* The Japanese version is the authoritative version, and this English translation is intended for reference purposes only. Should any discrepancies or doubts arise between the two versions, the Japanese version will prevail.

The University of Tokyo Rules for the Handling of Personal Information, etc.

Established on March 17, 2005
Board Resolution
The University of Tokyo Rules No. 333

Chapter 1. General Provisions

(Purpose)

Article 1.

The purpose of these Rules is to protect the rights and interests of individuals while ensuring the proper and smooth operation of affairs and businesses of The University of Tokyo (hereinafter referred to as the "University"), in view of a significant increase in the use of personal information and other information relating to an individual at the University.

(Definitions)

Article 2.

The definitions of the terms used in these Rules shall be governed by the Act on the Protection of Personal Information (Act No. 57 of 2003; hereinafter referred to as the " Personal Information Protection Act") and the 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 other relevant laws and regulations.

Chapter 2. Management System for Personal Information etc.

(Senior Protection Manager)

Article 3.

1. One senior protection manager shall be appointed at the University, and an executive staff designated by the president shall serve as the senior protection manager.

2. The senior protection manager shall supervise affairs related to the proper handling of information defin(r)-6( )5(i)14(n)9(f)12

(3) Formulation, revision or abolition of these Rules and other rules and regulations concerning the handling of personal information, etc. at the University

(4) Guidance, advice and supervision with regards to Paragraph 2, Items 2, 4 and 6 of Article 4 at each Faculty/Graduate School stipulated in Paragraph 1 of the same article

(5) Response to reports and consultations from the Organization Senior Protection Managers

(6) In addition to what is listed in the preceding items, services provided for in the rules and regulations concerning the handling of personal information, etc. at the University.

4. The senior protection manger may investigate each organization when it is deemed necessary for the management of personal information, etc.

5. The senior protection manager shall organize the general protection management committee and represent it as its chairperson. In such case, the general protection management committee shall be deemed to be in charge of the duties set forth in the preceding two paragraphs.

6. The senior protection manager shall provide for the matters necessary concerning the operation of the general protection management committee.

(Organization Senior Protection Managers)

Article 4.

1. One organization senior protection manager shall be appointed at each organization or any other division (i.e. university academic organizations, university library systems, the University of Tokyo Archives, the university joint education and research institutes, research institutions and Tokyo College established at the University of Tokyo Institutes for Advanced Study (UTIAS), the interdisciplinary research institutes, the national joint-use institutes, the collaborative research organizations, the Secondary School attached to the Faculty of Education, the University of Tokyo Hospital, Research Hospital, Institute of Medical Science and divisions; the same shall apply hereinafter), and heads of the respective organizations or other divisions or substitute persons (general managers and the manager of internal audit group in the case of divisions) shall serve as organization senior protection managers.

2. Organization senior protection managers shall take charge of ensuring the proper management of the personal information, etc. at each organization or any other divisions, and shall be in charge of the following duties.

(1) Establish a system for the management of personal information, etc. in the organizations or other divisions

(2) Formulation, revision and abolition of the detailed regulations of the relevant organization or division pertaining to these rules

(3) Appointment and supervision of protection managers

(4) Understanding and supervision of the status of the management of personal information, etc. in the relevant organization or division

(5) Reporting and consultation on necessary matters concerning the proper management of personal information, etc. to the senior protection manager

(6) In addition to what is listed in the preceding items, services provided for in the rules and regulations concerning the handling of personal information, etc. at the University.

3. The organization senior protection manager may, conduct necessary investigation concerning the management of personal information, etc. in their relevant organization or division if deemed necessary.

4. When multiple organizations or divisions are involved in the handling of personal information, etc., the organization senior protection managers of each organization or division shall be responsible for the handling of personal information, etc. in collaboration with each other and shall be jointly responsible under Paragraph 2.

(Protection Managers)

Article 5.

1. One or more protection managers shall be appointed at each organization or division designated by the relevant organization senior protection manager.

2. Protection managers shall assist the organization senior protection managers and shall be in charge of the following duties with regards to the proper management of personal information, [redacted] to the relevant organizations or divisions.

(1) Appointment and supervision of protection officers and administration officers

(2) Reporting and consulting on necessary matters concerning the management of personal information, etc. to the organization senior protection manager

(3) In addition to what is listed in the preceding items, the services provided for in the rules and regulations concerning the handling of personal information, etc [redacted] iversity.

3. When handling personal information, etc. using an information system, the prot [redacted] nager shall be in charge while cooperating with the manager of the information system.

4. When multiple organizations or divisions are involved in the handling of perso [redacted] tion, etc., the protection manager of each organization or division shall assist the organization s [redacted] ction manager of the organization or division to which they are affiliated.

(Protection Officers)

Article 6.

1. One or more protection officers shall be appointed by the relevant protection m [redacted] ach organization or division.

2. The protection officers shall assist protection managers and shall be in charge o [redacted] wing duties with regards to the proper management of the Personal Information, etc. at each organi [redacted] ivision.

(1) General affairs concerning the management of personal informa [redacted] xcluding the Individual Number set forth in Article 2, Paragraph 5 of the Numbers act and specific personal information set forth in

(3) In addition to what is listed in the preceding items, the services provided for in the rules and regulations concerning the handling of personal information, etc. at the University.

(Administration Officers)

Article 7.

1. Protection managers shall appoint one or more staff members (hereinafter referred to as the "administration officer") who handle specific personal information, etc.

2. Protection managers shall specify the extent to which specific personal information, etc. is to be handled by each administration officer.

(Establishment of Systems for Specific Personal Information, etc.)

Article 8.

Protection managers shall establish the following systems for specific personal information, etc.:

(1) a communication system that allows an administration officer, who has become aware of facts relating to the breach (or signs of the occurrence of a breach) of the provisions of related laws, regulations, rules and the like, to report the matter to the protection manager

(2) a communication system that allows executive, academic and administrative staff members (including dispatched workers; hereinafter referred to as "academic and administrative staff"), who have become aware of the occurrence or signs of occurrences of incidents such as leaks, loss or damage of specific personal information, etc. (hereinafter referred to as "leakage, etc."), to report to the protection manager

(3) clarification of the allocation of duties and responsibilities of the respective organizations where specific personal information, etc. is handled by multiple departments, and

(4) a response system when becoming aware of the occurrence or sign of incidents such as leakage, etc. of specific personal information, etc.

(Organizations, etc. Pertaining to Disclosure Requests)

Article 9.

The University of Tokyo Information Disclosure Committee shall be entrusted with disclosures etc. of personal information at the Univ8(l)14(l)-41 0 0 3p 0 595.4 841.8 r/495.4(o)8(i)1 0 0 1 127.65 306.88 Tm0 g0 G[(e)-8(t)14(c)-8(.)]TJETq

3.

other divisions including the granting of opportunities to participate in the education and training provided by the senior protection manager.

Chapter 5. Responsibilities of Academic and Administrative Staff

Article 16.

1. Academic and administrative staff must handle personal information, etc. in conformity with the purport of the Incorporated Administrative Agencies Personal Information Protection Act and the Numbers Act, and in compliance with the provisions of related laws, regulations, rules and the like, as well as the instructions of the senior protection manager, organization senior protection managers, protection managers, protection officers and administration officers.

Article 17.

Academic and administrative staff shall not, without due cause, inform other of the contents of personal information, etc. they have come to know in the course of performing their duties, or use it for unjust purposes.

Chapter 6. Handling of Personal Information, etc.

(Specification of the Purpose of Use)

Article 18.

1. When handle personal information, academic and administrative staff shall specify the purpose of use (hereinafter referred to as the "Purpose of Use") only in the cases where it is necessary to perform affairs handling the said personal information.
2. Academic and administrative staff shall not change the purpose of use beyond the scope that is reasonably considered to be related to the purpose of use before the change.

(Restrictions from the Purpose of Use)

Article 19.

No academic or administrative staff shall handle personal information beyond the scope necessary for achieving the purpose of use specified pursuant to the provisions of the preceding article, except in the following cases.

(1) In accordance with laws and regulations
(2) Cases in which the provision of personal information is necessary for the protection of life, body or property of an individual, and in which it is difficult to obtain the consent of the individual
(3) Cases in which the provision of personal information is necessary to improve public health or promote the sound growth of children, and in which it is difficult to obtain the consent of the individual
(4) Cases in which the handling of personal information is necessary to cooperate with a state organization, local government or an individual or business operator entrusted by either of the

(Prohibition of Improper Use)

Article 21.

Academic and administrative staff shall not use the personal information in a manner that encourages or is likely to induce illegal or unjust acts.

(Appropriate Acquisition of Information)

Article 22.

1. Academic and administrative staff shall not obtain personal information by deception or other wrongful means.

2. No academic or administrative staff shall acquire personal information requiring consideration without obtaining the prior consent of the individual, except in the following cases.

(1) In accordance with laws and regulations

(2) Where the provision of personal information is necessary for the protection of the life, body or property of an individual and where it is difficult to obtain the consent of the person

(3) Where the provision of personal information is specially necessary for improving public health or promoting the sound growth of children and where it is difficult to obtain the consent of the person

(4) Where the handling of personal information is necessary for cooperating with a state organization, a local government or an individual or an individual or business operator entrusted by either of the former two in executing the affairs prescribed by laws and regulations, and in which obtaining the consent of the individual would likely impede the execution of the affairs concerned

(5) When it is necessary to handle said personal information requiring consideration for academic research purposes (including cases where part of the purpose of handling the said personal information requiring consideration is for academic research purposes, and excluding cases where it is likely to infringe the rights and interests of the individuals)

(6) Where the personal information requiring consideration is to be obtained from an academic research institution etc., and where the said personal information requiring consideration is necessary for academic research purposes (including cases where part of the purpose of handling the said personal information requiring consideration is for academic research purposes, and excluding cases where it is likely to infringe the rights and interests of the individuals) (limited to cases where the said academic research institution, etc. conducts academic research jointly with the University.)

(7) Where the personal information requiring consideration is disclosed to the extent permitted under the law by the individual, national organization, local government, academic research institution, etc., press organization, person who engages commercially in writings, religious organization, political organization, foreign government, foreign governmental organization, foreign local government or an international organization, or a person who engages commercially in academic

research organization, etc., a press organization, a person who engages commercially in writings, religious organization or political organization in a foreign country

(8) Where the person obtains the personal information that is obviously necessary for consideration from viewing the individual or by taking a photograph of the individual

(9) In the cases listed in each item of Article 29, Paragraph 2 (including cases where it is applied by replacing the terms pursuant to the provision of Article 35, Paragraph 6 and the cases where it is applied by replacing the terms pursuant to Article 36, paragraph 2) when the personal information requiring consideration is the personal data provided.

(Ensuring Accuracy)

Article 23.

1. Academic and administrative staff shall endeavor to keep personal information accurate and up-to-date within the scope necessary for achieving the purpose of use, and endeavor to delete said personal information without delay when it is no longer required.
2. In the event of any errors are found in the contents of the personal information, academic and administrative staff shall make corrections etc. in accordance with the instructions of the protection officers.
3. Academic and administrative staff shall delete personal data or dispose of the media on which the personal data is stored on in a manner that makes it impossible for the personal data to be recovered or read, in accordance with the instructions of the protection manager, once the personal data or the media on which it is stored is no longer required.

(Security Control Measures)

Article 24.

1. The organization senior protection manager shall take necessary and appropriate measures to prevent the leakage, etc. of personal data being handled and for the safe management of personal data.
2. The organization senior protection manager shall establish necessary and appropriate measures for the safe management of the personal data and shall ensure that academic and administrative staff observe them.

(Contracting Out the Business etc.)

Article 25.

1. When an organization senior manager contracts out the handling of personal data, in whole or in part, they shall conduct necessary and appropriate supervision of the contracted party in order to ensure the safe management of the entrusted personal data.
2. When contracting out the handling of personal data, the protection managers shall take necessary measures, such as confirming at the time of selection, the management capability of personal data, specify the following items in the contract, and confirm in writing the necessary matters such as the status of the management of managers and employees, management of the implementation system and personal information at the contracted party.

(1) Measures equivalent to the safety management measures taken by the University shall be taken

(2) Obligations to maintain the confidentiality of personal data and prohibit the use of the personal data for other purposes

(3) Matters concerning the conditions pertaining to sub-contracting (including cases where the sub-contractor is a subsidiary of the contractor (meaning a subsidiary as prescribed in Article 2, Paragraph 1, Item 3 of the Companies Act (Act No. 86 of 2005), the same shall apply hereinafter)), such as restrictions or preapproval, etc.

(4) Matters concerning restrictions on reproduction, copying etc. of the personal data

(5)

(Restriction on Reproduction, etc.)

Article 27.

With respect to the following acts, protection managers shall, according to the nature of the personal data, including

(7) Where the said third party is an academic research institution, etc. and it is necessary for said third party to handle the personal data for academic research purposes (including cases where part of the purpose of providing the personal data is for academic research purposes and excluding cases where there is a risk of unreasonable infringement of the rights and interests of the individual).

2. The person who receives such personal data shall not fall under the category of a third party with regards to the application of the provisions of the preceding paragraph in the following cases.

(1) Where the personal

Information Protection Committee, measures to be taken by the third party for the protection of personal information and other information that will be helpful for the individual in question.
3. In the event that personal data is provided to a third party in a foreign country (limited to a person who has a system provided for in Paragraph 1, Item (3)), the academic or administrative staff shall, pursuant to the provisions of the Rules of the Personal Information Committee, take the necessary measures to ensure the continuous implementation of the appropriate measures by the third party, and at the request of the individual, provide the person with information on the necessary measures.

(Preparation, etc. of Records Pertaining to Provision to a Third Party)
Article 31.
1. When the University provides personal data to a third party, academic and administrative staff shall, pursuant to the provisions of the Rules of the Personal Information Protection Committee, prepare records concerning the date when the personal data was provided, the name of the third party, and any other matters specified by the Rules of the Personal Information Protection Committee. Provided, however, that this shall not apply where the provision of such personal data falls under any of the items of Article 29, Paragraph 1 or

(2) The name and address of the third party and, in the case of a corporation, the name of its representative.

(3)

to third parties, except in cases based on laws and regulations and pursuant to the Rules of the Personal Information Protection Committee, publicize in advance the items of personal information contained in the anonymized processing information to be provided to third parties and the method of provision thereof, and clearly indicate to said third parties that the information pertaining to said provision is anonymized processing information.
2. Academic and administrative staff shall not, when handling anonymized processing information, except in cases based on laws and regulations, acquire descriptions, etc. deleted from relevant personal information, personal identification codes or information concerning the method of processing, or collate said anonymized processing information with other information in order to identify the individual concerned pertaining to the personal information used in preparing the said anonymized processing information.
3. Academic and administrative staff shall take necessary measures for the proper management of the anonymized processing information in accordance with the standards set forth in the Rules of the Personal Information Protection Committee as necessary to prevent leakage of the anonymized processing information.
4. In the event that the University outsources the handling of anonymized processing information (including two or more stages of outsourcing), academic and administrative staff shall entrust the contracted party to comply with the provisions of the preceding two paragraphs.

(Preparation and Provision of Anonymized Processing Information of Administrative Agencies, etc.)
Article 38.
1. The senior protection manager may prepare anonymized processing information of administrative agencies, etc. (limited to information that constitutes and anonymized processing information file of administrative agencies, etc.) in accordance with the provisions of Chapter 5, Section 5 of the Personal Information Protection Act.
2. The senior protection manager shall establish rules concerning the handling of anonymized processing information of administrative agencies, etc.

(Preparation and Publication of Personal Information File Register)
Article 39.
1. The organization senior protection managers shall report to the senior protection manager the contents provided separately as necessary matters for the preparation of personal information file register with regards to the handling of personal information in each organization.
2. The senior protection manager shall prepare and publish the personal information file register based on the reports pursuant to the provisions of Paragraph 1.

Chapter 7. Ensuring Security of Information Systems, etc.

(Access Control)
Article 40.
Protection managers shall take measures necessary for access control, including the setting up of functions to identify the level of authority (hereinafter referred to as the "authentication functions") using passwords and other

(Preventing Theft of Terminals, etc.)

Article 52

Protection managers shall take necessary measures for the prevention of theft or loss of terminals including fixing terminals or locking offices.

Article 53.

Unless a protection manager deems it necessary, academic and administrative staff must not take any internal terminals to areas outside the organization or bring in any terminals from outside of the organization.

(Preventing Browsing by Third Party)

Article 54.

When using terminals, academic and administrative staff shall take necessary measures to ensure that personal information, etc. cannot be browsed by a third party, including ensuring that they log off from the information systems depending as and when necessary, depending on the conditions of use.

(Verification of Entered Information, etc.)

Article 55.

Academic and administrative staff shall, according to the importance of the personal information, etc. handled using the information systems, shall compare and verify source documents and the entered details, confirm details of such personal information, etc. before and after handling, verify the content thereof using existing retained personal information, etc.

Chapter 8. Managing the Security of the Information System Offices, etc.

(Controlling Entrance and Exit)

Article 58.

Protection managers shall specify the persons authorized to enter an office where devices (including the main server that handles

the

Chapter 9. Handling of Specific Personal Information, etc.

(Restrictions on the Use of Individual Numbers)

Article 63.

Protection managers shall take measures to limit the use of individual numbers to the affairs restricted in advance by the Numbering Act.

(Restrictions on Requests for Provision of Specific Personal Information, etc.)

Article 64.

Academic and administrative staff shall not request the provision of individual numbers except in cases necessary for processing affairs related to individual numbers or other cases specified by the Numbers Act.

(Restrictions on the Creation of Specific Personal Information Files)

Article 65.

Academic and administrative staff shall not create specific personal information files, except in cases necessary for processing affairs related to individual numbers or other cases specified by the Numbers Act.

(Restrictions on Collection, Storage and Provision of Specific Personal Information, etc.

Article 66.

Academic and administrative staff shall not collect, retain or provide personal information, including the Individual Numbers of others, except in cases that fall under any of the items of Article 19 of the Numbers Act.

(Clarification of Areas for Han

2. With regards to the Individual Numbers, these Rules shall apply to the Individual Number even after the death of the individual concerned, and the person in charge of handling the affairs shall take the necessary measures.

Chapter 10. Response to Security Problems

(Incident Reporting and Measures to Prevent Recurrence)

Article 74.

When becoming aware of an incident that would become a problem in terms of security, such as cases where one becomes aware of the occurrence or sign of an occurrence of incident of leakage, etc. of personal information, etc. and where being aware of a fact or signs pointing to facts that an affairs handling officer is in breach of the provisions of related laws and regulations and rules, academic and administrative staff

Article 79.

Protection managers shall, under the supervision of the organization senior managers, analyze the causes leading to the incident and take measures necessary to prevent the recurrence thereof.

(Publication, etc.)

Article 80.

1. The senior protection manager shall, according to the nature, impact and other factors of an incident, take measures including the publication of facts and

Chapter 12. Cooperation with Administrative Agencies

Article 84.

The University shall properly manage the personal information held by it based on the "Basic Policy on the Protection of Personal Information" (Cabinet Decision 4 of April 2, 2004), by closely cooperating with relevant ministries and agencies.

Supplementary Provisions

These Rules shall come into force as from April 1, 2005.

Supplementary Provisions

These Rules shall come into force as from January 1, 2011.

Supplementary Provisions

These Rules shall come into force as from April 1, 2015.

Supplementary Provisions

These Rules shall come into force as from November 1, 2015.

Supplementary Provisions

These Rules shall come into force as from April 1, 2016.

Supplementary Provisions

These Rules shall come into force as from December 1, 2017.

Supplementary Provisions

These Rules shall come into force as from April 1, 2018.

Supplementary Provisions

1. These Rules shall come into force as from April 1, 2019.
2. For the purpose of the provisions of Article 4 during the date of enforcement of these Rules to March 31, 2021, the “The University of Tokyo Archives” in the same article shall be deemed to be replaced with “The University of Tokyo Archives, University-wide Centers listed in the Supplementary Provisions of the Regulations for the partial revision of the University of Tokyo Rules on Basic Organization (The University of Tokyo Rules No. 3, April 26, 2018).

Supplementary Provisions

These Rules shall come into force as from March 1, 2020.

Supplementary Provisions

These Rules shall come into force as from April 1, 2021.

Supplementary Provisions

These Rules shall come into force as from April 1, 2022.