

Regulations Governing Personal Data File Security Maintenance Plan and Processing Method for the Civil Aviation Enterprise

Full text promulgated by MOTC decree on October 16, 2014

Amendment to Articles 6 and 23 promulgated by MOTC decree on December 2, 2015

Renamed and amendment to Articles 2, 6, 12, and addition of Article 17-1, was promulgated by MOTC decree on June 1, 2022(The original title “Regulations Governing Personal Information File Security Maintenance Plan and Processing Method for the Civil Air Transport Enterprise”)

Article 1

These Regulations are prescribed pursuant to the provisions of Article 27 Paragraph 3 of the Personal Data Protection Act (hereinafter referred to as “the Act”).

Article 2

The Regulation is applicable to the following civil aviation enterprise:

1.A national and foreign civil air transport enterprise operating scheduled air transport service.

2.A general aviation enterprise operating international business charter service.

The national and foreign civil air transport enterprises and the general aviation enterprises mentioned in the preceding paragraph (hereinafter referred to as “the enterprise”) shall draw up plans for maintaining the security of personal data files (hereafter referred to as “the Plans”), for the purpose of ensuring the secure maintenance and management of personal data files, to prevent the theft, alteration, damage, destruction or disclosure of personal data.

The content of the Plans shall include the relevant organization and procedures prescribed in Articles 3 to 22, and the Plans shall be periodically reviewed and brought into conformity with related laws and regulations as newly prescribed or amended.

Article 3

The enterprise may appoint designated personnel or establish a dedicated organization to enforce personal data security with the allocation of appropriate resources.

The responsibility of the designated personnel or dedicated organization as referred to in the preceding paragraph shall be as follows:

1.Planning, prescribing, amending and executing matters concerning plans for maintaining the security of personal data files, and methods of handling personal data after termination of business.

2.Stipulating policies for the protection and management of personal data, as the basis and specific purposes for the collection, processing and use of personal data,

and other matters concerning protection, and announcing these to ensure that they are clearly understood by all members of staff.

- 3.Periodically conducting basic knowledge guidance or specialist education and training for staff members, to ensure that they clearly understand the provisions of laws and regulations relating to personal data protection, the scope of staff members' responsibilities relating to personal data protection, and the various methods or management measures for protecting personal data.

Article 4

The enterprise shall check all personal data in its custody; define those personal data are included in the scope of the Plans and establish the archives; and confirm of any change periodically.

Article 5

The enterprise shall, in accordance with the scope of personal data as defined in the previous article and the related procedures, analyze the possible occurrence of risk, and set appropriate control measures based on the results of risk analysis.

Article 6

The enterprise shall adopt the following matters for responding to the theft, alteration, damage, destruction or disclosure of personal data in its custody:

- 1.Adopt appropriate responsive measures to control consequential harm to the parties concerned.
- 2.Ascertain the current situation of the incident, and use appropriate means to notify the parties concerned. The notified information includes the fact of the incident which occurs on personal data, measures which the enterprise takes and the advisory service line provided.
- 3.Formulate preventive mechanisms, to avoid the recurrence of such kind of incident.

The enterprise shall fill in the Personal data infringement incident notification and record form (the format is shown in the attached table) and notify Civil Aviation Administration of MOTC within 72 hours after discovering the incident mentioned in the preceding paragraph. If the notification is not made within the time limit, the reason for the delay shall be attached.

After the incident in the preceding paragraph is reported, the competent authority may take appropriate supervision and management measures in accordance with the functions and powers conferred by Articles 22 to 26 of the Act.

Article 7

The enterprise shall establish the following management procedures respectively for ordinary personal data:

- 1.Examining and confirming whether the collection, processing and use of personal data includes personal data and the specific purposes thereof prescribed in Article 6 of the Act.
- 2.Confirming whether the collection, processing and use of personal data as prescribed in Article 6 of the Act is in compliance with the requirements of applicable laws and regulations.
- 3.Where personal data does not fall within the ambit of Article 6 of the Act, but is considered to need special management, it may still be managed similarly or by the setting of a special management procedure.

Article 8

The enterprises shall adopt the following steps for compliance with the provisions of Articles 8 and 9 of the Act concerning obligation to notify:

1. Examine whether the specific purposes of the collection and processing of personal data match the reasons for exemption from notification.
2. Adopt appropriate means of notification in accordance with the situation of the data collection.

Article 9

The enterprise shall examine whether its collection and processing of personal data has a specific purpose and legal imperative in compliance with the provisions of Article 19 of the Act.

Examination of the use of personal data shall determine whether it is in compliance with the provisions of Article 20 Paragraph 1 of the Act, and is within the scope of the specific purpose of use; when personal data is used outside the scope of the specific purpose, examination shall determine whether there is a legally prescribed condition for use outside the specific purpose.

Article 10: When the enterprise commissions another to collect, process or use personal data, in whole or in part, it shall conduct proper supervision of the commissioned party as prescribed in Article 8 of the Enforcement Rules of the Act, and set clear contractual requirements concerning the matters and methods of supervision.

Article 11

When the enterprise uses personal data for marketing for the first time, it shall provide the parties concerned with a free-of-charge means of expressing refusal to accept the

marketing, and after an expression of refusal by a party concerned, shall immediately cease to use that party's personal data for marketing, and announce this to all of its staff.

Article 12

Before the enterprise conducts the international transmission of personal data, it shall comply with the following provisions:

1. Examine whether the Ministry of Transportation and Communications has issued an applicable order or injunction limiting international transmission under the provisions of Article 21 of the Act, and shall comply therewith.
2. Inform the data owner of the area to which his/her personal data is to be transferred internationally. Additionally, the data recipient should be supervised in the following areas:
 - (1) The scope, category, specific purpose, period, region, subject, and method of the intended processing or use of personal data.
 - (2) Matters related to the data owner's exercise of the rights specified in Article 3 of the Act.

Article 13

The enterprise shall adopt the following methods to provide the parties concerned with the means to exercise the rights prescribed in Article 3 of the Act:

1. Confirming that the parties concerned are the subject of the personal data or are duly authorized to act on their behalf.
2. Providing the parties concerned with means of exercising their rights, and complying with the relevant time limits prescribed in Article 13 of the Act.
3. Informing whether there is a charge for necessary costs and expenses.
4. If it is determined that there is a reason why the exercise of their rights by a party concerned may be refused under Articles 10 and 11 of the Act, the reason shall be given in notification to the party concerned.

Article 14

The enterprise shall adopt the following methods to maintain the accuracy of all personal data in its custody:

1. Examining whether the procedure of collecting, processing and using personal data is correct.
2. When incorrect personal data is discovered, promptly correcting or supplementing it, and informing all parties to whom it has previously been provided for use.
3. Where there is a dispute as to the correctness of personal data, the matter shall be

handled as prescribed in Article 11 Paragraph 2 of the Act.

Article 15

The enterprise shall periodically review the personal data in its custody to confirm the specific purpose for keeping data still exists and not expired. If not, proceed according to Paragraph 3 of Article 11 of the Act.

Article 16

The enterprise may adopt the following personnel management measures:

1. In accordance with operational needs, to a suitable degree setting various limits on the authority of members of staff and controlling their access to personal data.
2. Reviewing the personnel with responsibility for all relevant work procedures involving the collection, processing and use of personal data.
3. Setting confidentiality obligations in contracts with all staff members.

Article 17

The enterprise may adopt the following data security management measures:

1. When using computer or automatic machine related equipment to collect, process and use personal data, appropriately set rules for use of portable devices or storage media.
2. If the content of personal data under custody has a need for encryption, adopt appropriate encryption mechanisms when collecting, processing or storing the data.
3. When a work process entails a need for backing up personal data, it shall be accorded the same protection as original documents in accordance with the provisions of the Act.
4. Where personal data is recorded on or in paper, magnetic disk, magnetic tape, compact disk, microfiche, IC chip, or other medium, appropriate preventive measures must be adopted to prevent the disclosure of such personal data when the medium is scrapped or transferred to other purpose.

Article 17-1

In accordance with business requirements, the enterprise shall take the following data security measures when collecting, processing, or utilizing personal data through an information and communications system:

1. Confirmation and protection mechanism for user identity.
2. Masking mechanism for the display of personal data.
3. Security encryption mechanism for Internet transmission.
4. Access control and protection monitoring measures for personal data files and

databases.

5. Countermeasures to prevent external network intrusion
6. Monitoring and response mechanisms for illegal or abnormal use behaviors. The measures Subparagraphs 5 and 6 of the preceding paragraph shall be regularly practiced and reviewed for improvement.

Article 18

The enterprises must adopt the following environmental management measures in respect of the environment of paper, magnetic disks, magnetic tapes, compact disks, microfiches, IC chips, computers, automatic machines or devices, or other media on or in which personal data is kept:

1. Implementing appropriate methods of input and output control in accordance with differences of business content.
2. Requiring all staff members to keep secure custody of storage media containing personal data.
3. Giving consideration to the establishment of suitable protective equipment or technology for each different media environment.

Article 19

After the enterprise terminates business, it may consider taking the following measures in respect of personal data, and keep relevant records as prescribed:

1. Destruction: Record the method, time and location of destruction, and keep proof of method of destruction.
2. Transfer: Record the reason for transfer, the transferee, method, time and location of transfer, and the legal basis for the transferee being permitted to take custody of the personal data.
3. Other deletion or termination of processing or use of personal data: Record the method, time and location of the deletion or termination of processing or use.

Article 20

The enterprise shall establish a mechanism for the audit of personal data security, and conduct routine or special inspection for assuring the Plans or the means for handling personal data after the termination of operation are duly executed.

Article 21

The enterprise may take appropriate measures, by adopting mechanisms for keeping records of the use of personal data, or the retention of tracking data in automatic machines or devices, or other relevant proof, to provide when necessary for explaining

the situation of the execution of its Plan.

Article 22

The enterprise shall give appropriate consideration to the current situation of business execution, public opinion, technological development, changes in law and regulations, and other pertinent factors, in examining whether the Plan it has made is appropriate, and shall amend the Plan when necessary.

Article 23

This Regulation shall come into full force as of January 1 2015.

The Amendment of this Regulation shall become effective on the date of promulgation.

Attachment

Personal Data Infringement Incident Notification and Record Form		
Name of non-government agency _____ Notification agency	Time of notification: at hh/mm on MM/DD/YYYY	
	Person of notification:Signature (seal)	
	Title:	
	Telephone:	
	E-mail:	
	Address:	
Time of occurrence		
Type of incident	<input type="checkbox"/> Stolen <input type="checkbox"/> Disclosure <input type="checkbox"/> Altered <input type="checkbox"/> Damaged <input type="checkbox"/> Destruction <input type="checkbox"/> Other	The total number of personal data infringed (approximately)
		<input type="checkbox"/> Number of general personal data____ <input type="checkbox"/> Number of special personal data____
Cause and summary of incident		
Damage condition		
Possible consequences of personal data infringement		
Responding measure to be adopted		
When and how to notify the personal data owner		
Notified within 72 hours following the discovery of personal data infringement		<input type="checkbox"/> Yes <input type="checkbox"/> No. Reason: