Content

Title：	Regulations Governing Personal Data File Security Maintenance Plans and Processing Methods After Termination of Business for Online Retail Industry and Online Retailing Service Platform Ch
Date：	2021.12.30
Legislative：	1.Promulgated on September 17, 2015 2.Amended on December 30, 2021

Content：

Article 1 These Regulations are formulated in accordance with the ersonal Data Protection Act (hereinafter referred to as the Act), Article 27, Paragraph 3.

Article 2 “Online retail industry” as mentioned in these Regulations refers to any company limited by shares that retails merchandise via the Internet and whose registered capital is NT$10 million or more, or which is one of the companies or business firms designated by the Ministry of Economic Affairs (hereinafter referred to as the Ministry). However, industries that are specially approved, or that are licensed or regulated by special management laws and regulations, shall be excluded.
“Online retailing service platform” as mentioned in these Regulations refers to any company limited by shares that provides an Internet platform for other retail industry and whose registered capital is NT$10 million or more, or which is one of the companies or business firms designated by the Ministry. However, industries that are specially approved, or that are licensed or regulated by special management laws and regulations, shall be excluded.

Article 3 To comply with the provisions of this Act, these Regulations, and other relevant laws and regulations, and in accordance with the business scale and characteristics, online retail industry shall reasonably allocate operating resources to establish a personal data management unit or an appropriate organization.
Appropriate resources shall be allocated for the following responsibilities:
1.Formulation and revision of a personal data protection and management policy (hereinafter referred to as the PDPMP).
2.Formulation, revision and implementation of a security and maintenance plan for the protection of personal data files and guidelines on disposing personal data following a business termination (hereinafter referred to as the SMP).
Formulation and revision of PDPMP and SMP shall be approved by the online retail industry’s representative or other authorized persons in charge.

Article 4 Online retail industry shall publicly disclose the PDPMP to employees and cause employees to clearly understand and comply with said PDPMP. Policy content shall include the following:
1.Complying with domestic laws and regulations on personal data protection.
2.Collecting, processing, and using personal data for specific purposes in a reasonable and secure manner.
3.Protecting the collected, processed, and used personal data files with technology at the level of security that

could be reasonably expected.
4.Setting up a point of contact for the principal parties of personal data (hereinafter referred to as the Parties) to exercise the rights concerning personal information or to file complaint or seek consultation.
5.Mapping out contingency plans for handling personal data stolen, tampered, damaged, destroyed, leaked, or other incidents.
6.If the collection, processing, and use of personal data are outsourced, properly monitoring outsourced service providers.
7.Continuing to fulfill the obligation of maintaining the SMP to ensure security of personal data files.

Article 5 The SMP in Article 3 shall include specific content meeting the provisions of Articles 6 to 19.
Online retail industry shall review, from time to time, the applicable personal data protection laws and regulations, and review and revise the SMP in a timely manner; the same shall apply with any changes in business operation or environmental condition.
When necessary, the Ministry may require online retail industry to submit the SMP and relevant documents, and may implement appropriate supervision and management measures in accordance with the authority conferred by Articles 22 to 25 of this Act.

Article 6 Online retail industry shall, in a timely manner, conduct annual inspections of the personal data files they have collected, and of their operational procedures for collecting, processing, and using such data. They shall also, based on such inspections, construct a personal data file inventory and a personal data operating procedures instruction manual.

Article 7 Online retail industry shall every year assess legal or other risks they may face due to the collection, processing, or use of personal data, and formulate appropriate control and response measures.

Article 8 The response measures mentioned in the preceding article shall include response mechanisms for stolen, tampered, damaged, lost, or leaked personal data. The content of the measures shall contain specific regulations pertaining to the following matters:
1.Methods for reducing and controlling damages to the Parties caused by the incident.
2.Notifying the Parties, in a timely manner and via appropriate methods such as e-mail, text message, telephone, or other means convenient for the Parties, regarding occurrence of the incident, management status thereof, the dedicated phone number for subsequent follow-up, and other channels for enquiries.
3.Corrective and preventive mechanisms to avoid recurrence of similar incidents.
4.Requirement that, in the event of a major incident, notification be sent within 72 hours of discovering the incident to the municipal or county (city) competent authority where the company is headquartered via email, using the format of the attached form, with a copy of the notification sent to the Ministry. The reporting shall be updated in a timely manner in accordance with the development of the incident. In addition, the overall investigation and handling process, outcome, and review shall be submitted to the municipal or county (city) competent authority where the company is headquartered, with a copy sent to the Ministry.
A “major incident” as mentioned in the preceding Subparagraph 4 refers to a situation in which the stolen, tampered, damaged, lost, or leaked personal data

will endanger normal operations of the online retail industry or the rights and interests of a large number of parties.
Attachment Personal Data Infringement Incident Notification and Record Form.pdf

Article 9

Unless otherwise provided by the law, online retail industry shall formulate specific procedures and mechanisms for the following matters, and produce effective ways to maintain the operation:
1.Inspection to ensure that the collection and processing of personal data conform to the legitimate circumstances and specific purposes defined in these Regulations, Article 19, Paragraph 1 or conform to other lawful reasoning.
2.Inspection to ensure that the use of personal data conforms to the specified purpose at the time of collection; or conforms to other specific purposes allowed by these Regulations; or conforms to other lawful reasoning. To use the personal data for purposes other than those to which the Parties have given written consent, the written consent shall be confirmed to comply with the Act, Article 7, Paragraph 2.
3.Inspection to ensure that notification regarding obligations stipulated in Articles 8 and 9 of the Act are delivered via appropriate and convenient methods that are to the Parties. When there is an exemption from notifications, the legal basis for the exemption shall be verified.
4.Inspection to ensure that, when using a Party’s data personal data for marketing purposes for the first time, the Party is provided with a channel to refuse marketing. The online retail industry shall pay all required fees for such.
5.Inspection to ensure that when a Party refuses marketing, the use of the personal information for marketing is immediately terminated, and that relevant personnel are all notified or measures are adopted to prevent such personnel from reusing the data for marketing.
6.Inspection to ensure that the collection, processing, and use of personal data comply with the provisions of the Act, Article 5.
7.Before the international transfer of personal data, analysis of possible impacts and risks from the transfer shall be conducted, and appropriate security protection measures shall be taken.
8.When the specified purpose no longer exists; the time limit expires; the circumstances defined in the Act, Article 19, Paragraph 2 apply; or the collection, processing, or use of personal data violates the provisions of the Act, then the collection, processing, or use of personal data shall be deleted or terminated in accordance with the law.
9.If the specified purpose no longer exists or the time limit has expired but the processing or use of personal data is not to be deleted or stopped, the continuation shall be based on the necessity of conducting business and with the written consent of the Parties.
10.Inspection to ensure that the personal data is correct. Disputes arising from the accuracy or incorrectness of data shall be handled in accordance with the provisions of the Act, Article 11, Paragraphs 1, 2, and 5.
11.Regarding the exercise of the rights of the Parties listed in the Act, Article 3:
(1)The means for the exercise of rights shall take into

	consideration the need for secure management of personal data and the convenience of the Parties. (2)Appropriate means of verification shall be adopted to confirm the identities of the Parties and their authorized representatives, or to require that the Parties or their authorized representatives provide explanations of their identities. (3)Fees may be charged for the cost of providing enquiries or making copies; however, the charges shall be stated in advance. (4)The deadlines stipulated in the provisions of these Regulations, Article 13 shall be observed. (5)In cases where the exercise of rights can be legitimately refused or the processing period can be extended, the Parties shall be provided with written notification regarding the reasons for the refusal or the reasons for the extension. 12.Commissioning another party to conduct the collection, processing, or use of personal data in whole or in part, standards and evaluation mechanisms shall be in place for selecting and appointing the agents. In addition, appropriate methods of supervision shall be clearly stipulated in the agent contract or related documents and shall be implemented accordingly. 13.When ommissioning by others to process personal data in whole or in part, and if the instruction of the entrusting organization violates the Act or other personal data protection laws and regulations, the entrusting organization shall be notified immediately. Online retail industry that transfer Parties' personal data internationally shall check whether restrictions by the Ministry apply, and shall inform the Ministry regarding the region where the personal data is to be transferred. In addition, they shall supervise the data recipients with regard to the following: 1. The planned scope, category, specific purpose, time period, territory, recipients, and methods of the processing or use of personal data. 2. Matters related to the Parties' exercising of rights prescribed in the Article 3 of the Act.
Article 10	Online retail industry that has mechanisms to protect the personal data of consumers shall remind them in a timely manner to use the mechanisms, and shall make appropriate announcements.
Article 11	Online retail industry shall take into account factors such as the nature of the business; the personal data access environment; tools and methods of personal data transmission; and the types and quantities of personal data as such online retail industry adopt appropriate security management measures for personnel, operations, equipment, and technology.
Article 12	The personnel security management measures mentioned in the preceding article shall include the following: 1.Verifying the person in charge of business processes related to collection, processing, and use of personal data. 2.Setting the scope of authority for personnel handling collection, processing, or use of personal data, as well as the authority to access personal data storage media in accordance with business execution needs; regular inspection of the necessity for such authorized scopes, and control of access to personal data. 3.Setting confidentiality obligations in contracts with all staff members.
Article 13	The operations security management measures mentioned in Article 11 shall include the following:

1.Formulating and implementing norms for the use of the personal data in storage media.
2.Before disposing of personal data storage media or using it for other purposes, all personal data stored in the media shall be destroyed or deleted in an appropriate manner. When commissioning another party to perform the above-mentioned actions, the provisions of Article 9, Subparagraph 12 shall apply mutatis mutandis, and shall be subject to appropriate supervision.
3.In the collection, processing, or use of personal data, if there is a necessity for encryption or masking, it shall be conducted using appropriate encryption or masking mechanisms.
4.Appropriate security protection mechanisms shall be in place when transmitting personal data.
5.Depending on the importance of the stored personal data, appropriate backup mechanisms shall be adopted; such backups shall be protected as with the original data.

Article 14 The equipment security management measures mentioned in Article 11 shall include the following:
1.As required by different operation content and environments, implementing necessary security and environmental controls.
2.Properly maintaining and controlling the physical equipment used in the collection, processing, and use of personal data.
3.Establishing necessary protective equipment and technologies for different operating environments.

Article 15 The technology security management measures mentioned in Article 11 shall include the following:
1.Adopting appropriate security mechanisms to avoid unauthorized access to computers, related equipment, and systems for collecting, processing, and using personal data. These mechanisms shall include but are not limited to, setting up necessary control mechanisms for access rights to personal data and regularly verifying the effectiveness of such control mechanisms.
2.Regularly verifying that the computers, related equipment, and systems for collecting, processing, and using personal data have the necessary security capabilities. These capabilities shall include, but are not limited to, adopting appropriate security mechanisms to deal with threats caused by malicious programs and system vulnerabilities.
3.When conducting software and hardware testing, actual personal data shall be avoided. If the use of actual personal data is required, the procedures and security management methods for such use shall be clearly defined.
4. Computers, related equipment, and systems for collecting, processing, and using personal data shall be regularly inspected for usage and personal data access status.

Article 16 Online retail industry shall conduct personal data protection and management awareness promotion, education, and training for the employees every year, to ensure that such employees understand regulatory requirements related to personal data protection, the scope of responsibility, and all operational procedures for personal data protection. Education and training shall also be conducted every year for representatives, persons-in-charge, and management units or appropriate organizations referred to in Article 3 in accordance with the tasks and roles in the SMP.

Article 17 When all or part of business is terminated, online

	retail industry shall delete, destroy, or terminate the relevant personal data. If such personal data is to be transferred to a third party, it shall be first confirmed whether the third party has the legal right to collect said personal data. The transfer in the preceding paragraph shall be conducted in a legal and appropriate manner.
Article 18	Online retail industry shall regularly conduct internal SMP audits, submit evaluation reports, by the personal data management units and appropriate organizations which is defined in Article 3, and adopt the following improvement measures: 1.PDPMP and SMP revision. 2.If there are any indications of regulatory violations or risk of regulatory violations in the evaluation report, relevant improvement and preventive measures shall be formulated and adopted.
Article 19	Online retail industry shall maintain the following records and documentation for SMP implementation, unless otherwise stipulated by other laws and regulations: 1.Records for provision or transfer of personal data to third parties. Such records shall include data including the recipients, basis, reasons, methods, times, and places for such provision or transfer. 2.Records for verification of the correctness of personal data and documentation of additions and changes to the data. 3.Records regarding the Parties' exercise of rights stipulated in the Act Article 3 and handling processes thereof. 4.Records for reasons, methods, times, and places when deleting, terminating the processing or use, or destroying personal data or personal data storage media. 5.Records for personal data system access. 6.Data backups and records confirming the validity thereof. 7.Records for additions, changes, and deletions to personnel authorizations. 8.Records for actions taken in response to incidents. 9.Records for regular inspections of information systems for processing personal data. 10.Records for awareness promotion, education, and training. 11.Records for SMP audits and improvements. 12.Other necessary records and documentation.
Article 20	For online retailing service platforms, the provisions of Articles 3 to 19 shall apply mutatis mutandis. Such platforms’ SMPs shall include the following: 1.For platform users, appropriate personal data protection and management awareness promotion or education and training shall be conducted. 2.Personal data protection rules shall be formulated, and platform users shall be required to comply with the rules.
Article 21	These Regulations shall enter into force on the date of promulgation.