



제438회국회(임시회)
제2차 정무위원회

개인정보 보호법 일부개정법률안

검 토 보 고

〈 개인정보보호 중심 설계(PbD) 인증 제도 법제화〉
■ 김승원의원 대표발의(의안번호 제2218704호)

2026. 8.

정 무 위 원 회
수석전문위원 곽현준

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	3

I. 제안경위

1. 제 안 자: 김승원의원 등 10인
2. 제 안 일: 2026. 4. 29.
3. 회 부 일: 2026. 4. 30.

II. 제안이유 및 주요내용

최근 디지털 기술의 발전에 따라 네트워크 카메라, 로봇 청소기, 지문·안면인식 도어락, 스마트 가전 등과 같은 개인정보 처리 기능이 있는 제품이 국민 일상 생활에 널리 활용되고 있으나, 그러한 제품에 개인정보 보호 요소가 충분히 반영되어 있는지 여부를 검증할 수 있는 체계가 부족하여, 우수 제품 등의 개발과 소비자의 선택이 제한되고 있는 상황임.

이에 보호위원회는 개인정보 처리 기능이 있는 제품(하드웨어 및 소프트웨어를 포함한다. 이하 같다)이 이 법에 따른 개인정보 보호 원칙과 정보주체의 권리 보장 등을 고려하여 설계되었는지 등에 관하여 인증할 수 있도록 하고, 인증 운영에 필요한 심사 절차, 사후관리, 인증 제품의 보급 촉진 등에 관한 사항을 규율함으로써 제조사의 자발

적 노력과 소비자의 관심을 유도하는 한편, 관련 제품의 경쟁력 강화를 지원하고자 함(안 제32조의3 신설 등).

Ⅲ. 검토의견

□ 개정안은 개인정보보호위원회가 개인정보 처리 기능이 있는 제품이 개인정보 보호 원칙과 정보주체의 권리 보장을 고려하여 설계되었는지 등에 관하여 인증할 수 있도록 하고, 인증의 유효기간, 인증취소 요건, 인증시험대행기관, 인증기준과 절차 등 인증제도 운영에 필요한 사항을 규정하려는 것임(안 제32조의3 신설).

○ 또한 인증 업무에 종사하거나 종사하였던 자에 대한 비밀유지의무를 신설하고, 인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한 자에 대하여 과태료를 부과할 수 있도록 함(안 제60조제3의2호, 제75조제2항제15의2호 신설).

현행	개정안
<신설>	제32조의3(개인정보 보호 중심 설계 인증) ① 보호위원회는 개인정보 처리 기능이 있는 제품(하드웨어 및 소프트웨어를 포함한다. 이하 같다)이 이 법에 따른 개인정보 보호 원칙과 정보주체의 권리 보장을 고려하여 설계되었는지 등에 관하여 인증할 수 있다. ② 제1항에 따른 인증의 유효기간은 인증을 받은 날로부터 3년으로 하되, 대통령령으로 정하는 바에 따라 그 기간을 연장할 수 있다.

현행	개정안
	③ 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령으로 정하는 바에 따라 제1항에 따른 인증을 취소할 수 있다. 다만, 제1항에 해당하는 경우에는 취소하여야 한다. 1. 거짓이나 그 밖의 부정한 방법으로 인증을 받은 경우 2. 인증의 전제나 근거가 되는 중대한 사실이 변경된 경우 3. 제4항에 따른 사후관리를 거부 또는 방해한 경우 4. 제11항에 따른 인증기준에 미달하게 된 경우 5. 개인정보 보호 관련 법령을 위반하고 그 위반 사유가 중대한 경우 ④ 보호위원회는 제1항에 따른 인증의 실효성 유지를 위하여 연 1회 이상 사후관리를 실시하여야 한다. ⑤ 보호위원회는 제1항에 따른 제품이 제11항에 따른 인증기준에 적합한지 여부를 확인하는 시험을 효율적으로 수행하기 위하여 필요한 경우에는 대통령령으로 정하는 지정기준을 충족하는 기관을 인증시험대행기관으로 지정할 수 있다. ⑥ 보호위원회는 제5항에 따라 지정된 인증시험대행기관이 다음 각 호의 어느 하나에 해당하면 지정을 취소

현행	개정안
	<u>할 수 있다. 다만, 제1호에 해당하는 경우에는 그 지정을 취소하여야 한다.</u> <u>1. 거짓이나 그 밖의 부정한 방법으로 지정을 받은 경우</u> <u>2. 제5항에 따른 지정기준에 미달하게 된 경우</u> <u>⑦ 보호위원회는 제1항에 따른 인증을 받고자 하는 제품이 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의6에 따른 정보통신망연결기기등에 관한 인증을 이미 받은 경우에는 제11항에 따른 인증기준 중 일부 항목에 대하여 심사를 면제할 수 있다. 이 경우 인증심사의 세부 면제 범위에 대하여는 보호위원회가 정하여 고시한다.</u> <u>⑧ 보호위원회는 제1항에 따른 인증을 받은 제품의 보급을 촉진하기 위하여 공공기관 등에게 우선 구매하도록 요청하는 등 대통령령으로 정하는 바에 따라 필요한 지원을 할 수 있다.</u> <u>⑨ 제1항에 따른 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.</u> <u>⑩ 보호위원회는 대통령령으로 정하는 전문기관으로 하여금 제1항에 따른 인증, 제4항에 따른 사후관리, 제</u>

현행	개정안
제60조(비밀유지 등) 다음 각 호의 업무에 종사하거나 종사하였던 자는 직무상 알게 된 비밀을 다른 사람에게 누설하거나 직무상 목적 외의 용도로 이용하여서는 아니 된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다. 1. ~ 3. (생략) <u><신설></u> 4. ~ 6. (생략) 제75조(과태료) ① (생략) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다. 1. ~ 15. (생략) <u><신설></u> 16. ~ 27. (생략) ③ ~ ⑤ (생략)	5항에 따른 인증시험대행기관 지정, 제6항에 따른 인증시험대행기관 지정 취소 등에 관한 업무를 수행하게 할 수 있다. ⑪ 그 밖에 인증기준과 절차, 취소 기준 등에 관하여 필요한 사항은 대통령령으로 정한다. 제60조(비밀유지 등) ----- ----- ----- ----- ----- ----- 1. ~ 3. (현행과 같음) 3의2. 제32조의3에 따른 개인정보 보호 중심 설계 인증 업무 4. ~ 6. (현행과 같음) 제75조(과태료) ① (현행과 같음) ② ----- ----- ----- 1. ~ 15. (현행과 같음) 15의2. 제32조의3제9항을 위반하여 인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한 자 16. ~ 27. (현행과 같음) ③ ~ ⑤ (현행과 같음)

□ 개인정보보호위원회(이하 “보호위원회”라 함)는 가정용 CCTV, 로봇청소기 등 개인정보 처리 기능이 있는 제품들의 안전성을 확보하고 제조사의 책임과 소비자의 선택권을 강화하기 위해 2023년부터 ‘개인정보 보호 중심 설계(Privacy by Design¹⁾, 이하 “PbD”라 함)’ 인증을 시범 운영하고 있음.

○ 이는 개인정보 보호를 기술이나 서비스 설계의 초기 단계부터 내재화하려는 접근 방식으로, PbD 인증항목은 4개 유형의 총 71개 항목으로 구성되어 있음.

< PbD 인증 기준 >

인증 영역	인증 항목	비고
I. 기본적인 요구 사항	▶ 개인정보 식별 및 목적, 개인정보 처리 흐름, 개인정보 처리의 주체 식별, 불필요한 개인정보 전달 방지, 개인정보 위험 식별 및 개인정보보호 통제의 이행, 사용자가 구성 가능한 설정 및 기본 설정의 안전한 변경 등	14개
II. 개인정보 처리의 적법성	▶ 아동 등 개인정보 처리에 대한 동의, 마케팅 목적의 개인정보 처리에 대한 동의, 개인위치정보 처리에 대한 동의, 민감정보와 고유식별정보 처리의 적합성, 정보주체 이외로부터 개인정보 수집의 제한, 개인정보의 이용 및 제공의 제한, 개인정보의 파기, 개인정보 처리의 투명성 보장, 개인정보의 처리 정지 및 동의 철회 요구에 대한 권리 보장, 개인정보의 전송 요구에 대한 권리 보장, 완전히 자동화된 개인정보 처리 요구에 대한 권리 보장 등	28개

1) Privacy by Design : 제품 또는 서비스의 기획, 제조, 폐기 등 전 과정에서 개인정보 보호 요소를 충분히 고려함으로써 개인정보 침해를 사전에 예방하는 설계 개념

III. 정보보안 및 프라이버시 강화	▶ 안전한 인증정보 사용, 사용자 인증 및 권한 관리, 반복된 인증 시도 제한, 안전한 암호 알고리즘 사용, 안전한 업데이트 수행, 정보 노출 방지, 중요정보 완전 삭제, 원격 접속 통제, 프라이버시 강화 기술의 적용 등	22개
IV. 조직적 보호 조치	▶ 개인정보 처리방침의 문서화 및 관리, 개인정보의 안전성 확보, 개인정보보호 책임자 임명, 개인정보보호 준수 의무 및 교육 보장, 개인정보 사고 대응 및 소비자와 의사소통 등	7개
합계		71개

주) 제품별 기능이나 처리하는 개인정보의 특성 등에 따라 인증항목 차등 적용
 자료: 개인정보보호위원회

- 2023년부터 2025년까지 가정용 CCTV 등 총 7개 제품이 인증을 받았으며, 2026년에는 일상에서 사용되는 IT 제품뿐만 아니라 중소기업 등이 업무상 사용하는 솔루션(셀러 톨, 고객관리 S/W, 보안솔루션 등) 분야까지 확대하여 운영할 계획임.

< 2023년~2025년 PbD 인증 제품 현황 >

구분	PbD 인증제품(제조사)	인증마크
2023년	가정용 CCTV (SK쉴더스(주))	
2024년	개인영상정보 비식별화 시스템 ((주)엔트랩), 로봇청소기 (삼성전자(주)), 스마트 경로당 키오스크 ((주)블록오디세이)	
2025년	홈 카메라 ((주)트루엔), 가정용 로봇 (삼성전자(주)), 로봇청소기 (엘지전자(주))	

자료: 개인정보보호위원회

- 개정안은 PbD 인증 제도를 법제화하려는 것으로, 최근 기술 발전에 따라 개인정보 처리 기능이 있는 다양한 디지털 제품이 일상에서 널리 활용되고 있는 상황에서 PbD 인증을 통해 제품의 개인정보보호 수준

을 높여 국민이 안심하고 인증된 제품을 구매·이용할 수 있는 환경을 조성하는 데 기여할 것으로 기대됨.

- 또한 개인정보보호 요소가 제품 설계 단계부터 고려되는 문화를 확산시킴으로써 개인정보 침해를 사전에 예방하고, 기업의 자율적인 개인정보보호 수준 향상에 기여할 것으로 보임.

□ 다만, 현재 과학기술정보통신부가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의6²⁾에 근거하여 시행하고 있는 정보통신망 연결기기 등 정보보호인증(“IoT 보안인증”이라 함) 제도와 인증대상 및 인증기준에서 유사·중복되는 측면이 있어 이에 대한 검토가 필요할 것으로 보임.

2) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제48조의6(정보통신망연결기기등에 관한 인증) ① 과학기술정보통신부장관은 제4항에 따른 인증시험대행기관의 시험 결과 정보통신망연결기기등이 제2항에 따른 인증기준에 적합한 경우 정보보호인증을 할 수 있다.

② 과학기술정보통신부장관은 제1항에 따른 정보보호인증(이하 “정보보호인증”이라 한다)을 위하여 정보통신망의 안정성 및 정보의 신뢰성 확보 등에 관한 인증기준을 정하여 고시할 수 있다.

③ 과학기술정보통신부장관은 정보보호인증을 받은 자가 다음 각 호의 어느 하나에 해당하는 경우에는 그 정보보호인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 그 정보보호인증을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 정보보호인증을 받은 경우
2. 제2항에 따른 인증기준에 미달하게 된 경우

④ 과학기술정보통신부장관은 정보통신망연결기기등이 제2항에 따른 인증기준에 적합한지 여부를 확인하는 시험을 효율적으로 수행하기 위하여 필요한 경우에는 대통령령으로 정하는 지정기준을 충족하는 기관을 인증시험대행기관으로 지정할 수 있다.

⑤ 과학기술정보통신부장관은 제4항에 따라 지정된 인증시험대행기관(이하 “인증시험대행기관”이라 한다)이 다음 각 호의 어느 하나에 해당하면 인증시험대행기관의 지정을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 그 지정을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 지정을 받은 경우
2. 제4항에 따른 지정기준에 미달하게 된 경우

⑥ 과학기술정보통신부장관은 정보보호인증 및 정보보호인증 취소에 관한 업무를 한국인터넷진흥원에 위탁할 수 있다.

⑦ 정보보호인증·정보보호인증 취소의 절차 및 인증시험대행기관의 지정·지정취소의 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

○ IoT 보안인증의 인증대상인 ‘정보통신망연결기기등’은 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 ‘침해사고가 발생했거나 발생할 가능성이 큰 기기·설비·장비’ 또는 ‘침해사고가 발생할 경우 정보통신망의 안정성 및 정보의 신뢰성 확보에 중대한 위험성을 가져오는 기기·설비·장비’로,³⁾

가전·자동차·금융·의료·주택·통신 등 각 분야에서 개인정보 처리 기능이 있는 기기들이 상당하여 이들 기기는 대부분 PbD 인증의 대상이 될 것으로 보임.

< 분야별 정보통신망연결기기등 >

- | |
|--|
| 1. 가전 분야: 스마트 홈네트워크에 연결되는 멀티미디어 제품, 주방가전 제품 또는 생활가전 제품 등의 가전제품 또는 그 제품에 사용되는 기기·설비·장비 |
| 2. 교통 분야: 다음 각 목의 제품 등에 사용되는 기기·설비·장비
가. 「국가통합교통체계효율화법」 제2조제16호에 따른 지능형교통체계
나. 「드론 활용의 촉진 및 기반조성에 관한 법률」 제2조제1호에 따른 드론
다. 「자동차관리법」 제2조제1호에 따른 자동차
라. 「선박법」 제1조의2제1항에 따른 선박 |
| 3. 금융 분야: 「전자금융거래법」 제2조제8호에 따른 전자적 장치 |
| 4. 스마트도시 분야: 「스마트도시 조성 및 산업진흥 등에 관한 법률」 제2조제 |

3) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제45조(정보통신망의 안정성 확보 등) ① 다음 각 호의 어느 하나에 해당하는 자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.

1. 정보통신서비스 제공자
2. 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 대통령령으로 정하는 기기·설비·장비(이하 “정보통신망연결기기등”이라 한다)를 제조하거나 수입하는 자

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」

제36조의2(정보통신망연결기기 등의 범위) 법 제45조제1항제2호에서 “대통령령으로 정하는 기기·설비·장비”란 별표 1의3에 따른 분야 중 어느 하나의 분야에 속하는 기기·설비·장비로서 다음 각 호의 기기·설비·장비(이하 “정보통신망연결기기등”이라 한다)를 말한다.

1. 침해사고가 발생했거나 발생할 가능성이 큰 기기·설비·장비
2. 침해사고가 발생할 경우 정보통신망의 안정성 및 정보의 신뢰성 확보에 중대한 위험성을 가져오는 기기·설비·장비

- 2호에 따른 스마트도시서비스에 사용되는 기기·설비·장비
5. 의료 분야: 「의료기기법」 제2조제1항에 따른 의료기기 중 통신기능을 보유한 기기·설비·장비
 6. 제조·생산 분야: 제품의 제조·생산 또는 용역을 관리하기 위하여 제어·점검·측정·탐지 등의 용도로 사용되는 기기·설비·장비
 7. 주택 분야: 「건축법」 제2조제1항제4호에 따른 건축설비 중 지능형 홈네트워킹에 연결되는 기기·설비·장비
 8. 통신 분야: 「전파법」 제2조제16호에 따른 방송통신기자재 중 무선 또는 유선으로 통신이 가능한 방송통신기자재

자료: 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 [별표 1의3]

○ 또한, IoT 보안인증을 받기 위해서는 식별 및 인증, 데이터 보호, 암호, 소프트웨어 보안, 업데이트 및 기술지원, 운영체제 및 네트워크 보안, 하드웨어 보안 등 7개 영역의 인증기준을 충족해야 하는데, 인증항목 중 21개가 PbD 인증항목과 동일함.

<IoT 보안인증 기준 중 PbD 인증과 동일한 인증항목>

인증 영역	인증 항목	비고
식별 및 인증	<u>안전한 인증정보 사용, 사용자 인증 및 권한 관리,</u> <u>비인가 상호인증 제한, 반복된 인증시도 제한,</u> <u>정보노출 방지, 안전한 세션 관리</u>	6개
데이터 보호	<u>전송 데이터 보호, 저장 데이터 보호,</u> 중요정보 저장 영역 보호강화, 개인정보 법적 준거성, <u>중요정보 완전삭제</u>	5개
암호	<u>안전한 암호 알고리즘 사용, 안전한 암호키 생성,</u> 안전한 암호키 관리, 안전한 난수 생성	4개
소프트웨어 보안	시큐어 코딩, <u>소스코드 난독화,</u> 소프트웨어 보안기능 시험, <u>알려진 취약점 조치,</u> 불필요한 기능 및 코드 제거, 안전한 소프트웨어 적용, <u>감사기록</u>	7개

업데이트 및 기술지원	<u>모델명 및 제품정보 확인, 안전한 업데이트 수행,</u> 업데이트 파일의 안전성 보장, 업데이트 실패 시 복구, 업데이트 기술 지원, 업데이트 정보 제공, 자동업데이트 기능 제공	7개
운영체제 및 네트워크 보안	안전한 운영체제 적용, <u>불필요한 계정 통제,</u> <u>불필요한 서비스 및 포트 통제,</u> 불필요한 네트워크 인터페이스 비활성화, 실행코드 및 설정파일 무결성 검증, 장애 시 시스템 복원, 서비스 거부 공격 대응, 운영체제 기능 보호, 접근권한 최소화, 비인가 소프트웨어 설치·실행차단, <u>원격접속 통제,</u> 네트워크 트래픽 통제	12개
하드웨어 보안	안전한 부팅 및 자체시험, 자체시험 실패 시 대응, 하드웨어 장애 대응, 무단 훼손 방어, 부채널 공격 대응, 메모리 공격 대응, 비휘발성 메모리 보호, <u>외부 인터페이스 보호,</u> <u>내부 인터페이스 보호</u>	9개
합계		50개

주) 동일 인증항목은 볼드체 및 밑줄로 표시
자료: 개인정보보호위원회 제출자료를 바탕으로 작성성

○ 이와 같이 유사한 인증항목을 포함하고 있는 IoT 보안인증과 PbD 인증이 별도로 운영될 경우, 기업 입장에서는 각 인증의 적용 대상과 요구사항의 차이를 명확히 이해하기 어려워 인증 취득 과정에서 혼선이 발생할 가능성이 있고, 특히 동일한 조치에 대하여 서로 다른 방식의 증빙이나 평가를 요구하는 경우 인증 준비에 추가적인 부담이 발생할 수도 있음.⁴⁾

○ 개정안은 이러한 문제를 완화하기 위해 IoT 보안인증을 이미 받은

4) IoT 보안인증은 제품의 보안성 확보를, PbD 인증은 개인정보 보호체계 구축을 각각 목적으로 하는 제도라는 점에서 동일한 인증항목이라 하더라도 평가범위 및 심사관점에는 차이가 있을 수 있음.

경우 PbD 인증기준 중 일부 항목의 심사를 면제할 수 있도록 규정하고 있는데,⁵⁾ 중복되는 인증항목에 대한 반복적인 심사를 최소화하여 기업의 부담을 완화하고 인증제도 운영의 효율성을 높이기 위하여 필요한 조치로 판단됨.

- 그런데, 개정안은 심사 면제의 세부 범위를 보호위원회 고시에 위임하고 있어 실제 부담 완화 효과는 향후 마련될 면제 범위에 따라 달라질 수 있으므로, 인증항목의 범위와 실질적 동일성을 충분히 고려하여 면제 범위 또는 심사절차 간소화 방안 등을 마련함으로써 기업의 부담과 혼선을 최소화할 필요가 있을 것으로 보임.⁶⁾

또한, PbD 인증 신설로 인한 기업들의 인증 관련 비용과 시간 등의 절감을 위해서는 장기적으로 IoT 보안인증과 통합하여 하나의 인증 제도로 시행하는 방안 또한 모색할 필요가 있을 것으로 보임.⁷⁾

- 다음, 개정안은 PbD 인증 업무에 종사하거나 종사하였던 자에 대한 비밀유지의무를 신설하고, 인증을 받지 아니하였음에도 거짓으로 인증의

5) 제32조의3(개인정보 보호 중심 설계 인증) ⑦ 보호위원회는 제1항에 따른 인증을 받고자 하는 제품이 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의6에 따른 정보통신망연결기기등에 관한 인증을 이미 받은 경우에는 제11항에 따른 인증기준 중 일부 항목에 대하여 심사를 면제할 수 있다. 이 경우 인증심사의 세부 면제 범위에 대하여는 보호위원회가 정하여 고시한다.

6) 이에 대해 보호위원회는 '22년~'23년 당초 PbD 인증 항목을 개발하는 과정에서 모든 IT제품은 정보보호 기능이 기본적으로 적용되어야 한다는 전문가 의견을 반영하여 각 인증의 공통적인 항목(21개)에 대해서는 아예 별도의 기준을 마련하기보다 기존의 인증기준을 준용하여 사업자의 부담을 최소화하였고, IoT 인증을 받은 제품이 PbD 인증을 신청하면 정보보안 부분은 기존 시험성적서만 제출토록 해서 별도의 비용부담이 없도록 할 계획이라고 설명하고 있음.

7) 정부는 중복 인증으로 인한 부담 완화가 필요하다는 업계의 의견을 고려하여 종전에 개별적으로 운영되던 '개인정보보호 관리체계 인증(PIMS)'과 '정보보호 관리체계 인증(ISMS)'을 하나로 통합한 '통합인증제도'인 '정보보호 및 개인정보보호 관리체계 인증'(ISMS-P : Personal information & Information Security Management System)을 2018년 11월 7일부터 시행한 바 있음.

내용을 표시하거나 홍보한 자에 대하여 과태료를 부과할 수 있도록 규정하고 있음.

- 인증심사 과정에서 제품의 설계·운영방식, 보안조치 등 기업의 영업상·기술상 정보가 제출될 수 있다는 점에서 인증 업무 종사자에게 비밀유지의무를 부과할 필요가 있고, 인증을 받지 않은 제품에 대해 인증을 받은 것처럼 표시하거나 홍보하는 행위는 소비자의 오인을 초래하고 인증제도에 대한 신뢰를 저해할 수 있다는 측면에서 이에 대한 제재규정을 마련하는 것은 타당하다고 보임.

- 한편, 개정안은 인증에 필요한 비용을 충당하기 위한 수수료 부과 근거는 별도로 두지 않고 있는데, 인증항목을 시험·평가하기 위한 최소 경비를 징수할 수 있는 근거를 마련할 필요가 있고, 국민의 권리·의무와 관련된 수수료 납부와 관련된 내용은 법률에 명시적으로 규정하는 것이 바람직하다는 점 및 유사 입법례⁸⁾를 감안하면, 인증기관이 인증 신청자에게 수수료를 부과할 수 있도록 근거를 규정하는 방안⁹⁾에 대한 고려가 필요하다고 봄.

8) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조(정보보호 관리체계의 인증) ⑪ 제1항 및 제2항에 따른 인증의 방법·절차·범위·수수료, 제8항에 따른 사후관리의 방법·절차, 제10항에 따른 인증취소의 방법·절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

「건축법」 제65조의2(지능형건축물의 인증) ④ 국토교통부장관은 건축물을 구성하는 설비 및 각종 기술을 최적으로 통합하여 건축물의 생산성과 설비 운영의 효율성을 극대화할 수 있도록 다음 각 호의 사항을 포함하여 지능형건축물 인증기준을 고시한다.

1. 인증기준 및 절차
2. 인증표시 홍보기준
3. 유효기간
4. 수수료
5. 인증 등급 및 심사기준 등

□ 참고로, 개정안에 대한 관계 부처 및 이해관계자 의견은 다음과 같음.

- **보호위원회**는 국민 일상에서 활용되는 개인정보 처리 기기의 안전성을 강화하고, 제조사의 자발적 노력 유도 등을 위해 개인정보 보호 중심 설계 인증제 신설이 필요하다는 입장임.
- **과학기술정보통신부**는 PbD 인증은 기존 IoT 보안인증과 인증대상·기준이 유사하여⁹⁾ 기업에 혼선·추가적 부담으로 작용할 여지가 존재하므로, 기존 제도와의 정합성 확보 방안 마련 등 별도 법정 인증 신설 필요성에 대한 추가 검토가 우선되어야 한다는 의견을 제출함.
 - 이에 대해 **보호위원회**는 인증기준의 경우 취약점 조치 등 공통 항목이 일부 중복될 수 있으나, IoT 인증을 받은 기기는 관련 시험항목이 면제되어 기업의 추가 부담 우려는 낮다는 의견임.
- **국가사이버안보센터**는 공공기관에 도입하는 제품에 대해서는 보호위원회가 인증한 제품 중 국가정보원장이 안전성을 확인한 제품을 우선구매 지원 대상으로 하도록 요건을 강화할 필요가 있다는 입장임.¹⁰⁾

9) 시범인증으로 수행중인 PbD 인증 71개 항목 중 기술부분 21개는 IoT 보안인증과 동일하며, 나머지 50개의 경우에도 법률적·관리적 부분에 IoT 보안인증과 일부 중복성 존재

10) 「**사이버안보 업무규정**」

제9조(사이버보안 예방 조치 등) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협을 예방하기 위하여 중앙행정기관등의 장이 시행하는 정보화사업(「지능정보화 기본법」 제11조제1항에 따른 지능정보화계획에 따른 사업을 포함한다)에 대하여 보안성 검토를 실시하고, 그 보안성 검토 결과의 이행 여부를 확인할 수 있다.

② 국가정보원장은 중앙행정기관등의 정보보호시스템, 암호장치, 암호모듈 및 보안기능이 있는 정보통신기기(이하 “정보보호시스템등”이라 한다)의 도입·운영 및 「클라우드컴퓨팅 발전 및 이용자 보호에

- 이에 대해 **보호위원회**는 다른 법률에 특별한 규정이 있는 경우 해당 법률이 우선 적용되는 점 등을 고려할 때¹¹⁾ 개정안에 국가정보원의 안전성 확인에 관한 사항을 명시할 필요성은 낮으며, 다만 PbD 인증 제품 중 국가정보원의 안전성 확인이 필요한 제품이 있다면 해당 규정이 우선 적용됨을 명확히 안내하겠다는 입장임.

- **한국인터넷기업협회**는 기존 사전 적정성 검토 제도¹²⁾와 연계하거나 준용하여 기업과 행정청의 중복심사 부담을 최소화할 필요가 있고, 사후관리를 제품별 연 1회 이상 실시하는 것은 사실상 매년 인증을 갱신하는 것과 유사한 부담으로 작용할 수 있으며, 공공기관 우선 구매에 관하여는 법률에 규정하기보다 조달청의 예규, 구매지침, 납품 기준 등을 통해 반영하는 방식이 보다 적절하다는 의견을 제출함.

관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스(이하 이 조에서 “클라우드컴퓨팅서비스”라 한다)의 이용에 관한 보안대책을 수립할 수 있다.

③ 국가정보원장은 중앙행정기관등이 도입·운영하거나 이용하는 정보보호시스템등 및 클라우드컴퓨팅서비스가 제2항에 따른 보안대책에 적합한지 검증할 수 있다.

④ 국가정보원장은 정보보호시스템등을 직접 개발하여 중앙행정기관등에 보급할 수 있다.

⑤ 국가정보원장은 중앙행정기관등의 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템의 취약요소를 발굴·개선하기 위해 보안관리 수준을 측정할 수 있다. 이 경우 그 항목·절차·시기 등을 해당 중앙행정기관등의 장에게 미리 통보해야 한다.

⑥ 제5항에도 불구하고 제7조 각 호에 따른 기관 중 국가정보원장과 국방부장관이 협의하여 정하는 기관에 대해서는 국방부장관이 보안관리 수준을 측정한다. 이 경우 국가안보에 필요하다고 판단되거나 국가정보원장의 요청이 있는 경우에는 관련 내용을 국가정보원장에게 통보해야 한다.

11) 「개인정보 보호법」

제6조(다른 법률과의 관계) ① 개인정보의 처리 및 보호에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.

- 12) 사전 적정성 검토 제도: 신청인이 인공지능(AI) 등 신기술·신서비스 기획·개발 단계에서 기존 법해석·집행 선례만으로는 명확한 개인정보 보호법 준수방안을 찾기 어려운 경우, 보호위원회와 협력하여 신청 대상 신기술·신서비스 환경에 적합한 법 적용방안을 마련하고, 이를 신청인이 이행하면 사후에 불이익한 처분을 부과하지 않는 제도

- 이에 대해 **보호위원회**는 사전 적정성 검토 제품이 PbD 인증을 신청할 경우에는 기존 검토결과를 적극 참조하여 기업 부담을 최소화할 계획이고, 개정안 내용은 제품별 연 1회 사후관리가 아니라 보호위원회가 연 1회 이상 사후관리를 하도록 한 것으로 오해 소지가 있다면 이를 명확히 할 필요가 있으며, 법률에 명시적인 규정이 없으면 조달청 예규, 지침 등에 반영하는 것이 사실상 어려운 실정을 고려할 필요가 있다는 입장임.

문 의 처
02)6788-5108