An Introduction to Taiwan's Regulations Regarding the Security Maintenance and Administration of Personal Information Files in in Digital Economy Industries

An Introduction to Taiwan's Regulations Regarding the Security Maintenance and Administration of Personal Information Files in in Digital Economy Industries

2023/11/29

I. Preface

The Personal Data Protection Act (below, the "Act"), Article 27, paragraph 3 authorizes all central government authorities in charge of specific industries to formulate regulations regarding security standards and maintenance plans for their concerned industries.

Beginning August 27, 2022, Taiwan transferred authority over information services, software publishers, businesses that do retail sales of goods purely via the Internet, third-party payment providers, and other businesses in digital economy industries from the Ministry of Economic Affairs to the newly-established Ministry of Digital Affairs (MODA). Businesses in the digital economy industries collect, process, and use large amounts of important personal data, and therefore bear a relatively heavy responsibility for maintaining the security of personal data. In light of this, and in accordance with the Act, Article 27, paragraph 3, the MODA therefore promulgated the Regulations Regarding the Security Maintenance and Administration of Personal Information Files in in Digital Economy Industries (below, the "Regulations") on October 12, 2023. These Regulations specify the standards for digital economy industries' personal data file security maintenance plans and rules governing the handling of personal data following a business termination (below, "security and maintenance plans", or "SMPs").

These regulations apply to all businesses in the digital economy industries. In order to reinforce responsibility for personal data security maintenance in the digital economy industries, tiered management is applied to businesses at different scales. The key points of these Regulations are introduced below.

II. Where the Regulations apply

As stipulated in the Regulations, Article 2, the "digital economy industries" that these Regulations apply to refer to any natural person, private juridical person, or other group, that engages in any of the following business operations: 4871 Retail Sale via Internet (industries that engage in retail sales to others via the Internet, but not including television, radio, phone, or other electronic means, nor postal sales); 582 Software Publishing; 620 Computer Programming, Consultancy and Related Activities; 6312 Data Processing, Hosting and Related Activities (industries that engage in processing customers' data, server & website hosting, and other related services, but not including online audio/video streaming services); 639 Other Information Service Activities; or 6699 Other Activities Auxiliary to Financial Service Activities Not Elsewhere Classified (third-party payment industries, but not including other fund management activities). For the specific industries covered, see Attachment 1 of the Regulations.

III. Security maintenance and management measures

The relevant measures are stipulated in Articles 3 to 17 of the Regulations. In consideration that the businesses so regulated may collect, process, or use large amounts of personal data as part of their business activities, they bear a larger responsibility for maintaining the security of personal data than does the average enterprise. In compliance with the Regulations, every such enterprise is required to formulate an SMP, the content of which shall comply with the specifications in Articles 5 to 17. This includes putting in place management personnel and relevant resources; defining and inventorying the scope of personal data; risk assessment; putting internal management procedures in place; and other such matters.

These Regulations also adopt tiered management for businesses based on their capital levels, in order to reinforcement the frequency at which security maintenance measures are performed. The specific regulations for security maintenance measures are introduced below.

1. Formulating an SMP

In accordance with the Regulations, Article 3, and in order to maintain the security of personal data, each enterprise shall, within three months of the date the Regulations take effect, plan and formulate their SMP. Every enterprise shall also cause all staff members to understand and fully implement the SMP. In order to monitor implementation, the MODA may require that each enterprise submit its implementation of SMP; the enterprise shall then submit their implementation status information in written form within the specified time limit.

2. Making the protection policy known internally

In accordance with the Regulations, Article 4, and to make sure that everyone in the enterprise comprehends and implements personal data protection, each enterprise shall make its personal data protection policies known to all personnel within the enterprise. Matters that must be explained include Taiwan's legal regulations and orders on personal data protection; how personal data may only be collected, processed, and used for specific purposes and in a reasonable, secure way; that protective technology must be at a level of security that could be reasonably expected; points of contact for rights relating to personal data; personal data contingency plans; and proper monitoring of outsourced service providers to whom personal data is outsourced. All of this must be done to make sure that every enterprise carries out their duty for comprehensive, continuous SMP implementation.

3. SMP content

(1) Putting in place management personnel with relevant resources

In accordance with the Regulations, Article 5; in accordance with both the Regulations as a whole and other laws and orders regarding the protection of personal data; and in order to implement personal data protection, each enterprise shall do the following things: Weigh the size and characteristics of their business to reasonably allocate operating resources; take responsibility for the personal data protection and management policy; and formulate, revise, and implement their SMP. Also, the enterprise's representative or the representative's authorized personnel shall carry out formulation and revision, in order to make sure that the SMP's content is fully carried out.

(2) Establishing the scope of personal data

In accordance with the Regulations, Article 6, in order to define the scope of personal data to be included in the SMP, each enterprise shall periodically check the status of personal data that is collected, processed, or used.

(3) Risk assessment and management mechanisms for personal data

In accordance with the Regulations, Article 7, in a timely manner, and in accordance with their already-established personal data scopes and the processes in which their business involves the collection, processing, or use of personal data, each enterprise shall evaluate risks that may arise within their scope and processes. Based on the risk evaluation results, each enterprise shall then adopt appropriate security management and response measures.

(4) Incident prevention, reporting, and response mechanisms

In accordance with the Regulations, Article 8, and in order to reduce/control damages to data subjects resulting from personal data theft, tampering, damage, destruction, leakage, or other such security incidents, each enterprise shall formulate response, reporting, and prevention mechanisms:

1. Response mechanism: Methods to be followed after a security incident has occurred, to reduce/control damages to data subjects, and appropriate ways to notify data subjects after an incident investigation, as well as what such notifications shall contain.
2. Notification mechanism: Post-incident notifications to data subjects, in a form (such as email, text message, phone call, etc.) that makes it convenient for such subjects to learn what has occurred and what the incident handling status is; also, providing data subjects with a hotline or other way of seeking information later on.
3. Prevention mechanism: A post-incident mechanism for discussing and adjusting the prevention measures.

Within 72 hours after an enterprise learns that a personal data security incident has occurred, the enterprise shall use Attachment 2, the Enterprise Personal Data Leak Reporting Form, to notify the MODA of matters such as: A description of what caused the incident; an incident summary; the damage status; possible results from the personal data leakage; proposed response measures; proposed method and time for notifying data subjects; etc. Alternately, the enterprise may notify the special municipality or county/city government to then notify the MODA. If the enterprise is unable to report the incident within the time limit or is unable to supply complete reporting information all at once, the enterprise shall attach explanation of the reasons for the delay, or provide the information in stages. After the MODA or the special municipality or county/city government receives a report, they may implement reasonable handling in accordance with Articles 22 to 25 of the Act.

(5) Internal management procedures for personal data collection, processing, and usage

In accordance with the Regulations, Article 9, in order to ensure that their collection, processing, and use of personal data complies with the laws and orders regarding the protection of personal data, each enterprise shall do the following: Formulate internal management procedures; assess whether the use, processing, or collection of special categories of personal data are involved; assess data subjects' consent has been obtained; assess whether the legal circumstances create an exemption from the obligation to inform; etc. The internal management measures shall also include providing data subjects with information on their rights in accordance with the Act, Article 3; putting in place mechanisms for ensuring the accuracy of and inquiring regarding personal data; and periodically reviewing whether the specific purposes for collecting personal data still exist or have expired.

(6) Limits, notifications, and monitoring for international transfers

In accordance with Article 10 of the Regulations and Article 21 of the Act, when an enterprise's transfer of personal data across a national border affects data subjects to the extent that there is a major national interests concern, the enterprise shall assess whether MODA restrictions apply to the transfer. The enterprise shall also notify the data subjects of the region(s) that the data is transferred to; perform appropriate monitoring of the data recipient; and provide the data subjects with information on their rights in accordance with the Act, Article 3.

(7) Data, personnel, and equipment security management measures

1. Data security management measures: In accordance with the Regulations, Article 11, and when personal data is backup, kept confidential, or transferred by various means based on the risk assessment results, each enterprise shall put in place protective measures against abnormal access behaviors. When an enterprise provides information/communication technology services, the enterprise shall also put in place and regularly monitor intrusion countermeasures, abnormal access monitoring and contingencies, anti-malware mechanisms, account password verification, system testing, and other such data security management measures.
2. Personnel security management measures: In accordance with the Regulations, Article 12, each enterprise shall contractually specify the obligation to maintain confidentiality with all staff members; identify personnel who job duties involve collecting, processing, or using personal data; and periodically assess the appropriateness and necessity of personnel's permissions to access personal data.
3. Equipment security management measures: In accordance with the Regulations, Article 14, and to prevent personal data being stolen, tampered with, damaged, destroyed, or leaked, each enterprise shall put in place appropriate media protection for personal data storage devices. The protection requirements include management measures such as technology, equipment and secured environments that meet a specific level of security.

(8) Education and training

In accordance with the Regulations, Article 13, each enterprise shall periodically use education and training to ensure that all staff members understand the following things: The laws and regulations pertaining to personal data protection; their personal duties and roles within their scopes of responsibility; and the requirements for all SMP management procedures, mechanisms, and measures. For any enterprise that engages in retail sales via the Internet, their SMP shall include user training and education regarding personal data protection and management; and the enterprise shall also formulate personal data protection rules for compliance.

(9) Continuous audit, recording, and improvement mechanisms

1. Data security auditing mechanisms: In accordance with the Regulations, Article 15, each enterprise shall periodically do internal audits of personal data, then put the audit results into an evaluation report that reviews improvements to the enterprise's protection policy, SMP, etc. If there are any deficiencies, the enterprise shall make corrections.
2. Use of records, tracking data, and retention of evidence: In accordance with the Regulations, Article 16, and as part of carrying out its SMP, each enterprise shall retain a minimum of five years of records on the collection, processing, and use of personal data; tracking data for automated machinery; and evidence of having implemented the SMP. After an enterprise's operations cease, it shall retain records of the destruction, transfer, or other deletion of personal data for a minimum of five years.
3. Comprehensive, continuous improvement for personal data security maintenance: In accordance with the Regulations, Article 17, any time an enterprise's SMP is not implemented, the enterprise shall adopt corrective and preventive measures. Also, based on the SMP's implementation status, its handling methods/implementation status, developments in data technology, adjustments to the enterprise's business, and changes in the law and regulations, each enterprise shall periodically review and amend its SMP.

4. Tiered management

In accordance with the Regulations, Article 18, and to prevent relatively small businesses having to take on excessive personal data management costs, tiered management is applied. For an enterprise with a specific business scale (having capital of NT$10 million or more, or holding 5,000 or more personal data records), stronger security measure implementation is required, namely, the personal data security measures shall be implemented, reviewed, and improved at least once every twelve months. If an enterprise reaches NT$10 million or more in capital after the Regulations take effect, or if an enterprise's number of personal data records held reaches 5,000 or more as a result of direct or indirect data collection, then within six months of meeting those conditions, the enterprise shall implement and review the improvement measures at least once every twelve months.

5. Outsourced personal data

Commercial outsourcing in the digital economy comes in many forms. In light of this, and in order to make clear each enterprise's security management obligations with regard to the collection, processing, and use of personal data, Article 19 of the Regulations clearly spells out what duties shall be carried out with regard to any outsourcing that touches on personal data. When an enterprise outsources the collection, processing, or use of personal data, it is considered equivalent to the enterprise's own activity. Thus, the enterprise shall understand and follow the legal orders and regulations on personal data set by the central government authorities in charge of the outsourcing party's industries. Any oversight responsibilities arising from outsourcing the collection, processing, or use of others' personal data shall be clearly stipulated in the outsourcing contract or other such documents.

IV. Conclusion

The Regulations Regarding the Security Maintenance and Administration of Personal Information Files in in Digital Economy Industries are designed to balance development for Taiwan's digital economy industries with comprehensive, continuous improvement of personal data security maintenance. In pursuit of those goals, the Regulations clarify what each enterprise must do: Plan, formulate, and carry out security maintenance plans for personal data that falls within the bounds of the enterprise's business; ensure that all staff members receive training on personal data protection; provide personal data subjects with channels to file complaints and seek consultation on their rights; and inform the government authorities in charge of the digital economy about the enterprise's SMP, including the status of any personal data security incidents. All this is done in hopes that the security measures will continuously improve the security of personal data in Taiwan's digital economy industries.

Wen, Chih Chiang
Associate Legal Researcher

Release : 2023/12