○Management Regulations on Personal Information, etc. of National Institute of Maritime, Port and Aviation Technology

June 23, 2016
Institute Regulations No. 31

Revised: June 30, 2017 Institute Regulations No. 60
Revised: January 31, 2020 Institute Regulations No. 92

Table of Contents

Chapter I General Provisions

(Purpose)

Article 1. The purpose of these Regulations is to specify matters necessary for the appropriate management of personal information and individual numbers retained by the National Institute of Maritime, Port and Aviation Technology (hereinafter referred to as the "Institute"), in connection with the handling of retained personal information and individual numbers (hereinafter collectively referred to as "Retained Personal Information, etc.") as specified in the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003; hereinafter referred to as the "Act") and the Act on the Use of Numbers to Identify Specific Individuals in

Administrative Procedures (Act No. 27 of 2013; hereinafter referred to as the "Numbers Act").

(Definitions)

Article 2. The terms used in these Regulations shall be in accordance with the terms used in the Act and the Numbers Act.

Chapter II Management Systems

(General Protection Manager)

Article 3. The institute shall have in place one General Protection Manager, and the Director of the General Affairs Division shall concurrently serve in such position.

(2) The General Protection Manager shall be in charge of general coordination of the affairs concerning the management of Retained Personal Information, etc. at the Institute.

(Protection Manager)

Article 4. Each section, office, etc. that handles Retained Personal Information, etc. shall have in place one Protection Manager, and the head of such section, office, etc. or a substitute thereof shall concurrently serve in such position.

(2) The Protection Manager shall be in charge of ensuring the appropriate management of Retained Personal Information, etc. in each section, office, etc. In cases where Retained Personal Information, etc. is handled by an information system, the Protection Manager shall perform his/her duties in cooperation with the administrator of such information system.

(3) The Protection Manager shall designate staff members (hereinafter referred to as "Staff Members Responsible for Handling Affairs") who handle individual numbers and specific personal information (hereinafter collectively referred to as "Specific Personal Information, etc.") and their roles.

(4) The Protection Manager shall designate the scope of Specific Personal Information, etc. to be handled by each Staff Member Responsible for Handling Affairs.

(5) The Protection Manager shall establish the following organizational structure:

(i) A reporting and communication system available in the event that facts that violations of these Regulations, etc. by any Staff Member Responsible for Handling Affairs or indications thereof are ascertained;

(ii) A reporting and communication system available in the event that the occurrence of a case of leakage, loss, or corruption (hereinafter referred to as "Leakage, etc.") of Specified Personal Information, etc. or indications thereof are ascertained;

(iii) Clarification of the division of duties and responsibilities between multiple departments available in cases where Specific Personal Information, etc. is handled by multiple departments; and

(iv) Response system available in the event that the occurrence of a case of Leakage, etc. of Specific Personal Information, etc. or indications thereof are ascertained.

(6) When the Protection Manager has made the designations or established the organizational system

set forth in the preceding three paragraphs, he/she shall promptly inform the General Affairs Section of the General Affairs Division of the details of said designation or establishment.

(Supervision of Staff Members Responsible for Handling Affairs)

Article 4-2. The protection Manager shall provide necessary and appropriate supervision to Staff Members Responsible for Handling Affairs so that Specific Personal Information, etc. will be handled appropriately.

(Staff Members Responsible for Protection)

Article 5. Each section, office, etc. that handles Retained Personal Information, etc. may have in place one or more Staff Members Responsible for Protection designated by the Protection Manager of such section, office, etc.

(2) The Staff Members Responsible for Protection shall assist the Protection Manager and be in charge of affairs concerning the management of Retained Personal Information, etc. in each section, office, etc.

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

Article 6. The General Protection Manager shall, when he/she deems it necessary in order to decide, communicate or coordinate, etc. important matters pertaining to the management of Retained Personal Information, etc., establish a Committee consisting of relevant staff members, and convene meetings of said Committee on a regular basis or as needed.

(2) The Committee shall be presided over by the General Protection Manager, shall be composed of relevant staff members, and shall be convened by the General Protection Manager as necessary. The General Affairs Section of the General Affairs Division shall carry out the general affairs of the Committee.

Chapter III Education and Training

(Education and Training)

Article 7. The General Protection Manager shall provide staff members, etc. who are engaged in the handling of Retained Personal Information, etc. (refers to all persons working at the Institute; the same shall apply hereinafter) with enlightenment and other necessary education and training to improve their understanding of the handling of Retained Personal Information, etc. and to raise their awareness with regard to the protection of personal information.

(2) The General Protection Manager shall provide the staff members engaged in affairs concerning the management of information systems that process Retained Personal Information, etc. with the necessary education and training on the management, operation, and security measures of information systems in order to manage Retained Personal Information, etc. appropriately.

(3) The General Protection Manager shall periodically provide education and training to the Protection Manager and Staff Members Responsible for Protection in order to manage Retained Personal

Information, etc. in each section, office, etc. appropriately.
(4) The Protection Manager shall take necessary measures against staff members, etc. of his/her section, office, etc., such as granting an opportunity to participate in education and training conducted by the General Protection Manager, in order to manage Retained Personal Information, etc. appropriately.

Chapter IV Responsibilities of Staff, etc. Regarding Personal Information

(Responsibilities of Staff, etc.)

Article 8. In light of the purport of the Act and the Numbers Act, staff, etc. must handle Retained Personal Information, etc. in accordance with the provisions of relevant laws, regulations, etc. and the instructions of the General Protection Manager, the Protection Manager, and the Staff Members Responsible for Protection.
2 In the event that a staff member, etc. commits an act in violation of the Act, the Numbers Act, other relevant laws and rules, or these Regulations, etc., such staff member shall be dealt with strictly.

Chapter V Handling of Retained Personal Information, etc.

(Access Restrictions)

Article 9. The Protection Manager shall, as appropriate for the details of the Retained Personal Information, etc., such as its confidentiality, limit the scope of the staff, etc. who have the authority to access said Retained Personal Information, etc. and the details of such authority to the minimum extent necessary for said staff, etc. to perform their duties.
(2) Staff, etc. who do not have access authority shall not access Retained Personal Information, etc.
(3) Even when staff, etc. have access privileges, they shall not access Retained Personal Information, etc. for purposes other than official business purposes.

(Restrictions on Duplication, etc.)

Article 10. Even in cases where staff, etc. handle Retained Personal Information, etc. for official business purposes, the Protection Manager shall limit the cases in which the staff, etc. may perform the acts listed in the following items as appropriate for the confidentiality and other details of said Retained Personal Information, etc., and the staff, etc. shall abide by the instructions of the Protection Manager when performing said acts:
(i) Duplication of Retained Personal Information, etc.;
(ii) Transmission of Retained Personal Information, etc.;
(iii) Sending or carrying outside of the Institute a medium on which Retained Personal Information, etc. is recorded; and
(iv) Other acts that may hinder the appropriate management of Retained Personal Information, etc.

(Correction, etc. of Errors)

Article 11. In the event that staff, etc. find an error, etc. in the details of Retained Personal Information,

etc., the staff, etc. shall make corrections, etc. in accordance with the instructions of the Protection Manager.

(Media Management, etc.)

Article 12. Staff, etc. shall, in accordance with the instructions of the Protection Manager, store the media on which Retained Personal Information, etc. is recorded in a designated place, and when deemed necessary, store them in a fireproof safe, lock them, etc.

(Disposal, etc.)

Article 13. When Retained Personal Information, etc. or the media (including media built into terminals and servers) on which Retained Personal Information, etc. is recorded becomes unnecessary, staff, etc. shall erase such information or dispose of such media by a method that renders it impossible to restore or decipher such Retained Personal Information, etc., in accordance with the instructions of the Protection Manager.

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

Article 14. The Protection Manager shall prepare a ledger, etc. and record the status of the handling such as the use and storage of the Retained Personal Information, etc. as appropriate for the details of such Retained Personal Information, etc., such as its confidentiality.

(Restrictions on the Use of Individual Numbers)

Article 15. Staff Members Responsible for Handling Affairs shall use individual numbers only when processing the affairs specified in the Numbers Act.

(Restriction on Requests for Provision of Individual Numbers)

Article 15-2. Staff Members Responsible for Handling Affairs shall not request the provision of individual numbers, except in cases where it is necessary for the processing of affairs related to individual numbers or where otherwise specified in the Numbers Act.

(Restrictions on Handling, etc. of Specific Personal Information, etc.)

Article 15-3. Staff, etc. other than Staff Members Responsible for Handling Affairs shall not handle, collect, or retain the Specific Personal Information, etc. of others.

(2) Staff Members Responsible for Handling Affairs shall not handle Specific Personal Information, etc. outside the scope designated pursuant to Article 4, paragraph (4).

(Restrictions on Preparation of Specific Personal Information Files)

Article 15-4. Staff Members Responsible for Handling Affairs shall not prepare specific personal information files, except in cases where it is necessary for the processing of affairs related to individual numbers or where otherwise specified in the Numbers Act.

(Handling Area)

Article 15-5. The Protection Manager shall clarify the area where affairs that handle Specific Personal Information, etc. are to be conducted, and shall implement physical security management.

Chapter VI Ensuring Security, etc. in Information Systems

(Access Control)

Article 16. The Protection Manager shall take necessary measures for access control, such as establishing functions to identify authority (hereinafter referred to as the "Authentication function") using passwords, etc. (refers to passwords, IC cards, biometric information, etc.; the same shall apply hereinafter), as appropriate for the content of Retained Personal Information, etc., such as its confidentiality (limited to Retained Personal Information, etc. processed by information systems; the same shall apply hereinafter in this Chapter (excluding Article 26)).

(2) The Protection Manager shall draw up a regulation for the management of passwords, etc. (including periodic or ad hoc reviews thereof) and take necessary measures to prevent passwords, etc. from being read, etc. in case where the measures as set forth in the preceding paragraph are taken.

(Access Records)

Article 17. The Protection Manager shall record the status of access to the Retained Personal Information, etc., as appropriate for the content of such Retained Personal Information, etc., such as its confidentiality, preserve such records (hereinafter referred to as "Access Records") for a fixed period of time, and take necessary measures to analyze said Access Records periodically.

(2) The Protection Manager shall take the necessary measures for the prevention of falsification, theft, or unauthorized deletion of Access Records.

(Monitoring of Access Statuses)

Article 17-2. The Protection Manager shall take the necessary measures to monitor improper access to Retained Personal Information, etc. such as setting up a function to display a warning message when more than a certain amount of information that contains or is likely to contain Retained Personal Information, etc. is downloaded from information systems, and periodically confirming such settings, as appropriate for the content and quantity of said Retained Personal Information, etc., such as its confidentiality.

(Setting of Administrator Privileges)

Article 18. The Protection Manager shall take the necessary measures, such as minimizing the administrator privileges of information systems, in order to minimize damage when such administrator privileges are wrongfully stolen and to prevent internal unauthorized operations, etc., as appropriate for the details of Retained Personal Information, etc., such as its confidentiality.

(Prevention of Improper External Access)

Article 19. The Protection Manager shall take necessary measures, such as route control by setting up a firewall, in order to prevent improper external access to information systems that process Retained Personal Information, etc.

(Prevention of Leakage, etc. by Unauthorized Programs)

Article 20. In order to prevent leakage, loss, or corruption of Retained Personal Information, etc.

caused by unauthorized programs, the Protection Manager shall take necessary measures to resolve publicly disclosed vulnerabilities related to software, and to prevent infection by identified unauthorized programs, etc. (including always keeping the introduced software up-to-date).

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

Article 20-2. In the event that staff, etc. temporarily duplicate, etc. Retained Personal Information, etc. for the purpose of processing, etc., said staff, etc. shall limit the scope of said duplication, etc. to the minimum necessary and promptly delete the information that is no longer needed after the processing is completed. The Protection Manager shall, as needed, intensively check the implementation status of deletion, etc., as appropriate for the details of such Retained Personal Information, etc., such as its confidentiality.

(Encryption)

Article 21. The Protection Manager shall take the necessary measures for encryption as appropriate for the content of the Retained Personal Information, etc., such as its confidentiality.

(2) Based on the preceding paragraph, staff, etc. shall appropriately encrypt the Retained Personal Information, etc. to be processed by said staff, etc., as appropriate for the details of the Retained Personal Information, etc., such as its confidentiality.

(Restrictions on Connection of Devices and Media with Recording Functions)

Article 22. The Protection Manager shall take necessary measures, such as restricting the connection of devices and media with recording functions, such as smartphones and USB memory devices, to information system terminals, etc. (including taking action to update such devices), in order to prevent the leakage, loss, or corruption of the Retained Personal Information, as appropriate for the content of such Retained Personal Information, such as its confidentiality.

(Terminal Restrictions)

Article 23. The Protection Manager shall take the necessary measures to restrict the terminals that process Retained Personal Information, etc. as appropriate to the content of said Retained Personal Information, etc., such as its confidentiality.

(Prevention of Theft of Terminals, etc.)

Article 24. The Protection Manager shall take necessary measures, such as securing terminals in place and locking offices, to prevent theft or loss of terminals.

(2) Staff, etc. shall not take terminals outside the Institute or bring terminals inside the Institute, except when the Protection Manager deems it necessary.

(Prevention of Viewing by Third Parties)

Article 25. When using terminals, staff, etc. shall take necessary measures, such as ensuring that they log off information systems as appropriate according to use conditions, so that the Retained Personal Information, etc. will not be viewed by third parties.

(Collation of Input Information, etc.)

Article 26. Staff, etc. shall, according to the importance of the Retained Personal Information, etc. processed by information systems, compare the input source documents with the input content, confirm the content of such Retained Personal Information before and after processing, and check against existing Retained Personal information, etc.

(Backup)

Article 27. The Protection Manager shall take the necessary measures to backup and dispersedly store Retained Personal Information, etc. according to the importance of such Retained Personal Information, etc.

(Management of Information System Design Documents, etc.)

Article 28. The protection Manager shall take the necessary measures for the storage, duplication, and disposal, etc. of documents such as design documents and configuration drawings of information systems pertaining to Retained Personal Information, etc., so that said documents will not become known to outside parties.

Chapter VII Security Controls for Information System Rooms, etc.

(Access Controls)

Article 29. The Protection Manager shall designate persons who have the authority to enter rooms and other areas (hereinafter referred to as "Information System Rooms, etc.") where equipment such as core servers that process Retained Personal Information, etc. are installed, and shall take measures such as confirmation of requirements, recording of entry and exit, identification of non-affiliated persons, presence of staff or monitoring by monitoring equipment when non-affiliated persons enter, restriction of or inspection upon the entry, use, or removal of external electromagnetic recording media, etc. In addition, the same measures shall be taken, when deemed necessary, in cases where facilities for storing media recording Retained Personal Information, etc. are established.

(2) When the Protection Manager finds it necessary, he/she shall take measures such as facilitating the management of entry and exit by specifying the entrances and exits of Information System Rooms, etc., and restricting the display of the locations thereof.

(3) With regard to the management of entry and exit of Information System Rooms, etc. and storage facilities, the Protection Manager shall, when he/she deems it necessary, take necessary measures such as setting up an authentication function for entry, drawing up a regulation concerning the management of passwords, etc. (including periodic or ad hoc reviews thereof), and preventing passwords, etc. from being read.

(Management of Information System Rooms, etc.)

Article 29-2. The Protection Manager shall take measures such as installing locking devices, alarm devices, and monitoring equipment in Information System Rooms, etc., in preparation for unauthorized intrusion from the outside.

(2) In preparation for disasters, etc., the Protection Manager shall take necessary measures such as earthquake resistance, fire prevention, smoke prevention, and waterproofing in Information System Rooms, etc., and take measures such as securing a backup power supply for equipment such as servers and preventing damage to wiring.

Chapter VIII Provision of Retained Personal Information and Consignment of Work, etc.

(Provision of Retained Personal Information

Article 30. When providing Retained Personal Information, etc. to a party other than administrative organs and incorporated administrative agencies, etc. pursuant to the provisions of Article 9, paragraph 2, items (3) and (4) of the Act, the Protection Manager shall, in principle, exchange documents with the party to which the information is to be provided concerning the purpose of use, the laws and regulations on the basis of which the information is to be used, the scope of records and record items to be used, the form of use, etc.

(2) When providing Retained Personal Information, etc. to a party other than administrative organs and incorporated administrative agencies, etc. pursuant to the provisions of Article 9, paragraph 2, items (3) and (4) of the Act, the Protection Manager shall request such party to take measures to assure security and, when deemed necessary, conduct an on-site investigation, etc. prior to the provision of the Retained Personal Information, etc., or on an ad hoc basis, confirm the status of such measures to assure security, record the results of such confirmation and take measures such as requiring improvements.

(3) When providing Retained Personal Information, etc. to administrative organs and incorporated administrative agencies, etc. pursuant to the provisions of Article 9, paragraph 2, item (3) of the Act, the Protection Manager shall, when he/she deems it necessary, take the measures prescribed in the provisions of the preceding two paragraphs.

(4) Notwithstanding the provisions of the preceding three paragraphs, staff, etc. shall not provide Specified Personal Information, except in cases that fall under each item of Article 19 of the Numbers Act.

(Consignment of Work, etc.)

Article 31. In cases where consigning the handling of Retained Personal Information, etc. to an external party, necessary measures shall be taken to prevent the selection of a party that does not have the ability to appropriately manage personal information. In addition, the following matters shall be clearly stated in contracts, and necessary matters such as the management and implementation system of the responsible person(s) and business personnel at the consignee as well as matters concerning inspections of the status of personal information management shall be confirmed in writing:

(i) Obligations to maintain confidentiality regarding personal information, prohibit use for other purposes, etc.;

(ii) Matters concerning re-consignment conditions such as restrictions on, or prior approval of, re-consignment (including cases where the re-consignee is a subsidiary (refers to a subsidiary as prescribed in Article 2, paragraph 1, item 2 of the Companies Act (Act No. 86 of 2005)); the same shall apply in this item and paragraph (3)) of the consignee;
(iii) Matters concerning restrictions on the duplication, etc. of personal information;
(iv) Matters concerning actions taken in the event of leakage, etc. of personal information;
(v) Matters concerning erasure of personal information and return of media at the time of termination of consignment; and
(vi) Contract cancellation, liability for damages, and other necessary matters in the event of a breach of contract.
(2) When consigning work related to the handling of Retained Personal Information, etc. to an outside party, the management and implementation systems and the status of personal information management at the consignee shall be checked at least once a year, in principle, through on-site inspections, as appropriate for the content of the Retained Personal Information, etc. pertaining to the consigned work, such as its confidentiality, and for its volume, etc.
(3) In cases where work related to the handling of Retained Personal Information, etc. is re-consigned by a consignee, the consignee shall be required to take the measures set forth in Article 31, and the measures set forth in paragraph (2) shall be implemented either through the consignee or by the original consignor itself, as appropriate for the content of the Retained Personal Information, etc. pertaining to the re-consigned work, such as its confidentiality. The same shall also apply to cases where work pertaining to the handling of Retained Personal Information, etc. is consigned yet again by the re-consignee.
(4) When dispatched workers are to perform work pertaining to the handling of Retained Personal Information, etc., matters concerning the handling of personal information such as the obligation to maintain confidentiality shall be clearly stated in the worker dispatch contract.
(5) When providing Retained Personal Information, etc., or consigning work to third parties, in the light of reducing the risk of damage due to leakage, etc., anonymizing measures, such as replacing names with numbers, shall be taken as necessary, taking into consideration the purpose of use of the party to whom the information is provided, the details of the work to be consigned, the content such as the confidentiality of said Retained Personal Information, etc.

Chapter IX Actions Taken in Response to Problems with Ensuring Security

(Reporting of Cases and Measures to Prevent Recurrence)

Article 32. In the event that staff, etc. become aware of a case that poses a problem in ensuring the security of Retained Personal Information, etc., such as leakage, or the possibility of the occurrence of such case, they shall immediately report it to the Protection Manager who manages such Retained

Personal Information, etc.

(2) The Protection Manager shall promptly take the necessary measures to prevent the damage from spreading or restore to original state, etc.; provided, however, that measures that can be taken immediately to prevent the damage from spreading, such as unplugging the LAN cable of the relevant terminals, etc. suspected of having been subjected to unauthorized access or infection with malware from outside, shall be taken immediately (including by compelling staff to do so).

(3) The Protection Manager shall investigate the circumstances of the case, the damage situation, etc., and report to the General Protection Manager; provided, however, that in the event of a case deemed to be particularly serious, the outline of the case, etc. shall be immediately reported to the General Protection Manager.

(4) When the General Protection Manager receives a report based on the provisions of paragraph (3), the General Protection Manager shall promptly report to the President the details, background, and damage situation, etc. of the case, as appropriate for the details, etc. of the case.

(5) The General Protection Manager shall promptly provide information to the Ministry of Land, Infrastructure, Transport and Tourism on the details, circumstances, damage situation, etc. of the case, as appropriate for the details, etc. of the case.

(6) The Protection Manager shall analyze the cause of the incident and take the necessary measures to prevent recurrence.

(Publication, etc.)

Article 33. As appropriate for the details, impact, etc. of the case, measures shall be taken, such as publication of the facts of the case and measures to prevent its recurrence, and actions taken with regard to the principal of the Retained Personal Information, etc. relevant to the case in question. For cases that are to be publicized, information on the details of the relevant case, its background, and damage status, etc., shall be promptly provided to the Ministry of Land, Infrastructure, Transport and Tourism.

Chapter X Implementation of Auditing and Inspections

(Auditing)

Article 34. The Institute shall have one person responsible for auditing in place at the Institute, who shall be appointed in accordance with Article 4, paragraph 1 of the Internal Audit Regulations of the National Institute of Maritime, Port and Aviation Technology (Institute Regulations No. 16, April 1, 2016; hereinafter referred to as the "Internal Audit Regulations").

(2) The person appointed in accordance with Article 4, paragraph 2 of the Internal Audit Regulations shall be in charge of conducting auditing.

(3) In order to verify the appropriate management of Retained Personal Information, etc., the person responsible for auditing shall conduct audits (including external audits; the same shall apply

hereinafter) regarding the status of the management of Retained Personal Information, etc. at the Institute, including the status of the measures prescribed in Chapters 2 through 9, on a regular basis and as necessary, and shall report the results to the General Protection Manager.

(4) The Protection Manager shall inspect the recording media, processing routes, storage methods, etc. of Retained Personal Information, etc. in each section, office, etc. on a regular basis and as needed, and report the results to the General Protection Manager when deemed necessary.

(5) Based on the results of audits or inspections, etc., the General Protection Manager, the Protection Manager, etc. shall evaluate the measures for the appropriate management of Retained Personal Information, etc. from the viewpoint of effectiveness, etc., and when they find it necessary, shall take measures such as reviewing the relevant measures.

(Inspection)

Article 35. The Protection Manager shall inspect the recording media, processing routes, storage methods, etc. of Retained Personal Information, etc. in each section, office, etc. on a regular basis and as needed, and report the results to the General Protection Manager when deemed necessary.

(Evaluation and Review)

Article 36. With regard to the measures for the appropriate management of Retained Personal Information, etc., the General Protection Manager, the Protection Manager, etc. shall evaluate the measures for the appropriate management of Retained Personal Information, etc. based on the results of audits or inspections, etc. from the viewpoint of effectiveness, etc., and when they find it necessary, shall take measures such as reviewing the relevant measures.

Chapter X-II Collaboration with Administrative Agencies

(Collaboration with Administrative Agencies)

Article 36-2. Based on the "Basic Policy on the Protection of Personal Information" (Cabinet decision of April 2, 2004), the Institute shall, in close collaboration with the Ministry of Land, Infrastructure, Transport and Tourism, which has jurisdiction over the Institute, appropriately manage the personal information in its possession.

Chapter XI Miscellaneous Provisions

(Miscellaneous Provisions)

Article 37. In addition to what is provided for in these Regulations, matters necessary for the protection of personal information held by the Institute may be specified separately.

Supplementary Provisions (June 30, 2017 Institute Regulations No. 60）

Supplementary Provisions (January 31, 2020 Institute Regulations No. 92）

These Regulations shall come into effect on February 1, 2020.