

의안번호	제 호	의결사항
의결 연월일	20 . . (제 회)	

개인정보보호법시행령
일부개정령안

제출자	국무총리 (개인정보보호위원회 소관)
제출 연월일	20 . .

법제처 심사 전

1. 의결주문

개인정보 보호법 시행령 일부개정령안을 별지와 같이 의결한다.

2. 제안이유

「개인정보 보호법」 제32조의2에 따른 ‘개인정보 보호 인증(이하, ISM S-P 인증)’ 심사기준 및 방법 등을 구체화하여 개인정보 보호 제고에 기여하려는 것임.

3. 주요내용

가. 인증 기준 및 방법(안 제34조의2)

- 1) 법 제32조의2제1항에 따른 개인정보 보호 인증 기준 및 방법 구체화하여, 현장심사를 병행하고 개인정보 처리규모, 사회적 파급력 등을 고려하여 인증심사 기준을 차등하여 적용하도록 함
- 2) 국민 생활 파급력이 큰 대규모 기업, 침해·유출사고 발생 기업 등에 한정하여 일정 이상의 기술자격을 보유한 자가 취약점 점검을 수행할 수 있도록 함

나. 인증의 사후관리(안 제34조의5)

- 법 제32조의2제4항에 따른 사후관리 심사 방법 및 기준 구체화하여 현장심사를 병행하고, 기술인력의 취약점 점검을 사후심사 시에도 적용하도록 함

다. 과태료 부과기준 정비(안 제63조 별표2)

- ISMS-P 인증 의무대상자가 보유 중인 인증이 취소된 경우, 재발방지 대책을 수립하고 새로운 인증을 재취득할 수 있는 기간 부여 필요성을 반영하여 과태료 부과를 1년간 유예하도록 함

4. 주요토의과제

없 음

5. 참고사항

가. 관계법령 : 생 략

나. 예산조치 : 별도조치 필요 없음

다. 기 타 : 1) 신·구조문대비표, 별첨

2) 입법예고(2026. 9. 16. ~ 10. 26.)

개인정보 보호법 시행령 일부개정령안

개인정보 보호법 시행령 일부를 다음과 같이 개정한다.

제34조의2제1항에 후단을 다음과 같이 신설한다.

이때, 법 제32조의2제1항에 따른 인증을 받으려는 자의 개인정보 처리 규모, 사회적 파급력 등을 고려하여 인증의 기준을 차등하여 적용할 수 있다.

제34조의2제4항 중 “서면심사 또는 현장심사의 방법으로”를 “서면심사와 현장심사의 방법을 병행하여”로 하고, 같은 항에 단서를 다음과 같이 신설한다.

다만, 다음 각 호의 어느 하나에 해당하는 자에 대하여 현장심사를 실시하는 경우 「정보보호산업의 진흥에 관한 법률 시행규칙」 별표 1에 따른 중급 이상의 자격기준을 갖춘 기술인력이 취약점 점검을 수행할 수 있다.

제34조의2제4항에 각 호를 다음과 같이 신설한다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제49조의2제3항 각 호의 어느 하나에 해당하는 자로서 법 제32조의2제1항에 따른 인증을 받으려는 자
2. 법 제32조의2에 따른 인증을 받은 자로서 인증의 유효기간 내 「정

보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제7호
에 따른 침해사고가 발생한 자

3. 법 제32조의2에 따른 인증을 받은 자로서 인증의 유효기간 내 법 제
34조에 따른 유출등을 신고한 자

제34조의5제1항 중 “서면심사 또는 현장심사의 방법으로”를 “서면심사
와 현장심사의 방법을 병행하여”로 하고, 같은 항에 후단을 다음과 같이
신설한다.

이 경우 제34조의2제4항 단서 및 각 호는 사후관리 심사에 준용된다.
별표 2 제1호에 마목을 다음과 같이 신설한다.

마. 부과권자는 법 제32조의2제1항 단서에 해당하는 자가 법 제32조
의2제3항제2호 내지 제4호에 따라 인증이 취소된 경우에는 그 인
증이 취소된 날로부터 1년이 되는 날까지 법 제75조제2항제15호
에 따른 과태료를 부과하지 아니한다.

부 칙

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 별표 2 제1호마
목의 개정규정은 2027년 7월 1일부터 시행한다.

제2조(과태료에 관한 경과조치) 이 영 시행 전의 행위에 대한 과태료
의 적용은 종전의 규정에 따른다.

신·구조문대비표

현 행	개 정 안
제34조의2(개인정보 보호 인증의 기준·방법·절차 등) ① 보호위원회는 제30조제1항 각 호의 사항을 고려하여 개인정보 보호의 관리적·기술적·물리적 보호대책의 수립 등을 포함한 법 제32조의2제1항에 따른 인증의 기준을 정하여 고시한다. <후단 신설>	제34조의2(개인정보 보호 인증의 기준·방법·절차 등) ① ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- <u>. 이때,</u> <u>법 제32조의2제1항에 따른 인증을 받으려는 자의 개인정보 처리규모, 사회적 파급력 등을 고려하여 인증의 기준을 차등하여 적용할 수 있다.</u>
②·③ (생략)	②·③ (현행과 같음)
④ 법 제32조의2제1항에 따른 개인정보 보호 인증심사는 제34조의8에 따른 개인정보 보호 인증심사원이 <u>서면심사 또는 현장심사의 방법으로 실시한다. <단 서 신설></u>	④ ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- <u>서면심사와 현장심사의 방법을 병행하여 --. 다만,</u> <u>다음 각 호의 어느 하나에 해당하는 자에 대하여 현장심사를 실시하는 경우 「정보보호산업의 진흥에 관한 법률 시행규칙」 별표 1에 따른 중급 이상</u>

<신 설>

<신 설>

<신 설>

⑤・⑥ (생 략)

제34조의5(인증의 사후관리) ①
법 제32조의2제4항에 따른 사후
관리 심사는 서면심사 또는 현
장심사의 방법으로 실시한다.

<후단 신설>

의 자격기준을 갖춘 기술인력이
취약점 점검을 수행할 수 있다.

1. 「정보통신망 이용촉진 및
정보보호 등에 관한 법률 시
행령」 제49조의2제3항 각 호
의 어느 하나에 해당하는 자
로서 법 제32조의2제1항에 따
른 인증을 받으려는 자

2. 법 제32조의2에 따른 인증을
받은 자로서 인증의 유효기간
내 「정보통신망 이용촉진 및
정보보호 등에 관한 법률」
제2조제1항제7호에 따른 침해
사고가 발생한 자

3. 법 제32조의2에 따른 인증을
받은 자로서 인증의 유효기간
내 법 제34조에 따른 유출등
을 신고한 자

⑤・⑥ (현행과 같음)

제34조의5(인증의 사후관리) ① -

----- 서면심사와 현장심
사의 방법을 병행하여 -----.
이 경우 제34조의2제4항 단서
및 각 호는 사후관리 심사에 준
용된다.

② (생 략)	② (현행과 같음)
---------	------------

〈 의안 소관 부서명 〉

개인정보보호위원회 자율보호정책과	
연 락 처	(02) 2100 - 3084