


Content

Title :	Operation Directions Governing the Interconnection of MyData 
Date :	2023.06.01
Legislative :	<ol style="list-style-type: none"><li>1. Promulgated by EXECUTIVE YUAN Order No.1101500560B on 15th, April 2021.</li><li>2. Amended and promulgated by EXECUTIVE YUAN Order No. 11230000781 on 30th, January 2023.</li><li>3. Amended and promulgated by EXECUTIVE YUAN Order No. 11230007161 on 1st, June 2023.</li></ol>
Content :	<p>I. These directions are put in place to facilitate the smooth operation of The Autonomous Use of Personally Related Data (MyData) Platform, a platform that uses personalized data to create customized services for users, and to ensure the security of information and personal privacy. The Autonomous Use of Personally Related Data (MyData) Platform, upon data subjects' consent, provides immediate and single-time download and access services of personalized data.</p> <p>II. The Autonomous Use of Personally Related Data (MyData) Platform is developed, operated, and managed by the Ministry of Digital Affairs (hereinafter the moda).</p> <p>III. Terms used in the this document are defined as follows:</p> <ul style="list-style-type: none"><li>(i) The Autonomous Use of Personally Related Data (MyData) Platform (hereinafter the "platform"), created by moda, is a platform that, upon identity verification and consent by a natural or legal person (hereinafter, a "data subject"), serves as an interface that allows for instantaneous and single-time download of a data subject's personalized data.</li><li>(ii) A "data provider" is an organization specified under Article IV that stores or retains a data subject's personalized data, connects to the platform, and makes the immediate and single-time transfer of personalized data upon a data subject's identity verification and consent either directly on the platform or via a recognized third-party identity verification agency.</li><li>(iii) A "service provider" is an organization specified under Article IV that has immediate and single-time access to personalized data, and that, upon the data subject's identity verification and consent processed either on the platform or via a recognized third-party identity verification agency, connects to the platform and provides value-added services to a data subject.</li></ul> <p>IV. The following organizations may apply to the moda for endorsement either as a data provider or a service provider:</p> <ul style="list-style-type: none"><li>(i) The Executive Yuan, and its subordinate authorities (agencies), and non-departmental public bodies oversaw under their supervision.</li><li>(ii) Yuans other than the Executive Yuan, their subordinate authorities (agencies), and non-departmental public bodies under their supervision.</li><li>(iii) Municipality, city and county governments, their subordinate authorities (agencies), and non-departmental public bodies under their supervision.</li><li>(iv) Colleges and universities that have obtained approval from the Ministry of Education.</li><li>(v) State-owned enterprises that have obtained approval from their respective competent authorities.</li><li>(vi) Financial institutions and peripheral entities under the jurisdiction of the Financial Supervisory Commission (hereinafter the FSC) that have obtained approval from the FSC.</li></ul>

(vii) Other non-government authorities (agencies) with plans in compliance with the Cyber Security Management Act and Personal Information Protection Act in place for the protection of cyber security and personal data, and that have obtained approval from its central government authority in charge of the industry concerned.

V. Organization applicants to the platform shall act in accordance with the preceding articles, and shall, as a general rule, apply on a per-service basis for approval, and the application process shall be conducted as follows:

(i) Application for connection:

1. Authorities (agencies) and non-departmental public bodies under Subparagraphs 1 to 3 of the preceding article shall fill out and submit the application form to the moda.

2. Colleges and universities specified under Subparagraph 4 of the preceding article shall fill out and submit the application form to the Ministry of Education for approval. Upon approval, the application shall be sent to the moda. The Ministry of Education shall notify the applicant should an approval is not granted.

3. State-owned enterprises specified under Subparagraph 5 of the preceding article shall fill out and submit the application form to their respective competent authorities. Upon approval by the competent authorities, the application shall be sent to the moda. Competent authorities shall notify the applicant should an approval is not granted.

4. Financial institutions and peripheral entities specified under Subparagraph 6 of the preceding article shall fill out and submit the application form to the FSC. Upon approval by the FSC, the application shall be sent to the moda. The FSC shall notify the applicant should an approval is not granted.

5. Non-government authorities (agencies) specified under subparagraph 7 of the preceding article shall fill out and submit the application form with cyber security and personal data protection plans that are in line with the Cyber Security Management Act and Personal Information Protection Act to its central government authority in charge of the industry concerned. Upon approval by the central government authority, the application shall be sent to the moda. The central government authority shall notify the applicant should an approval is not granted.

6. Applicants under Subparagraphs 1 to 3 of the preceding article will have their service objectives and contents, terms of service provided to data subjects, and data transferred via the interface reviewed by the moda.

7. Applicants under Subparagraphs 4 to 7 of the preceding article will have their service objectives and contents, terms of service provided to data subjects, and data transferred via the interface reviewed by the Ministry of Education, applicable competent authorities of state-owned enterprises, the FSC, or central government authorities in charge of the industry of non-government authorities (agencies).

(ii) Any changes or terminations shall be submitted through an application form for approval seven business days prior to the effective day, as per the provisions of preceding subparagraphs.

(iii) Providers that have their service terminated may file for reinstatement of service as per the procedures outlined in Subparagraph 1.

(iv) Forms to be used for application specified under the preceding three subparagraphs will be published by the moda on the platform in a separate announcement.

The moda will notify the applicant of the outcome of applications submitted by each applicant under preceding paragraphs.

VI. Organizations connected to the platform shall comply with the following provisions:

- (i) Data providers shall:
  - 1. Implement identity verification to ensure safe and secure use of data subjects' personalized data.
  - 2. Provide accurate personalized data to data subjects.
- (ii) Service providers shall:
  - 1. Collect only the required amount of the data subjects' personalized data and use the data in a manner that is in line with its said purpose at the time of collection.
  - 2. Ensure that data subjects are adequately informed of the terms of service prior to their consent to the downloading of their personalized data.
  - 3. Not claim ownership of data subjects' personalized data obtained via connection to the platform.
- (iii) In the event of a temporary suspension of connection to the platform for any reasons, an announcement shall be made seven business days prior to the planned effective date on the platform of the organization and shall be sent by email or by mail to be published by platform, except in the event of an emergency.

VII. Regulations and audits regarding information security:

- (i) Service providers shall conduct annual internal audits on its procedures of the collection, processing, and use of data subjects' data, with audit records shall be written and archived for at least two years. Service providers shall follow audits conducted by the moda, the Ministry of Education, competent authorities of state-owned enterprise, the FSC, or central government authorities in charge of the industry of non-government authorities (agencies). In cases where data providers have established longer archive periods, those rules shall take precedence.
- (ii) Service providers under Subparagraphs 4 to 6 of Article IV shall follow the audits from the Ministry of Education, competent authorities of state-owned enterprises, the FSC or a third-party agency recognized by the aforementioned authorities on service providers' compliance with the laws and regulations on the protection of information security and personal data and make necessary improvements.
- (iii) Service providers under Subparagraph 7 of Article IV shall implement cyber security and personal data protection plans which shall be subjected to audits from central government authorities in charge of the industry and its recognized third-party agencies on the compliance with laws and regulations on information security and personal data protection. Service providers shall make necessary improvements as laid out by the audits.
- (iv) Data providers and the service providers shall document transfers of data subjects' data, archive said documents for a minimum of two years, and follow audits conducted by the moda, the Ministry of Education, competent authorities of state-owned enterprises, the FSC or central government authorities in charge of the industry of non-government authorities (agencies). Matters that shall be included in the aforementioned documents include but are not limited to titles of the data transferred, time of transfers, recipients, data subjects' identity, and transfer outcomes. In cases where data providers or service providers have established longer archive periods, those rules shall take precedence.
- (v) Data providers and service providers shall make improvements or implement supplemental measures to rectify any errors detailed in audit reports prior to complete resolution of issues.
- (vi) In the event of an incident, such as personalized data inaccuracy or a security breach on the part of a data provider, the data provider shall be solely accountable, and shall handle the incidence in accordance with applicable laws and regulations. Services with the moda may be terminated under such circumstance.
- (vii) In the event of an incident, such as an unauthorized use of personalized data or a security breach on the part of a service provider, the service provider shall be solely accountable, and shall handle the incidence in accordance with applicable laws and

regulations. Services with the moda may terminated under such circumstance.

VIII. Data providers and service providers shall comply with the Cyber Security Management Act, the Personal Data Protection Act, and other applicable laws and regulations with regard to the protection of information security and personal data. Colleges and universities shall also comply with applicable regulations and directions of the Ministry of Education. State-owned enterprises shall also comply with applicable regulations and directions of their respective competent authorities. Financial institutions and peripheral entities under the jurisdiction of the FSC shall also comply with the applicable regulations and directions of the FSC. Other non-government authorities (agencies) shall also comply with the applicable regulations and direction of their central government authorities in charge of the industry concerned.

IX. Entities violating the provisions of these Implementation Directions are subject to termination of cooperation from the moda. Violators shall also be held liable by applicable laws and regulations.

X. The platform reserves the right to adjust, temporarily suspend, or terminate its services based on legal, technological, market-related and policy considerations. An announcement will be made on the platform seven business days before any prospective alteration, suspension, or termination of service, except in the event of an emergency.

---

Files : Operation Directions Governing the Interconnection of MyData (ver. 20230911).odt

---

Data Source : Ministry of Digital Affairs Laws and Regulations Retrieving System