

Amendments to the Personal Information Protection Act, ISMS-P response strategy through professional consulting

Strategic Consulting Department Kim Young Woo Manager

■ Overview

The amended Personal Information Protection Act came into effect on September 15, 2023. This law was fully revised with the aim of strengthening the protection of data subjects' rights and securing interoperability with global norms, following the amendment of the 3 Data Acts in 2020. As a result, some revisions were also applied to the Personal information & Information Security Management System (hereinafter referred to as ISMS-P) maintained by companies. The details of the revisions are announced on the Personal Information Protection Commission website.

In this headline, we intend to analyze changes due to the revisions in 2023 and present countermeasures in order to provide help to companies that are currently maintaining ISMS-P or seeking to be newly certified in accordance with the amendment of the Personal Information Protection Act.

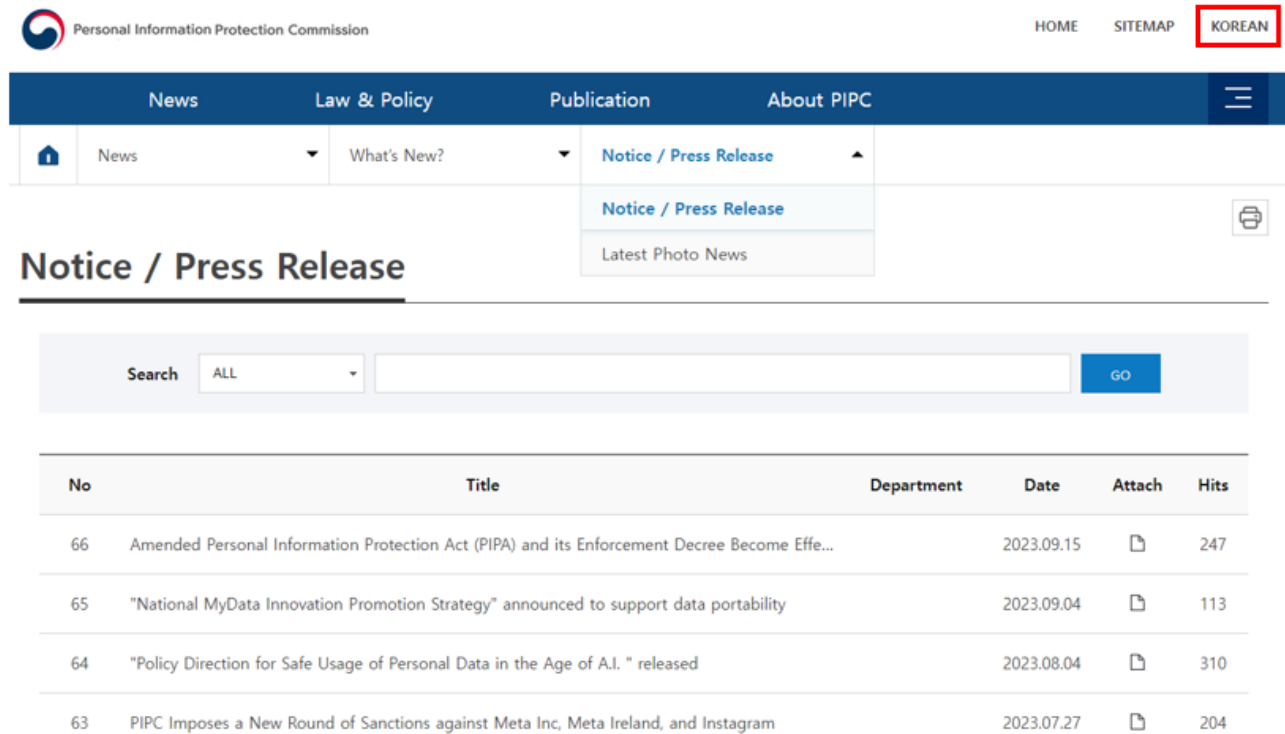


■ How to check the revised laws and details

Here's how to check the revised Personal Information Protection Act:

Checking legislative and administrative notices

After accessing the PIPC website, you can check information related to the amendment of the Personal Information Protection Act by clicking on the notice in the Notification/News tab.



The screenshot shows the homepage of the Personal Information Protection Commission (PIPC). The header includes the PIPC logo and name, along with navigation links for HOME, SITEMAP, and KOREAN. A dark blue navigation bar contains tabs for News, Law & Policy, Publication, and About PIPC. Below this, a dropdown menu is open for 'News', showing options for 'What's New?', 'Notice / Press Release', and 'Latest Photo News'. The 'Notice / Press Release' option is selected, and the page title is 'Notice / Press Release'. A search bar is visible with a dropdown set to 'ALL' and a 'GO' button. Below the search bar is a table listing recent notices.

No	Title	Department	Date	Attach	Hits
66	Amended Personal Information Protection Act (PIPA) and its Enforcement Decree Become Effe...		2023.09.15		247
65	"National MyData Innovation Promotion Strategy" announced to support data portability		2023.09.04		113
64	"Policy Direction for Safe Usage of Personal Data in the Age of A.I. " released		2023.08.04		310
63	PIPC Imposes a New Round of Sanctions against Meta Inc, Meta Ireland, and Instagram		2023.07.27		204

Source: Personal Information Protection Commission (www.pipc.go.kr)

■ ISMS-P certification control item mapping

ISMS-P certification control items were mapped according to the revision of the Personal Information Protection Act. As a result, among the major revisions, a total of 21 ISMS-P certification control items in 4 areas (excluding the principles of the Personal Information Protection Act as they are not legal changes), including the mobile video device provisions and the special provisions for information and communications services, were mapped. Details are as follows:

〈Table 1〉 Personal Information Protection Act vs. ISMS-P Certification Control Items

Revised Personal Information Protection Act	ISMS-P Certification Control items (21)	
Mobile video device provisions	3.1.6	Installation and operation of visual data processing devices
Modification of special provisions for information and communications services (Unification of online and offline provisions)	1.1.5	Policy making
	2.5.4	Password management
	2.10.8	Patch management
	3.2.1	Personal information status management
	3.4.1	Destruction of personal information
Method for obtaining consent and additional use/provision	3.1.1	Collection and use of personal information
	3.1.2	Consent to collection of personal information
	3.1.5	Indirect collection of personal information
	3.3.2	Outsourcing of personal information processing
	3.5.3	Notification to data subjects
Prohibition of using personal information for personal purposes	3.2.4	Out-of-purpose use and provision of personal information
Measures to ensure safety, such as special provisions for public system operating institutions	1.1.4	Establishment of range
	2.1.2	Maintenance of the organization
	2.5.6	Reviewing access rights
	2.9.4	Log and access record management
	2.9.5	Checking log and access records
Cross-border transfer and cease and desist order	3.3.4	Cross-border transfer of personal information
Improving the certification standards system focusing on the principles of the Personal Information Protection Act	2.4.7	Work environment security
	2.6.3	Application access
	3.2.5	Processing of pseudonymized information

Source: Personal Information Protection Commission Notification No. 2023-8, October 5, 2023, and Ministry of Science and ICT notice No. 2023-33, October 5, 2023 partial amendment,

2023 information security & personal information protection conference—reference (title: Key details of the amendments to the Personal Information Protection Act)

■ Major amendments to the Personal Information Protection Act (ISMS-P mapping criteria)

The main amendments to the Personal Information Protection Act linked to ISMS-P certification control items are as follows:

- ① Establishment of operating standards for mobile image processing devices
- ② Unifying regulations on information and communications service providers and offline personal information controllers by reorganizing special provisions for information and communications service providers into general provisions
- ③ Partially relaxing the legal basis for collecting and using personal information
- ④ Strengthening the standards for use of personal information
- ⑤ Strengthening safety measure standards for institutions operating major public systems, etc.
- ⑥ Expanding the requirements for cross-border transfer of personal information to meet international standards

〈Table 2〉 Major amendments to the Personal Information Protection Act linked to ISMS-P certification control items

Amended Personal Information Protection Act	Key contents of the amendments
Mobile video device provisions	(Amendment details) In principle , the act of recording personal video information using a mobile visual data processing devices for business purposes in public places , etc. is restricted .
	(Exception) Exceptions are permitted in cases where personal information is collected and used, or when the data subject does not express his/her intention to refuse even though he/she was aware of the recording.
	When filming, the fact of filming must be indicated with lights, sounds, signs and announcements, in writing , etc.
	(Enforcement Decree) New provisions were established, including the specific scope of mobile video devices, reasons for exceptions to restrictions on the operation of video devices in bathrooms and restrooms, and methods for indicating the fact of filming .
Modification of special provisions for information and communications services (Unification of online and offline provisions)	(Amendment details) By unifying the special provisions for information and communications services with the general provisions, the principle of ' same behavior – same provisions ' is applied to all personal information controllers.
	Special provisions that are similar to or overlapping with general provisions are integrated and reorganized into general regulations to unify different provisions between online and offline business operators.
	The damage compensation guarantee system, domestic agent designation system, notification of personal information use details, etc., which are only in special provisions, have been converted to general provisions and extended .
Method for obtaining consent and additional use/provision	The consent system to ensure data subjects' actual right to consent and to support reasonable collection and use of personal information by companies, etc. has been improved.
	The phenomenon of 'consent universalism' has been improved by reorganizing the 'required consent' provision in the special provisions for information and communications services, and the requirements for lawful processing of personal information other than consent have been activated .
	Public health purposes , such as COVID-19, have also been added to collection and use requirements .
	Processing requirements have been improved to enable flexible response in urgent cases to protect the life of citizens, etc.
	(Enforcement Decree) The mandatory consent practices have been improved by clarifying valid consent standards and distinguishing the legal basis for personal information that can be processed without consent and disclosing it in the processing policy .
Prohibition of using personal information for personal purposes	(Amendment details) The act of 'using' another person's personal information in excess of the permitted authority without legitimate authority has been added to the prohibited acts provision in Subparagraph 3 of Article 57 .
Measures to ensure safety, such as special provisions for public system operating institutions	(Enforcement Decree) For public institutions that process citizens' personal information on a large scale, safety and transparency are reinforced by strengthening public system security measures, improving personal information file registration , and disclosing personal information impact assessment results .

	Safety measure standards for organizations operating major public systems, etc. have been strengthened.
	Targets of public institutions' personal information file registration targets have been modified.
	The basis for disclosing the results of public institutions' personal information impact assessment has been prepared.
Cross-border transfer and cease and desist order	(Amendment details) To strengthen interoperability with overseas laws, the legal requirements for cross-border transfers other than consent have been diversified , and protective measures have been strengthened by establishing a new cease and desist order right .
	for cross-border transfers have been diversified to include cases where personal information protection has been certified and the level of personal information protection of the country or international organization to which personal information is transferred is recognized as guaranteed .
	In cases where there is a significant risk of damage to the data subject due to violations of the law or the country to which personal information is transferred does not adequately protect personal information, the right to order personal information controllers to cease and desist cross-border transfers has been newly established.

Source: 2023 information security & personal information protection conference—reference
title: Key details of the amendments to the Personal Information Protection Act)

■ Amendments to the ISMS-P Notice

In accordance with the revision of the law, “Ministry of Science and ICT notice Personal Information Protection Commission Notice No. 2023-08 – “ 「Notice on information protection and personal information protection management system certification, etc. 」 ” was implemented with partial amendments on October 5, 2023. As a result of analyzing the ISMS-P certification control items, they are classified into 5 categories as shown in the table below.

〈Table 3〉 Classification criteria for revised ISMS-P control items

No.	Description	Before change
①	Partial transfer of detailed inspection items of item 3.2.3	3 cases
②	Item name changed	11 cases
③	Improved certification standards by reflecting amendments to the Enforcement Decree	7 cases
④	Newly inserted	1 case
⑤	Deleted	2 cases

Source: Personal Information Protection Commission notice No. 2023-8, October 5, 2023, and Ministry of Science and ICT notice No. 2023-33, October 5, 2023, partial amendment

<Table 3> Details analyzed through the ISMS-P revised classification criteria for control items are as follows:

<Table 4> Details of the changes according to the revision of the ISMS-P notice

ISMS-P control items				Details of the change
Before		After		
2.4.7	Work environment security	2.4.7	Work environment security	① Partial transfer of detailed inspection items of item 3.2.3
2.6.3	Access to application programs	2.6.3	Access to application programs	① Partial transfer of detailed inspection items of item 3.2.3
2.12.1	Safety measures in preparation for disasters	2.12.1	Safety measures in preparation for disasters	② Item name changed
3.1.2	Consent to collection of personal information	3.1.1	Consent to collection of personal information	② Item name changed ③ Improved certification standards by reflecting amendments to the Enforcement Decree
3.1.1	Limitation to collection of personal information	3.1.2	Limitation to collection of personal information	③ Improved certification standards by reflecting amendments to the Enforcement Decree
3.1.5	Indirect collection protection measures	3.1.5	Indirect collection of personal information	② Item name changed ③ Improved certification standards by reflecting amendments to the Enforcement Decree
3.1.6	Installation and operation of visual data processing devices	3.1.6	Installation and operation of visual data processing devices	③ Improved certification standards by reflecting amendments to the Enforcement Decree
3.1.7	Measures taken when used for promotional and marketing purposes	3.1.7	Collection and use of personal information for marketing purposes	② Item name changed
3.2.3	Limitation to display of personal information and protective measures when using it	-	-	⑤ Deleted
3.2.4	Protecting users' access to terminals	3.2.3	Protecting users' access to terminals	② Item name changed
-	-	3.2.5	Processing pseudonymized information	① Partial transfer of detailed inspection items of item 3.2.3 ③ Improved certification standards by reflecting amendments to the Enforcement Decree ④ Newly inserted
3.3.2	Notifying data subjects due to the outsourcing of work	3.3.2	Outsourcing of personal information processing	② Item name changed ③ Improved certification standards by reflecting

ISMS-P control items				Details of the change
Before		After		
				amendments to the Enforcement Decree
3.3.3	Transfer of personal information due to transfer of business, etc.	3.3.3	Transfer of personal information due to transfer of business, etc.	② Item name changed
3.3.4	Cross-border transfer of personal information	3.3.4	Cross-border transfer of personal information	② Item name changed
3.4.1	Destroying personal information	3.4.1	Destroying personal information	② Item name changed
3.4.3	Managing dormant users	-	-	⑤ Deleted
3.5.1	Disclosure of the privacy policy	3.5.1	Disclosure of the privacy policy	② Item name changed
3.5.3	Notification of use history	3.5.3	Notification to the data subject	② Item name changed ③ Improved certification standards by reflecting amendments to the Enforcement Decree

Source: Personal Information Protection Commission notice No. 2023-8, October 5, 2023, and Ministry of Science and ICT notice No. 2023-33, October 5, 2023, partial amendment

■ Preparations for ISMS-P control items

Let's look at what needs to be prepared according to the notified ISMS-P control items. First, it is necessary to revise the privacy policy and establish guidelines related to personal information. And you must check changes in existing control items and make preparations tailored to each company's system environment. Among the five criteria for changes in <Table 4> presented above, the details and preparations for each control item for the three criteria (transfer, improvement and new insertion), excluding ② item name changed and ⑤ deleted, are as follows:

<Table 5> Preparations for ISMS-P revision items

Control item		Details	Preparations for ISMS-P audit (evidence)
2.4.7	Work environment security	Establishing and implementing protection measures to prevent personal information and important information from being exposed or leaked to unauthorized persons through shared office equipment and personal work environments.	1) Status of protection measures for printouts and copies
2.6.3	Access to application programs	Limiting application program access rights according to each user's tasks and importance of access information, and establishing and applying standards to minimize exposure of unnecessary information	1) Masking personal information in the screen
3.1.1	Collection and use of personal information	Personal information must be collected and used legally and fairly, and the consent of the data subject must be obtained in a legal manner when collecting it based on the consent of the data subject. When collecting personal information of a child under the age of 14, consent from the legal representative must be obtained and confirmation of whether the legal representative has given consent is required.	1) Establishing guidelines for notification of use and provision details in accordance with legal standards 2) Notification results in the use and provision details 3) Privacy Policy
3.1.2	Limitation to collection of personal information	When collecting personal information, only the minimum amount of personal information necessary for the purpose of processing must be collected. The provision of goods or services to the data subject should not be refused on the grounds that the data subject does not agree to matters to which the data subject can selectively consent.	1) Privacy Policy
3.1.5	Indirect collection of personal information	When collecting personal information from someone other than the data subject or receiving it from a third party , the minimum amount of personal information necessary for the job must be collected or provided. Based on law or upon request from the data subject, the source of collection, purpose of	1) Privacy Policy

Control item		Details	Preparations for ISMS-P audit (evidence)
		processing, and right to request suspension of processing must be notified.	
3.1.6	Installation and operation of visual data processing devices	When installing and operating fixed visual data processing devices in a public place or operating mobile visual data processing devices in a public place for business purposes , legal requirements must be complied with and appropriate protection measures must be established and implemented depending on the purpose and location of installation.	1) Revising guidelines related to visual data processing devices 2) Privacy Policy
3.2.5	Pseudonym information processing	When processing pseudonymized information, legal requirements such as purpose restrictions, combination restrictions, safety measures, and prohibition obligations must be complied with, and pseudonymization procedures must be established and implemented to ensure an appropriate level of pseudonymization.	1) Pseudonymized information processing procedures and results 2) Results of pseudonymization (when using pseudonymized information) 3) Privacy Policy (Matters regarding the use and provision of pseudonymized information)
3.3.2	Outsourcing personal information processing	When outsourcing personal information processing to a third party, the details of the outsourced work and information related to the outsourcee, etc. must be disclosed, and when outsourcing work that promotes or recommends sales of goods or services, the details of the outsourced work and the outsourcee must be disclosed to the data subject.	1) Revising provisions and guidelines related to third party outsourcing 2) Privacy Policy
3.5.3	Notification to data subjects	Matters that need to be notified to the data subject, such as the details of use and provision of personal information, must be identified, and the contents must be notified periodically.	1) Establishing guidelines for notification of use and provision details in accordance with legal standards 2) Notification results in the use and provision details 3) Privacy Policy

* There are no detailed instructions related to the changed ISMS-P notice. So there may be some additions and changes.

Source: Personal Information Protection Commission notice No. 2023-8, October 5, 2023, and Ministry of Science and ICT notice No. 2023-33, October 5, 2023, partial amendment

■ Conclusion



According to this revision of the Personal Information Protection Act, companies maintaining ISMS–P certification audits or preparing to newly introduce it should make preparations after checking the previously introduced amendments. In particular, preparations must be made for major amendments, such as collection and use of personal information, limitation to collection of personal information, indirect collection of personal information, installation and operation of visual data processing devices, processing of pseudonymized information, outsourcing of personal information processing t, and notification items to data subjects.

Specifically, in order to prepare for the ISMS–P audit after the revision, In addition to revising the personal information processing policy, it is necessary to establish personal information–related guidelines for collection and use of personal information, installation and operation of visual data processing devices, outsourcing of personal information processing, and notification to data subjects. Public institutions need additional inspections as additional defects may be identified in accordance with the strengthened ‘Notice of standards for ensuring the safety of personal information’.

SK Shieldus supports the revision of privacy policies, establishment of guidelines, and inspection of possible defects necessary for ISMS-P audits based on the highest level of professional manpower. In addition, it provides a variety of customized consulting services that take into account each company's environment, including personal information protection consulting, compliance consulting, information protection management system consulting, mock hacking consulting, development security consulting, and comprehensive information security consulting.

We hope that you can respond effectively and systematically to continuously changing compliance through SK Shieldus' consulting services. For more information, please see [the official blog of SK Shieldus](#).

■ References

1. National Law Information Center, <https://www.law.go.kr/>
 - Personal Information Protection Act [enforced on September 15, 2023] [Law No. 19234, March 14, 2023, partial amendment]
 - Personal Information Protection Act Enforcement Decree [enforced on September 15, 2023] [Presidential Decree No. 33723, September 12, 2023, partial amendment]
2. Personal Information Protection Commission, <https://www.pipc.go.kr/np/>
 - Standards for ensuring the safety of personal information [enforced on September 22, 2023] [Personal Information Protection Commission notice No.2023-6, September 22, 2023, partial amendment]
 - Notice on information protection and personal information protection management system certification, etc. [Personal Information Protection Commission notice No.2023-8, October 5, 2023, partial amendment], [Ministry of Science and ICT notice No.2023-33, October 5, 2023, partial amendment]
3. KISA, information protection and personal information management system <https://isms.kisa.or.kr/main/>
4. 2023 information security & personal information protection conference–reference (title: Major amendments to the Personal Information Protection Act)