Retained Personal Information, etc.

Chapter 6　Ensuring of Safety, etc. on Information Systems

(Access Control)

Article 16　Protection administrators shall, in accordance with the confidentiality and contents of Retained Personal Information, etc. (limited to such information, etc. handled on information systems;　the same applies hereinafter in this Chapter (except in Article 25)), take measures necessary for access control, such as setting up a function for identifying the user's authority by such means as a password (meaning a password, IC card, biometric information, etc.; hereinafter the same applies) (hereinafter referred to as an "Authentication Function").

2　When protection administrators take the measures in the preceding paragraph, they shall set out provisions regarding the management of passwords, etc. (including the periodical and as-needed review of such passwords, etc.) and also take necessary measures, for example, to prevent the unauthorized reading of passwords, etc.

(Access Records)

Article 17　Protection administrators shall take necessary measures to record the access status of Retained Personal Information, etc. according to its confidentiality and contents, to store this record (hereinafter referred to as an "Access Record") for a certain period of time, and to periodically analyze such access record.

2　Protection administrators shall take necessary measures to prevent the falsification, theft, or unauthorized deletion of Access Records.

(Access Status Monitoring)

Article 18　Protection administrators shall, according to the confidentiality, contents, and amount of Retained Personal Information, etc., take necessary measures to monitor any improper access to such information, etc., such as setting up a function to display a warning when a certain volume or more of information that contains, or may contain, Retained Personal Information, etc. is downloaded from an information system and periodically checking the settings of such function.

(Setting of Administrator Privileges)

Article 18-2　Protection administrators shall, according to the confidentiality and contents of Retained Personal Information, etc., take necessary measures to minimize damage when the administrator privileges of the relevant information system are stolen and to prevent unauthorized operation, etc. from within, which includes minimizing such privileges.

(Prevention of Unauthorized Access from Outside)

Article 18-3　Protection administrators shall take necessary measures to prevent unauthorized access from outside to information systems that handle Retained Personal Information, etc., such as setting a firewall to control routes.

(Prevention of Leakage due to Malicious Programs)

Article 19　In order to prevent any leakage, loss, or damage of Retained Personal Information, etc. due to malicious programs, protection administrators shall take necessary measures to eliminate disclosed software vulnerabilities and to prevent infection by known malicious programs (including keeping installed software up to date at all times).

(Processing of Retained Personal Information, etc. on Information Systems)

Article 19-2　In the case where an employee is to, for example, temporarily reproduce

Retained Personal Information, etc. to process it, the part of the information, etc. to be reproduced shall be limited to the necessary minimum, and any information, etc. that is no longer necessary shall be promptly erased after the completion of processing.

2 Protection administrators shall prioritize the checking of the implementation status of erasure, etc. of Retained Personal Information, etc. as required according to the confidentiality and contents of the information, etc.

(Encryption)

Article 20 Protection administrators shall take necessary measures for encryption of Retained Personal Information, etc. according to the confidentiality and contents of the information, etc.

2 Based on the measures specified in the preceding paragraph, employees shall appropriately encrypt the Retained Personal Information, etc. that they process according to the confidentiality and contents of the information, etc.

(Restrictions on the Connection of Devices and Media with a Recording Function)

Article 21 Protection administrators shall take necessary measures to prevent any leakage of, loss of, or damage to Retained Personal Information, etc. according to the confidentiality and contents of the information, etc., such as restricting the connection of devices and media with a recording function, such as smartphones and USB flash drives, to information system terminals, etc. (including support for updating such devices).

(Limitation on Terminals)

Article 22 Protection administrators shall take necessary measures to limit terminals to be used for processing Retained Personal Information, etc. according to the confidentiality and contents of the information, etc.

(Prevention of Theft of Terminals, etc.)

Article 23 Protection administrators shall take necessary measures to prevent terminals from being stolen or lost, such as fixing terminals to their designated locations and locking offices.

2 Employees must not take any terminals to the outside or bring any terminals inside from the outside, unless their protection administrators find it necessary.

(Prevention of Browsing by Third Parties)

Article 24　In using terminals, employees shall take necessary measures to prevent Retained Personal Information, etc. from being browsed by any third party, such as thoroughly ensuring that the user is logged off from the information system according to the usage status.

(Verification, etc. of Input Information)

Article 25　Employees shall, among other actions and according to the degree of importance of specific Retained Personal Information, etc. handled on an information system, collate the original input document with the input contents, verify the contents of the information, etc. before and after processing, and cross-check the input information, etc. against the existing Retained Personal Information.

(Backup)

Article 26　Protection administrators shall take necessary measures to create backups and decentralize the storage of Retained Personal Information, etc. according to the degree of importance of the information, etc.

(Management of Information System Design Documents, etc.)

Article 26-2　In order to prevent any details of the design documents, configuration diagrams, etc. of information systems relating to Retained Personal Information, etc. from being exposed to the outside, protection administrators shall take necessary measures in relation to the storage, reproduction, disposal, etc. of such documents, diagrams, etc.

Chapter 7　Safety Management of Information System Rooms, etc.

(Entry and Exit Control)

Article 27　Protection administrators shall determine who has the authority to enter rooms where core devices that handle Retained Personal Information, etc., such as a server, are installed and other relevant areas (hereinafter referred to as an "Information System Room, etc."), and they shall also take such measures as confirming the reason for entering, recording entries/exits, identifying outsiders, ensuring an employee's presence or monitoring with surveillance equipment when an outsider enters, and restricting or checking for the carry-in, use, or taking-out of external electromagnetic recoding media, etc.

2　In the case where any facilities to store media for recording Retained Personal Information, etc. have been set up and where a protection administrator finds it necessary, the protection administrator shall take the same measures as those in the preceding paragraph.

3　If a protection administrator finds it necessary, the protection administrator shall take such measures as facilitating the entry/exit management by designating a specific entrance and exit of the relevant Information System Room, etc. and limiting displays indicating the location.

4　If a protection administrator finds it necessary for the entry/exit management of an Information System Room, etc. or storage facilities, the protection administrator shall set up an Authentication Function related to entry and take necessary measures, for example, to set out provisions concerning the management of passwords, etc. (including periodic and as-needed review of such provisions) and to prevent any unauthorized reading of passwords, etc.

(Management of Information System Rooms, etc.)

Article 28　Against any unauthorized access from outside, protection administrators shall take such measures as the installation of locking devices, alarm devices, and surveillance equipment in Information System Rooms, etc.

2　In case of disasters or other similar events, protection administrators shall take necessary measures in this regard, such as making Information System Rooms, etc. earthquake-resistant, fireproof, smokeproof, and waterproof, and also take such measures as securing a standby power system for devices, including servers, and preventing damage to wires.

Chapter 8　Provision of Retained Personal Information, etc. and Outsourcing of Operations, etc.

(Provision of Personal Data, Anonymized Personal Information Held by an Administrative Organ, etc., or Deleted Information)

Article 29　In the case where a protection administrator provides Personal Data to a person other than administrative organs, incorporated administrative agencies, etc. pursuant to the provisions of the items of Article 13, paragraph 1 of the Rules and Regulations, the protection administrator shall, in principle, exchange with the

recipient of the information a document setting out the purpose of use of such information by the recipient, the laws that are the basis of the work for which such information is to be used, the scope of records and record items to be used, the form of use, etc.

2 In the case where a protection administrator provides Personal Data to a person other than administrative organs, incorporated administrative agencies, etc. pursuant to the provisions of the items of Article 13, paragraph 1 of the Rules and Regulations, the protection administrator shall request that person to implement security measures and also, if finding it necessary, conduct field investigations, etc. before provision or on an as-needed basis, check the status of implementation of relevant measures, record the results of such check, and take such measures as requesting improvement.

3 In the case where a protection administrator provides Personal Data to an administrative organ, incorporated administrative agencies, etc. pursuant to the provisions of Article 13, paragraph 1, item (4) of the Rules and Regulations and where the protection administrator finds it necessary, the protection administrator shall take the measures specified in the preceding two paragraphs.

4 In accordance with the provisions of Article 38, paragraph 2 of the Rules and Regulations, protection administrators must not personally use or provide Anonymized Personal Information Held by an Administrative Organ, etc. or Deleted Information for purposes other than the purpose of its use, except under applicable laws and regulations.

5 If a protection administrator receives a report from a person who has executed a contract for use of Anonymized Personal Information Held by an Administrative Organ, etc. (hereinafter referred to as the "Counterparty") in accordance with the provisions of Article 38, paragraph 1 and Article 44 of the Rules and Regulations (including the case where the provisions of Article 44 apply mutatis mutandis pursuant to the provisions of Article 47) on any potential hindrance to the appropriate management of Anonymized Personal Information Held by an Administrative Organ, etc. implemented by the Counterparty on the basis of the details of a proposal prescribed in Article 110, paragraph 2, item (vii) of the Act, the

protection administrator shall immediately report it to the general protection administrator and also check the measures taken by the Counterparty in making corrections to the situation.

(Outsourcing of Operations, etc.)

Article 30　When a protection administrator is to outsource any operations relating to the creation of Anonymized Personal Information Held by an Administrative Organ, etc. or relating to the handling of Retained Personal Information, etc., the protection administrator shall take necessary measures to ensure that persons without competence to implement appropriate management of Personal Information, etc. are not selected as the undertaking party and shall also specify the following matters in a contract, etc. and confirm other necessary matters in writing, such as those regarding the inspection of the outsourced contractor's management of responsible persons and persons to engage in the relevant operations, implementation structure, and management status of Personal Information, etc.:

(1) Obligations such as the maintenance of confidentiality of Personal Information, etc. and the prohibition of use for unintended purposes;

(2) Matters concerning restrictions on subcontracting (including cases where the subcontractor is the outsourced contractor's subsidiary (meaning a subsidiary as prescribed in Article 2, paragraph 1, item (iii) of the Companies Act (Act No. 86 of 2005)); hereinafter the same applies in this Article) or conditions for subcontracting such as prior approval;

(3) Matters concerning restrictions on the reproduction, etc. of Personal Information, etc.;

(4) Matters concerning responses in the case where, for example, a leak of Personal Information, etc. occurs;

(5) Matters concerning the deletion of Personal Information, etc. and the return of media at the close of outsourcing; and

(6) The cancellation of the contract, liability for damages, and other necessary matters in the case of a contractual breach.

2　When a protection administrator is to outsource any operations relating to the creation of Anonymized Personal Information Held by an Administrative Organ, etc.

or relating to the handling of Retained Personal Information, etc., and also where Retained Personal Information, etc. is to be taken to the outside, the protection administrator shall apply to the general protection administrator for approval by using the separately designated application form for outsourcing of Retained Personal Information, etc.

3 Upon receiving an application under the preceding paragraph, the general protection administrator shall determine whether to give approval for the relevant outsourcing after review by the Committee and shall promptly notify the protection administrator; provided, however, that the review by the Committee may be omitted if it is deemed not particularly necessary by the general protection administrator.

4 When a protection administrator is to outsource any operations relating to the handling of Retained Personal Information, etc., the protection administrator shall, according to the confidentiality, contents, amount, etc. of the Retained Personal Information, etc. related to the operations to be outsourced, conduct an on-site inspection, in principle at least annually, to check the outsourced contractor's management system, implementation structure, and management status of Personal Information, etc.

5 If an outsourced contractor is to subcontract any operations relating to the creation of Anonymized Personal Information Held by an Administrative Organ, etc. or relating to the handling of Retained Personal Information, etc., the relevant protection administrator shall have the outsourced contractor take the measures specified in paragraph 1, and also the outsourcing party shall, personally or through the outsourced contractor, take the measures specified in the preceding paragraph according to the confidentiality and contents of the Retained Personal Information, etc. relating to the operations to be subcontracted. The same shall apply to cases where a subcontractor is to sub-subcontract any operations relating to the creation of Anonymized Personal Information Held by an Administrative Organ, etc. or relating to the handling of Retained Personal Information, etc. and to cases of any further subsequent contracting out.

6 If a protection administrator is to have any dispatched workers engage in any operations relating to the creation of Anonymized Personal Information Held by an

Administrative Organ, etc. or relating to the handling of Retained Personal Information, etc., the protection administrator shall specify matters concerning the handling of Personal Information and Anonymized Personal Information and Other Related Information Held by an Administrative Organ, etc., such as the obligation of confidentiality, in the relevant worker dispatch contract.

(Other)

Article 30-2　When Retained Personal Information, etc. is provided or any operations related thereto are outsourced, anonymization measures shall be taken where necessary, such as replacing names with numbers, from the perspective of reducing the risk of damage caused by leakage, etc., with due consideration given to the purpose of use at the recipient, the contents of the outsourced operations, and the confidentiality and contents of the information, etc.

Chapter 9　Dealing with Security Issues

(Case Report and Recurrence Prevention Measures)

Article 31　If an employee recognizes any case involving a security problem, such as a leak of Retain Personal Information, or any risk that a problematic case may arise, such employee shall immediately report it to the protection administrator in charge of the relevant Retained Personal Information, etc.

2　The protection administrator shall promptly take necessary measures to prevent the spread of damage, measures for restoration, etc.; provided, however, that any measures that can be implemented immediately to prevent the spread of damage, such as unplugging the LAN cable of the relevant terminal suspected of being subjected to unauthorized access from the outside or being infected with a malicious program, shall be taken immediately (including having any employee do so).

3　The protection administrator shall investigate the circumstances surrounding the occurrence of the case, the damage situation, etc. and report to the general protection manager ; provided, however, that if a case that the protection administrator finds to be particularly serious has occurred, the protection administrator shall immediately report to the general protection administrator on the details, etc. of the case concerned.

4　Upon receiving a report under the preceding paragraph, the general protection

administrator shall promptly report to the President on the details, circumstances, damage situation, etc. of the case concerned.

5 The protection administrator shall analyze the cause of the case concerned and take necessary measures to prevent its recurrence.

(Announcement, etc.)

Article 32 The general protection administrator and relevant protection administrator shall, according to the details, impact, etc. of the case concerned, take such measures as announcing the factual situation of the case and recurrence prevention measures and dealing with the Subject Person associated with the Retained Personal Information related to the case.

Chapter 10 Implementation of Audit and Inspection

(Audit)

Article 33 In order to verify the appropriate management of Retained Personal Information, etc., the audit controller shall, periodically and on an as-needed basis, conduct an audit (including external audits; hereinafter the same applies) on the status of management of Retained Personal Information, etc. at the University, which also covers the status of implementation of the measures set forth in Chapter 2 through the preceding Chapter, and report the results of the audit to the general protection administrator.

(Inspection)

Article 34 Protection administrators shall, periodically and on an as-needed basis, inspect the recording media, process route, storage method, etc. of Retained Personal Information, etc. in their respective Divisions/Offices, etc., and, when they find it necessary, they shall report the results of the inspection to the general protection administrator.

(Evaluation and Review)

Article 35 The general protection administrator, protection administrators, etc. shall evaluate measures for appropriate management of Retained Personal Information, etc. on the basis of the results of audits and inspections and from the perspective of effectiveness, etc., and, when they find it necessary, they shall take such measures as reviewing the above management measures.

Chapter 11　Cooperation with Administrative Organs

Article 36　On the basis of the Basic Policy on the Protection of Personal Information (Cabinet Decision on April 2, 2004) 4, the University shall appropriately manage the Personal Information that it retains in close cooperation with the Ministry of Education, Culture, Sports, Science and Technology.

Chapter 12　Miscellaneous Provisions

(Auxiliary Provisions)

Article 37　In addition to what is prescribed in these Regulations, necessary matters concerning the management of Retained Personal Information, etc. may be prescribed separately.