ONE ASIA LAWYERS

Overview of Amendments to the Personal Information Protection Law

October 15, 2021
One Asia Lawyers Tokyo Office
Hironori Matsumiya

On June 12, 2020, the "Act for Partial Revision of the Act on the Protection of Personal Information, etc." (hereinafter referred to as the "Revised Act") was promulgated. The Act on the Partial Revision of the Act on the Protection of Personal Information, etc. (hereinafter referred to as the "Revised Act") was promulgated on June 12, 2020 and is scheduled to come into effect in April 2022. The Personal Information Protection Commission of Japan (PSC) published the guidelines for the revised law on August 2, 2021, and preparations for its enforcement are now underway. The following is an overview of the revised law.

1 Background of the revision

The 2015 amendments to the Personal Information Protection Law (hereinafter referred to as the "Current Law") included provisions for a "so-called triennial review" (Article 12 of the Supplementary Provisions). The amendment was made based on the provision in the 2015 amendment to the Act on the Protection of Personal Information (hereinafter referred to as the "Current Act"), which included a provision on the "so-called triennial review" (Article 12 of the Supplementary Provisions), from the perspective of strengthening the protection and utilization of the rights and interests of individuals, responding to new risks associated with the increased distribution of cross-border data, and responding to the era of AI and Big Data.

The main points of the amendment are as follows

(1) The nature of individual rights
(2) Responsibilities to be observed by business operators
(3) How data should be utilized
(4) Penalties
(5) Extraterritorial application of laws and cross-border transfer

2 The nature of individual rights

(1) Relaxation of requirements for the right to request suspension of use, deletion, etc.

Under the current law, an individual's right to request the cessation of use or deletion

of personal information was limited to cases where the information was used for purposes other than those for which it was intended or was obtained illegally. In addition, requests to stop the provision of personal data to a third party were limited to cases where the data was provided to a third party without the consent of the individual or to a third party in a foreign country without the consent of the individual.

The revised law expands the scope to include cases where (1) the business no longer needs to use the retained personal data, (2) there is a leak, etc. of the retained personal data, or (3) there is a risk that the rights or legitimate interests of an individual will be harmed by the handling of other retained personal data (Article 30, Paragraph 5 of the revised law).

(2) Digitization of requests for disclosure of retained personal data

Under the current law, in principle, personal data in possession must be disclosed in writing, but now it can be disclosed by any method designated by the individual, including the provision of electromagnetic records (Article 28, Paragraph 1 of the revised law).

(3) Request for disclosure of records provided to a third party

It has been made possible for the individual to request the disclosure of records of the provision of personal data to third parties (Article 28, Paragraph 5 of the revised law).

(4) Conversion of short-term stored data into retained personal data

Short-term data to be deleted within 6 months, which was stipulated in the current law, is now included in retained personal data under the revised law, and is subject to disclosure, suspension of use, etc. (Article 2, Paragraph 7 of the revised law).

(5) Limiting the scope of personal data that can be provided under the opt-out provisions.

The scope of personal data that can be provided to third parties under the opt-out provisions has been limited to include (1) personal data that has been illegally obtained and (2) personal data that has been provided under the opt-out provisions (Article 23(2) of the revised law).

3 Responsibilities of business operators to be protected

(1) Mandatory reporting of leakage

When a leak, etc. occurs and there is a risk of harm to the rights and interests of an

individual, reporting to the Personal Information Protection Committee and notification to the individual are newly obligated (Article 22-2 of the revised law).
Under the current law, there was no legal obligation to report in the event of a leak. As a result, there were some businesses that did not respond proactively, and if the businesses did not even make a public announcement, there was a risk that the Committee would not be able to grasp the case and take appropriate action. In response to this situation, a reporting obligation has been established in this revision. The cases subject to the mandatory reporting of leaks, etc. are defined as leaks of personal information requiring consideration, leaks that may cause property damage, leaks due to unauthorized access, etc., and large-scale leaks exceeding 1,000 cases (Article 6-2 of the Enforcement Regulations of the Act on the Protection of Personal Information).

(2) Prohibition of use by inappropriate methods

It has been clarified that personal information shall not be used in an inappropriate manner, such as to facilitate illegal or unjust acts (Article 16-2 of the revised law).
In the current law, the prohibition of inappropriate use of personal information was not explicitly prohibited. As a result, there have been cases where personal information was used in a manner that may lead to infringement of the rights and interests of individuals, so this amendment prohibits businesses from using personal information in an inappropriate manner.

4 How to establish a system to encourage voluntary efforts by businesses

Enhancement of the authorized personal information protection organization system

With regard to the system of accredited organizations, in addition to the current system of accrediting organizations that cover the handling of personal information, etc. in all fields of the target business entity, it is now possible to accredit organizations that cover personal information, etc. in specific fields of the target business entity (Article 47, Paragraph 2 of the revised law).

5 How data should be utilized

(1) Relaxation of obligations of business operators for pseudonymized information

Pseudonym-processed information," in which names, etc., are deleted, has been created, and some obligations of businesses, such as the obligation to report leaks, etc., and the obligation to request disclosure and suspension of use, will be exempted if the information constitutes "pseudonym-processed information," provided that it is

limited to internal analysis (Article 35-2, Paragraph 9 of the revised law).

(2) Establishment of new regulations on the provision of personal-related information to third parties

The current law does not regulate the provision to third parties of information that does not fall under the category of personal data at the source, but is expected to become personal data at the recipient. Under the amendment, the provider is required to confirm with the recipient that the consent of the individual has been obtained (Article 26-2, Paragraph 1 of the amended law).

6 What the penalty should be

(1) Increase in the statutory penalty

The statutory penalty for violation of an order issued by the Personal Information Protection Commission has been raised to imprisonment for not more than one year or a fine of not more than one million yen. In addition, the statutory penalty for making a false report, etc. to the Committee has been increased to a fine of 500,000 yen or less (Articles 83 and 85 of the Revised Act).

(2) Increase in fines for corporations

With regard to fines for the crime of unauthorized provision of databases, etc., and for violations of orders, the maximum amount of fines for corporations has been increased to 100 million yen, taking into consideration the disparity in financial resources between corporations and individuals (Article 87, Paragraph 1 of the revised law).

7 Extraterritorial application of laws and cross-border transfer

(1) Strengthening of extraterrestrial application

Foreign business operators that handle personal information, etc. in connection with the provision of goods or services to persons in Japan are now subject to reporting and collection of orders secured by penalties (Article 75 of the revised law).

Under the current law, the authority that the Commission can exercise over a foreign business operator is limited to guidance and advice, which are non-enforceable powers such as recommendations. Since there was a risk that the Commission would not be able to take appropriate measures to deal with cases such as leakage in foreign countries, the amendment enables the Commission to take more effective measures against foreign business operators.

(2) Improving the provision of information on cross-border relocation

In addition to the requirements for business operators to be able to provide personal data to third parties located in foreign countries, the provision of information to the individual is now required as follows (Article 24 of the revised law)

(i) If the individual consents to the transfer, information shall be provided to the individual regarding the name of the country to which the personal data is to be transferred and the existence of a system for the protection of personal information in the country to which the data is to be transferred.

(ii) In cases where the transfer is made by an entity that has established a system that conforms to the standards, the entity shall periodically check the status of handling by the transferee entity and provide information upon request of the individual.