National Yang Ming Chiao Tung University Enforcement Rules of Personal Data Protection

Passed on September 28, 2021, at the 1st meeting of the Information Security and Personal Data Protection Committee for the 2021–2022 academic year

1. To regulate the collection, processing, and use of personal data; promote the reasonable use of personal data; and prevent the theft, tampering, damage, loss, and leakage of personal data, National Yang Ming Chiao Tung University (NYCU) hereby establishes the National Yang Ming Chiao Tung University Enforcement Rules of Personal Data Protection. The enforcement rules were formulated in accordance with NYCU's Regulations Governing Information Security and Personal Information Protection.
2. Terminology definitions:
   A. Personal data: Information such as the person's name, date of birth, ID Card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, sex life information, health examination results, criminal records, contact information, financial conditions, and social activities that can be used to directly or indirectly identify the individual.
   B. Personal data files: Person data file are files stored in paper or electronic format. Electronic personal data files include files and information system database files stored in personal computers.
3. All units shall assign staff members to serve as personal data protection staff, who are responsible for managing and compiling the personal data files of the unit. These files may be subject to subsequent audits.
4. Personal data file content that is inspected:
   A. At least once a year, all units shall perform personal data inspections, personal data updates, and risk assessments by using the personal data inspection checklist provided by the IT Service Center.
   B. Personal data file inspections are conducted to identify high-risk personal data. Such data may include:
      (1) Special personal data as defined in the Personal Data Protection Act
      (2) Personal financial information
      (3) ID Card number
      (4) Information that reveals an individual's vulnerable status
      (5) Detailed descriptions of personal characteristics
      (6) Information that negatively affects an individual
   C. Personal data file inspections include inspections of items such as data usage and data flow.
   D. Personal data file risk assessments evaluate the importance of reference materials and examine and assess the security risks of current data and the risks of such data being used in acts that violate the law.
5. During the collection, processing, or use of personal data, appropriate notification methods shall be applied unless otherwise stipulated by the law. When personal data are used for purposes other than that for which they were obtained, a check shall be conducted to determine whether the written consent of the parties involved for such use has been obtained, whether such use improves public welfare, or whether such use benefits the rights and interests of the parties involved. The following is a list of the types of information that shall be conveyed to the parties involved:
   A. Names of schools or institutions

B. Purpose of information collection
C. Personal data type
D. The time, locations, targets, and methods pertaining to the use of personal data
E. The parties involved are exercising their rights to collect, process, or use personal data in accordance with Article 3 of the Personal Data Protection Act.
F. The possible infringement of the parties' rights and interests if they choose not to provide personal data.

6. The personal data (e.g., medical records, healthcare data, genetic data, sex life information, health examination results, and criminal records) of an individual that can be used to directly or indirectly identify the individual shall not be collected and processed unless the consent of the individual has been obtained or the law stipulates otherwise. If the personal data of an individual are used for academic purposes, the data shall be properly handled such that they cannot be used to identify the individual.
7. Units that use information systems or cloud information services (e.g., questionnaire survey services that use Google Forms and Microsoft Forms) for administrative purposes that involve the collection of personal data shall pay attention to the following:
   A. Data collection minimization: Only appropriate, relevant, and necessary personal data that meet the established objectives for data collection can be collected. During the processing and use of such data, they may not be used outside the scope of the established objectives, and data processing and use shall correspond to the objectives of data collection.
   B. Access control: Attention shall be paid to file access authorization settings, and the principle of least privilege shall be adopted. That is, a user is only granted the authorizations necessary for completing their assigned tasks and completing objectives.
   C. A user who uses cloud information services shall read the setting content carefully and refrain from jointly editing personal data files with another individual. Additionally, a user shall refrain from granting to another individual the authorization to view the responses of other individuals (e.g., they shall not check the "Show summary charts and responses of others" box) to prevent other users from accessing user data, thereby causing a personal data leakage. Prior to the release of any information services, relevant settings shall be checked, operational tests shall be performed.
   D. Transmission confidentiality: Internet transmission shall be encrypted using HTTPS and TLS version 1.2 or newer.
   E. Data storage security: During the collection of personal data or other sensitive personal data as defined in Article 6 of the Personal Data Protection Act, such data shall be stored in an encrypted form.
   F. To avoid personal data leakage, a personal data storage period shall be set and collected personal data shall be deleted or destroyed at the end of the storage period or when the related operations have been completed.
8. All units shall assign specific staff members to manage and maintain the personal data stored in shared computers or automated equipment.
9. For non-routine operations or cross-unit data circulations that are being performed for the first time, a unit shall fill out the Data Usage Application form.
10. For the saving, transmission, and backing up of personal data that require encryption, appropriate encryption mechanisms should be adopted during the collection, processing, or use of such data. For information that is intended for the parties involved, care shall be taken to ensure that the files containing such information do not contain the personal data of any uninvolved parties and that the information is provided to the correct data

recipients. Hence, provision of information to unrelated individuals can be avoided.

11. If a written document or website announcement made by a unit contains the ID Card number of an individuals, the last 4 digits of the number must be concealed.
12. Personnel who process personal data shall use the email system provided by NYCU to transmit and encrypt these personal data files. They are prohibited from transmitting or disclosing personal data files through tools other than those provided by NYCU (e.g., instant messaging software, external web-based electronic devices [e.g., Webmail], peer-to-peer [i.e., P2P] software, Tunnel-related tools, cloud storage tools [e.g., Dropbox], social networking sites, blogs, public forums, and other Internet forms).
13. A user shall destroy the personal data stored in media such as paper, floppy disks, magnetic tapes, CD-ROMs, microfilms, and integrated circuit chips when the media are disposed of or used for other purposes. The user shall also fill out the Personal Data Destruction Record or Personal Data Transfer Termination Record.
14. During the collection, processing, and use of personal data, a trustor shall specify in a procurement contract the monitoring, information-security clauses, confidentiality, and disposal clauses that pertain to breach of contract. Additionally, a trustor shall manage the authority of outsourced and external personnel to access information and introduce personal data management processes. After a period of entrustment, a trustor shall return the accessed personal data to NYCU and sign the Affidavit for the Return and Destruction of Personal Data.
15. Appropriate monitoring measures shall be taken during the collection, processing, and use of the personal data provided by a trustee:
    A. The scope, type, objective, and duration of collecting, processing, or using a trustee's personal data shall be determined.
    B. Appropriate security and maintenance measures shall be taken by a trustee.
    C. When a trustee is appointed for a re-entrustment, the appointed trustee shall be identified.
    D. When the Personal Data Protection Act or contractual terms have been violated or breached, a trustee shall take remedial measures to resolve the issues disclosed by a trustor.
    E. Issues not disclosed by a trustor to a trustee.
    F. When an entrustment relationship is terminated or rescinded, a trustee shall return the personal data of a trustor and delete the personal data that were stored.
16. Technical management measures:
    A. Authentication mechanisms (e.g., account names and passwords) should be applied to computers, related equipment, and systems. A password should contain both uppercase and lowercase English letters and numbers and at least 8 digits. A password must be changed regularly, and the effectiveness of the authentication mechanisms must also be tested regularly.
    B. Antivirus software must be installed on computers, and virus patterns must be updated in real time.
    C. A computer operating system shall be maintained and updated, and the necessity of updating application software shall be evaluated.
    D. Screensaver and password lock prompts shall display within 15 minutes when a computer is idle.
    E. No file sharing software shall be installed on computers that control user access.
    F. The usage status and personal data access status of information systems that process personal data shall be checked regularly.
    G. A unit shall implement the necessary access controls on the basis of its work content, work environments, the personal data type and quantity that are involved, and it shall

manage personal data storage media in appropriate locations and by applying the appropriate methods.

17. The following records should be maintained to allow for an inspection of personal data protection to be conducted:
    A. Personal data delivery and transmission records.
    B. Personal data accuracy records and revised records.
    C. Records of parties exercising their rights.
    D. Records of changes to the authority of affiliated personnel (i.e., adding, changing, or removing their authority).
    E. Records of personal data deletions, destructions, and transfers.
    F. Records detailing the prevention, reporting, and processing of personal data protection incidents.
    G. Records of backups and restoration tests.
18. All units shall follow internal audit schedules and fill out the personal data management internal audit checklist.
19. The staff of all units shall complete the relevant education and meet the training hour requirements imposed by the competent authority.
20. These enforcement rules are in effect after they are passed at the meeting of the Information Security and Personal Data Protection Committee; the same shall apply to any amendments hereto.