○ Guidelines on Management of Personal Information Held by Kobe University

(Enacted on March 17, 2005)
Revised on March 29, 2019

Part 1 Purpose

The purpose of these Guidelines is to identify matters that should be complied with pertaining to the management of retained personal information, etc. and retained specific personal information, etc., and ensure proper management of the information from the perspective of protecting personal information, anonymized personal information, and specific personal information based on Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003; hereinafter referred to as the "IAA Personal Information Protection Act"), Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 27 of 2013; hereinafter referred to as the "Numbers Act"), and the Guidelines on Measures for Proper Management of Personal Information Held by Incorporated Administrative Agencies, etc. (Notification No. 85 of the Director General of the Administrative Management Bureau, Ministry of Internal Affairs and Communications, September 14, 2004).

Part 2 Definitions

1 Definition of the term "Personal Information" as used in these Guidelines is as that stipulated in Article 2, paragraph 2 of the IAA Personal Information Protection Act.
2 Definition of the term "Individual Identification Code" as used in these Guidelines is as that stipulated in Article 2, paragraph 3 of the IAA Personal Information Protection Act.
3 Definition of the term "Special Care-required Personal Information" as used in these Guidelines is as that stipulated in Article 2, paragraph 4 of the IAA Personal Information Protection Act.
4 Definition of the term "Retained Personal Information" as used in these Guidelines is as that stipulated in Article 2, paragraph 5 of the IAA Personal Information Protection Act, and refers to information held by Kobe University (hereinafter referred to as "University").
5 Definition of the term "Anonymized Personal Information" as used in these Guidelines is as that stipulated in Article 2, paragraph 9 of the IAA Personal Information Protection Act.
6 Definition of the term "Individual Number" as used in these Guidelines is as that stipulated in Article 2, paragraph 5 of the Numbers Act.
7 Definition of the term "Specific Personal Information" as used in these Guidelines is as that stipulated in Article 2, paragraph 8 of the Numbers Act.
8 The term "Specific Personal Information, etc." as used in these Guidelines refers to Individual Numbers and Specific Personal Information.
9 The term "Retained Specific Personal Information, etc." as used in these Guidelines refers to Specific Personal Information, etc., and is information held by the University.

Part 3 Management System

1 Positions of General Personal Information Protection Manager (hereinafter referred to as "General Protection Manager"), Personal Information Protection Manager (hereinafter referred to as "Protection Manager"), Personal Information Protection Sharing Manager (hereinafter referred to as "Protection Sharing Manager"), and Personal Information Protection In-charge (hereinafter referred to as "Protection In-charge") shall be established at the University ensure proper management of Retained Personal Information, Anonymized Personal Information and Retained Specific Personal Information, etc. (hereinafter referred to as "Retained Personal Information, etc.").
2 A position of Auditor shall be established at the University to audit the state of management of Retained Personal Information, etc.

Part 4　Education and Training

1 The General Protection Manager shall work towards increasing the knowledge regarding handling of the Retained Personal Information, etc. as well as conducting any other education and training required to raise awareness regarding the protection of the Retained Personal Information, etc. among the staff engaged in handling of the Retained Personal Information, etc. (including temporary staff; hereinafter referred to as "Staff").
2 The General Protection Manager shall conduct education and training for the Protection Manager, the Protection Sharing Manager, and the Protection In-charge so as to ensure proper management of Retained Personal Information, etc., on university premises.
3 The Protection Manager shall put in place any measures necessary to ensure proper management of the Retained Personal Information, etc. such as giving the Staff an opportunity to participate in the education and training conducted by the General Protection Manager.

Part 5　Staff Responsibilities

The Staff must handle the Retained Personal Information, etc. in accordance with the purpose of the IAA Personal Information Protection Act and Numbers Act, in compliance with any other relevant laws, rules and regulations, and in accordance with any instructions given by the General Protection Manager, the Protection Manager, the Protection Sharing Manager, and the Protection In-charge.

Part 6　Access Restrictions

1 The Protection Manager (in the case of Administrative Organizations, the Protection Sharing Manager; the same applies hereinafter till Part 13) shall limit the scope and permissions of Staff who have right to access the Retained Personal Information, etc. to the minimum required level for said Staff to perform their duties in accordance with the confidentiality and contents of said Retained Personal Information, etc.
2 Staff who do not have access rights must not access the Retained Personal Information, etc.
3 The Staff who has access rights must not access the Retained Personal Information, etc. for purposes other than those in direct course to their work duties.

Part 7　Restrictions on Reproduction, etc.

Even when the Staff handles the Retained Personal Information, etc. in course of their work duties, the Protection Manager shall, in relation to conduct set forth below, limit instances in which said actions can be performed in accordance with the confidentiality of said Retained Personal Information, etc., such that these actions are performed upon the instructions of the Protection Manager.

(1) Reproduction of Retained Personal Information, etc.;
(2) Transmission of Retained Personal Information, etc.;
(3) Sending or taking media containing the Retained Personal Information, etc. off premises;
(4) Any other conduct which may hinder proper management of Retained Personal Information, etc.

Part 8　Correction of Errors, etc.

If any error is discovered in the contents of the Retained Personal Information, etc., the Staff shall make corrections in accordance with the instructions of the Protection Manager.

Part 9　Management of Media, etc.

The Staff shall store media containing the Retained Personal Information, etc. in the stipulated location, in accordance with the instructions of the Protection Manager, and store and lock the same in a fireproof safe, as and when deemed necessary.

Part 10 Disposal, etc.

If the Retained Personal Information, etc. or media containing the Retained Personal Information, etc. (including in-built media provided in devices or on servers) is no longer required, the Staff shall delete said information, or dispose of said media in a manner that will make it impossible for said Retained Personal Information, etc. to be restored or deciphered, in accordance with the instructions of the Protection Manager.

Part 11 Recording of Handling Status of Retained Personal Information, etc.

The Protection Manager shall maintain a register in accordance with the confidentiality of Retained Personal Information, etc., in which they shall record the usage and storage status of said Retained Person Information, etc.

Part 12 Provision of Retained Personal Information, etc.

1 When providing the Retained Personal Information to a person other than those affiliated with administrative organs or incorporated administrative agencies pursuant to the provisions of Article 9, paragraph 2, items (3) and (4) of the IAA Personal Information Protection Act, as a general rule, the Protection Manager shall exchange documents concerning the purpose of usage of said information by the party receiving said information, the legal basis of the duties for which said information will be used, the scope and items to be recorded, and the form of usage, etc.
2 When providing the Retained Personal Information to a person other than those affiliated with administrative organs or incorporated administrative agencies pursuant to the provisions in Article 9, paragraph 2, items (3) and (4) of the IAA Personal Information Protection Act, if safety control measures are required and are deemed as necessary, the Protection Manager shall put in measures such as performing on-site inspections prior to, or at any time during, the provision of said information so as to check the status of these measures, as well as recording the results of these measures, and requesting improvements to these measures.
3 The Protection Manager shall put in place the measures prescribed in items 1 and 2 if it is deemed necessary to provide Retained Personal Information to an administrative organ or incorporated administrative agency pursuant to the provisions of Article 9, paragraph 2, item (3) of the IAA Personal Information Protection Act.
4 The Protection Manager shall put in place the measures prescribed in items 1 and 2 if it is deemed necessary to provide the Anonymized Personal Information pursuant to the provisions of Article 44-2 of the IAA Personal Information Protection Act.
5 The Protection Manager must not provide the Retained Specific Personal Information, etc. except when such provision of said information falls under any of the items prescribed in Article 19 of the Numbers Act.

Part 13 Task Outsourcing, etc.

1 When tasks that involve handling of the Retained Personal Information, etc. are outsourced outside, necessary measures must be put in place to prevent appointment of persons who do not have the capability to provide proper management of the Retained Personal Information, etc. Further, in addition to clearly stating the items set forth below in the contract, the contract shall confirm in writing the management and enforcement systems for the responsible personnel and workers at the outsourced company, and any necessary items relating to the inspection of the management status of the Retained Personal Information, etc.
   (1) Obligations to maintain confidentiality of the Retained Personal Information, etc. and prohibit utilization for unintended purposes;

(2) Matters relating to the subcontracting conditions, including restrictions on subcontracting (including cases where the subcontractee is a subsidiary company (a subsidiary as stipulated in provisions of Article 2, paragraph 1, item (3) of the Companies Act (Act No. 86 of 2005)). Same in this item and item (4)) and pre-approval;
(3) Matters relating to restrictions on reproduction of the Retained Personal Information, etc.;
(4) Matters relating to measures in the Instance(s) of leakage, etc. of the Retained Personal Information, etc.;
(5) Matters relating to the deletion or disposal of the Retained Personal Information, etc. and return of any media after the outsourcing work is completed;
(6) Termination of contract in the event of a breach of terms, liabilities, and other necessary matters.

2 When the tasks that involve the handling of Retained Specific Personal Information, etc. are outsourced outside, in addition to those stipulated in item 1, checks shall be put in place to confirm that the measures put in place by the subcontractee are equivalent to the security control measures that the University is obliged put in place as per the Numbers Act, and the items set forth below shall also be specified clearly in the contract.
(1) Matters relating to the scope, supervision, and education and training of personnel who handle Retained Specific Personal Information, etc.;
(2) Obligations to report on compliance with the contract contents.

3 When the tasks that involve handling of the Retained Personal Information, etc. are outsourced outside, as a rule, the status of the management system, enforcement system, and the management of Personal Information at the contractee shall be checked at least once a year via on-site inspection in accordance with the confidentiality of Retained Personal Information, etc., and level and contents thereof involved in the outsourced work.

4 When a contractee to whom tasks are outsourced re-outsources tasks that involve handling of the Retained Personal Information, etc., in addition to having the contractee put in place measures prescribed in item 1 (including measures prescribed in item 2 if the work involving handling of Retained Specific Personal Information, etc. is subcontracted), measures prescribed in item 3 must also be implemented via the contractee or by the contractee itself. The same shall be applicable when the secondary subcontractee re-outsources tasks that involve handling of the Retained Personal Information, etc.

5 If the tasks that involve handling of the Retained Personal Information, etc. is to be performed by temporary personnel, matters relating to handling of the Personal Information, including obligations to maintain confidentiality, shall be specified clearly in the temporary personnel's contract.

6 When providing the Retained Personal Information, or outsourcing tasks that involve handling of said information, consideration should be given to the confidentiality of Retained Personal Information, contents of the work being outsourced, and the intended use of said information by the party being provided with said information from the perspective of reducing risk of damages due to leakages and the like, and if necessary, anonymization measures must be put in place such as swapping names with numbers.

Part 14 Reporting of Incident(s) and Measures to Prevent Recurrence

1 Any person who knows of any occurrence, or risk of occurrence, of any instances (hereinafter simply referred to as "Incident(s)") that are problematic from the perspective of ensuring security, such as the occurrence of leakage, loss, or damage to Retained Personal Information, etc., shall immediately report said Incident(s) to the Protection Manager who manages said Retained Personal Information, etc.

2 The Protection Manager shall promptly put in place any necessary measures to prevent the spreading of any damages, or to ensure recovery therefrom.

3 The Protection Manager shall investigate how the Incident(s) occurred, and the extent of any damage caused thereby, and then report the findings to the General Protection Manager. However, should the Incident(s) be deemed particularly serious, said Incident(s) should be reported immediately to the General Protection Manager.

4 When receiving a report pursuant to the provisions stipulated in item 3, the General Protection Manager shall promptly report the details, background, and extent of damage of said Incident(s) to the President of the University depending on the details of said Incident(s).
5 The General Protection Manager shall promptly provide information concerning the details, background, and extent of damage of the concerned Incident(s) to the Ministry of Education, Culture, Sports, Science and Technology of Japan (MEXT) depending on the details of the Incident(s).
6 The Protection Manager shall analyze the cause(s) of the Incident(s) and put in place any necessary measures to prevent recurrence.

Part 15 Public Disclosure, etc.

1 Depending on the details and impact of the Incident(s), the General Protection Manager shall publicly announce the relevant facts and the measures put in place to prevent recurrence, and take further measures regarding any person(s) affected by said Incident(s) (person(s) refers to specific individuals identified by Retained Personal Information, etc.).
2 For Incidents(s) that are to be disclosed publicly, information on the details, background, and extent of damage of said Incident(s) shall be provided promptly to Administrative Management Bureau of Ministry of Internal Affairs and Communications.

Part 16 Audit

The Auditor shall, from time to time, perform audits on the status of the management of the Retained Personal Information, etc. in the University, including the status of the measures stipulated in Article 3 through Article 15 to verify proper management of the Retained Personal Information, and report those results to the General Protection Manager.

Part 17 Inspection

The Protection Manager shall periodically, and, as and when required, inspect any media on which the Retained Personal Information, etc. for which they are responsible is recorded as well as processing channels and storage methods, and, report those results to the General Protection Manager, if deemed necessary.

Part 18 Evaluation and Revision

The General Protection Manager and the Protection Manager shall evaluate any measures put in place to ensure proper management of the Retained Personal Information, etc. from the viewpoint of effectiveness based upon the results of audits or inspections, and, enact revisions or any other appropriate measures, if deemed necessary.

Part 19 Kobe University Information Security Policy

Handling of the information system by the University prescribed in the provisions of "6. Ensuring Security of Information Systems, etc." and "7. Security Management of Information System Office" of the Guidelines on Measures for Proper Management of Personal Information Held by Incorporated Administrative Agencies, etc. and other shall be as prescribed in Kobe University Information Security Policy.

Part 20 Cooperation with Ministry of Education, Culture, Sports, Science and Technology of Japan (MEXT)

The General Protection Manager shall maintain close cooperation with MEXT and perform proper management of Retained Personal Information, etc., based on "Basic Policy on the Protection of Personal Information" (approved by cabinet on April 2, 2004) 4.

Part 21 Other

Any necessary matters relating to the management of the Retained Personal Information, etc. pursuant to the provisions of these Guidelines shall be specified separately.

Supplementary Provisions (March 23, 2015)

These Guidelines come into effect from April 1, 2015.

Supplementary Provisions (March 29, 2019)

These Guidelines come into effect from April 1, 2019.