

개인정보 보호법 시행령

<목 차>

- 1.개인정보 보호 인증 대상자의 범위
- 2.개인정보 보호 기본계획 수립을 위한 자료제출
- 3.개인정보 보호책임자 지정·변경·해제시 준수사항
이행대상자의 범위와 신고절차
- 4.개인정보 유출등 발생시 정보주체에게 통지하여야
하는 정보
- 5.정보주체에게 정보유출 가능성이 있음을 통지해야
하는 범위와 정보

소관부처 및 작성자 인적사항	소관부처	개인정보보호위원회	작성 자	이름	김지영
	담당부서 (과)	개인정보보호정책 과		직급	행정사무관
	국장	이상민		연락처	02-2100-3057
	과장	공석		이메일	kjy260529 @mail.go.kr

2026. 05. 27. 작성

정 책 책 임 자 직 위 : 국 장 성 명 : 이상민 (서 명)

< 규제 개요 >

기본 정보	1.규제사무명	개인정보 보호 인증 대상자의 범위		
	2.규제조문	개인정보 보호법 시행령 제34조의 9		
	3.위임법령	개인정보 보호법 제32조의 21항		
	4.유형	신설	5.입법예고	2026.06.02~2026.07.13
규제의 필요성	6.추진배경 및 정부개입 필요성	추진배경 - 정보보호 및 개인정보보호 관리체계 인증(ISMS-P 인증)은 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 개인정보 보호법에 부합하는지 등에 관하여 인증하는 제도로써, 보안수준 향상과 사고예방 등 목적으로 운영 중 - ISMS-P 인증의 긍정적 효과에도 불구하고 해당 인증 취득은 기관·기업의 자율에 맡겨져 있어, 대규모 개인정보 처리 등 핵심 인프라에 대한 관리체계의 공백 발생 우려 - 이에, 인증체계 강화 필요성에 대한 국민 공감대가 형성되었고 매출액, 개인정보의 처리 규모 등을 고려하여 일정 기준에 해당하는 개인정보처리자에 대해 ISMS-P 인증을 의무화하도록 개인정보 보호법을 개정('26.3.10. 공포, '27.7.1. 시행) 정부개입 필요성 - 매출액, 개인정보 처리 규모 등을 고려한 ISMS-P 인증 의무대상자의 범위를 시행령을 통해 정하도록 위임(개인정보 보호법 제32조의2제1항단서)하여, 이를 구체화하여 규정할 필요 - ISMS-P 인증이 기존 자율 취득에서 일부 의무 취득으로 변경되는 점, 의무화 시행에 따른 기관·기업 부담 및 혼선을 최소화하여 변경된 제도의 조기 정착을 제고할 필요성이 있는 점 등을 고려하여 정부의 합리적 기준 수립 필요		
	7.규제내용	개인정보의 특성·규모, 매출액 등을 고려하여 공공·민간 중요 개인정보처리시스템을 대상으로 ISMS-P 인증 의무화 추진(개인정보 보호법 시행령 제34조의9 신설) - 의무대상자는 크게 네 가지 범주로 구분되며, ①주요 공공시스템 운영기관, ②이동통신사업자, ③본인확인기관, ④매출액 및 처리하는 개인정보 수를 고려한 대규모 개인정보처리자가 이에 해당됨		
	8.피규제집단 및 이해관계자	신설한 개인정보 보호법 시행령 제34조의9 기준을 충족하는 공공·민간의 주요 개인정보처리		
	9.도입목표 및 기대효과	ISMS-P 인증 의무 대상자를 구체화하여 대규모 개인정보 처리 등 핵심 인프라에 대한 관리체계의 공백 발생을 예방하고, 중요 개인정		

		보처리시스템에 대한 상시적 개인정보 안전관리체계를 구축하여 국민의 개인정보 보호 수준 강화				
규제의 적정성	10.비용편익분석 (단위:백만원)		비용	편익	순비용	
		피규제자	562.34		562.34	
		피규제자 이외				
		정성분석				
		주요내용	증을 취득한 자는 인증받은 내용을 표시하거나 홍보할 수 있으므로(개인정보 보호법 제32조의2 제6항) 기관·기업 이미지 제고에 기여할 수 있음 － 아울러, 인증 취득 및 사후심사(매 1년 주기)를 통해 개인정보처리시스템·개인정보 처리 조치 등에 대한 일정 기준을 지속적으로 유지한다면, 해킹 등 개인정보 침해·유출 사고를 예방하는데 기여할 수 있고 해당 사고에 따른 과태료·과징금·소송 비용 등을 절감할 수 있음 － 개인정보 침해·유출 사고 등을 예방할 수 있다면 국민의 개인정보를 안전하게 보호하는 것은 물론 개인정보 보호에 대한 국민 신뢰도를 향상시킬 수 있으며, 민간 기업의 경우에는 해당 신뢰도를 바탕으로 매출액 증대를 기대할 수 있음 － 특히 본 시행령을 통한 의무대상자가 공공 및 민간의 주요·대규모 개인정보처리자임을 고려하면 비용 대비 편익이 월등히 높을 것으로 판단됨			
	11.영향평가 여부	기술영향평가		경쟁영향평가	중기영향평가	
		해당없음		해당없음	해당없음	
기타	12.규제일몰제	대분류	소분류			
		일몰설정 예외기준	1. 국제조약 등에 따라 동일하게 적용 되어야 하는 규제		미해당	
			2. 국가의 질서 유지 및 국민생명·안전과 직접 관련된 규제		미해당	
			3. 사회통념상 보편적으로 통용되는 규범적 성격의 규제		미해당	
		경제규제 여부기준	4. 국민과 기업의 경제활동에 대한 규제		미해당	
			5. 경제활동에 직접영향을 주는 규제		미해당	
		일몰설정 세부기준	6. 피규제자의 규제부담이 매우 큰 규제		미해당	
			7. 한시적 목적을 위한 규제이거나 주기적인 검토가 필요한 규제		해당	
		일몰설정여부		일몰조문		연장여부

		재검토행	제62조의의3		신규
		일몰유형	일몰설정기간		일몰주기
		재검토행	20270101~20291231		3
13.우선허용 · 사후 규제 적용여부	해당 없음				
14.비용감축제 (단위:백만원)	적용여부	비용	편익	연간균등순비용	
	미적용	562.34		614.08	
15.규제정비 계획	개인정보보호법시행령 제34조의9				

<조문 대비표>

현 행	개 정 안
	제34조의9(개인정보 보호 인증 대상자의 범위) 법 제32조의2제1항 단서에서 “매출액, 개인정보의 처리 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 다음 각 호의 어느 하나에 해당하는 자를 말한다. 1. 제30조의2에 따른 공공시스템운영기관 중 보호위원회가 정하여 고시하는 자 2. 「전파법」 제10조에 따라 주파수를 할당받아 이동통신서비스를 제공하는 자로서 정보주체와 이동통신서비스의 이용에 관한 계약을 체결한 자 3. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3제1항에 따른 본인확인기관 4. 다음 각 목을 모두 충족하는 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다. 가. 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 1조원

현 행	개 정 안
	이상이고 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 제2항제3호의 정보통신서비스 부문 전년도 매출액이 100억원 이상인 자 나. 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 국내 정보주체의 수가 일일평균 3,000만명 이상인 자(단, 임·직원 정보는 제외한다)
제62조의3(규제의 재검토) ① 보호위원회는 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 3년마다(매 3년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 해야 한다. 1. ~ 9. (생 략)	제62조의3(규제의 재검토) ① 보호위원회는 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 3년마다(매 3년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 해야 한다. 1. ~ 9. (생 략) 10. 제32조제2항, 제3항에 따른 개인정보 보호책임자 지정, 변경, 해제시 준수하여야 할 대상자의 범위와 신고절차 : 2027년 1월 1일 11. 제34조의9에 따른 개인정보 보호

현 행	개 정 안
	인증 대상자의 범위 : 2027년 1월 1일

I. 규제의 필요성 및 대안선택

1. 추진배경 및 정부개입 필요성

○ 추진 배경

- 정보보호 및 개인정보보호 관리체계 인증(ISMS-P 인증)은 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 개인정보 보호법에 부합하는지 등에 관하여 인증하는 제도로써, 보안수준 향상과 사고예방 등 목적으로 운영 중
- ISMS-P 인증의 긍정적 효과에도 불구하고 해당 인증 취득은 기관·기업의 자율에 맡겨져 있어, 대규모 개인정보 처리 등 핵심 인프라에 대한 관리체계의 공백 발생 우려
- 이에, 인증체계 강화 필요성에 대한 국민 공감대가 형성되었고 매출액, 개인정보의 처리 규모 등을 고려하여 일정 기준에 해당하는 개인정보처리자에 대해 ISMS-P 인증을 의무화하도록 개인정보 보호법을 개정('26.3.10. 공포, '27.7.1. 시행)

○ 정부개입 필요성

- 매출액, 개인정보 처리 규모 등을 고려한 ISMS-P 인증 의무대상자의 범위를 시행령을 통해 정하도록 위임(개인정보 보호법 제32조의2제1항단서)하여, 이를 구체화하여 규정할 필요
- ISMS-P 인증이 기존 자율 취득에서 일부 의무 취득으로 변경되는 점, 의무화 시행에 따른 기관·기업 부담 및 혼선을 최소화하여 변경된 제도의 조기 정착을 제고할 필요성이 있는 점 등을 고려하여 정부의 합리적 기준 수립 필요

2. 규제 대안 검토 및 선택

① 대안의 비교

○ 규제대안의 내용

규제대안1	대안명	ISMS-P 인증 의무화 시행
	내용	자율적으로 취득했던 ISMS-P 인증을 중요·대규모 개인정보를 처리하는 기관·기업 대상(4개 범주로 구

		분되며 상세 내용은 아래 설명 참조)으로 의무화하여 시행함
규제대안2	대안명	ISMS-P 인증 자율 취득
	내용	ISMS-P 인증 취득에 대한 결정을 기관·기업 등이 자율적으로 판단하여 수행함
규제대안3	대안명	ISMS-P 인증 의무화 시행 및 의무대상 축소
	내용	의무대상에서 그 범위를 축소(1개 범주 삭제-본인확인 기관)하여 시행함

o 규제대안의 비교

구분	장점	단점
규제대안1	중요·대규모 개인정보처리 시스템에 대한 개인정보 보호 수준을 강화하여 개인정보 유출사고 예방 등에 기여 및 국민 편의 제고	ISMS-P 인증취득 관련, 기관·기업의 인증취득에 따른 비용* 발생 *다만, 인증취득 비용은 단순 비용(cost)에 그치지 않고 '개인정보 보호'에 대한 투자(invest)에 해당하여 편익을 동시에 발생시킴
규제대안2	ISMS-P 인증취득을 자유롭게 결정·선택할 수 있어 기관·기업의 자율성 보장	대규모 개인정보 처리 등 핵심 인프라에 대한 관리체계 공백 발생 및 개인정보 유출사고 우려
규제대안3	ISMS-P 인증취득 의무대상자 범위를 축소하여 기업의 자율성을 상대적으로 향상	본인확인기관을 의무대상에서 제외시킴으로서 중요 개인정보인 주민등록번호* 관리체계에 대한 감독 소홀 우려 *주민등록번호는 보호법상 '고유식별정보'로서 법령의 근거가 있어야 처리할 수 있는 등 엄격한 기준이 적용됨

② 이해관계자 의견수렴

이해관계자명	일시 · 장소 · 방법	제시의견	조치결과
	입법예고 예정 (2026.06.02.~07.13.)		

③ 대안의 선택 및 근거

- ①주요 공공시스템 운영기관의 경우, 개인정보 보호법 시행령 제 30조의2 및 「개인정보의 안전성 확보조치 기준(개인정보위 고시)」 제14조에 따라 개인정보위가 지정한 개인정보처리시스템을 운영하는 공공기관(공공시스템운영기관)이 의무대상자가 됨
- 위 규정에 따라 지정된 개인정보처리시스템(총 387개) 목록은 이미 공개(개인정보위 홈페이지 공지사항)되어 있어 수범자의 예측이 용이하며, 의무 대상은 고시 구체화를 통해 단계적으로 실시[81개(26.1. 기준) 시스템 우선 시행]할 예정으로서 대상자에 대한 침익적 소지가 낮을 것으로 보임
- ②이동통신사업자의 경우, ‘「전파법」 제10조에 따라 주파수를 할당받아 이동통신서비스를 제공하는 자로서 정보주체와 이동통신서비스의 이용에 관한 계약을 체결한 자’로 정하여 주요 이동통신사업자(3개)가 대상이 됨
- ③본인확인기관의 경우, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하, 정보통신망법)」 제23조의3제1항에 따라 방미통위로부터 지정받은 본인확인업무를 수행하는 23개 사업자로서 ‘본인확인 지원포털(identity.kisa.or.kr)’에서 확인 가능
- ④ISMS-P 인증 의무 대상이 되는 매출액 및 처리하는 개인정보 수를 고려한 대규모 개인정보처리자는 제도 초기 시행 등을 감안하여 최소화하고자 함
- ‘정보통신서비스 부문 매출액 100억원 이상’은 정보통신망법 제 47조제2항에 따른 정보보호 관리체계 인증(ISMS 인증) 의무대상 기준* 중 하나로서,
 - *ISMS-P는 ‘시스템 기반’의 인증 제도로써, ISMS-P 인증 취득을 위해서는 ISMS 인증 취득에 필요한 기준을 충족[ISMS-P 인증 취득을 위해서는 다.영역(개인정보 처리 단계별 요구사항)뿐만 아니라, ISMS 취득 시 필요한 가.영역(관리체계 수립·운영) 및 나.영역(보호대책 요구사항) 기준도 충족해야 함]해야 하는 등 제도적 정합성 고려
- ‘25년 ISMS 인증 의무대상자(정보통신서비스 부문 매출액 100억원 이상 기준을 충족하는 자 포함) 중, 매출액 1조 이상인 116개 기업을 대상으로 설문조사를 실시(‘26.2)한 결과, 정보주체 수가 3,000

만 명 이상이라고 응답한 기업은 9개(이 중, 정보통신서비스 부문 매출액 100억원 이상인 자는 7개)이고, 3,000만 명 미만이라고 응답한 기업은 69개, 미응답 기업은 38개였음

- 따라서, 본 ISMS-P 의무 대상 기준에 부합하는 기업 수는 7~45개로 추정됨

3. 규제목표

ISMS-P 인증 의무 대상자를 구체화하여 대규모 개인정보 처리 등 핵심 인프라에 대한 관리체계의 공백 발생을 예방하고, 중요 개인정보처리시스템에 대한 상시적 개인정보 안전관리체계를 구축하여 국민의 개인정보 보호 수준 강화

II. 규제의 적정성

1. 목적·수단 간 비례적 타당성

- ISMS-P 인증 의무 대상자 조항 신설의 목적은 기존 자율에 맡겨져 있던 ISMS-P 인증 취득을 의무화함으로써, 대규모 개인정보처리 등 핵심 인프라에 대한 관리체계 공백을 줄이고 정보주체의 개인정보를 보다 안전하게 관리하기 위함임
 - 다만, 의무화 취지 및 제도 초기 시행 등을 감안하여 기관·기업의 부담·혼선을 최소화하고 변경된 제도가 조기에 정착될 수 있도록 합리적 기준 수립 필요
- 공공 부문의 경우, 개인정보 보호법 시행령 제30조의2 및 「개인정보의 안전성 확보조치 기준(개인정보위 고시)」 제14조에 따라 지정된 개인정보처리시스템(총 387개)을 운영하는 기관이 의무 대상이 됨
 - 해당 시스템 목록은 이미 공개(개인정보위 홈페이지 공지사항)되어 있어 수범자의 예측이 용이하며, 고시 구체화를 통해 단계적으로 실시(81개 시스템 우선 시행)할 예정으로서 대상자에 대한 침익적 소지가 낮을 것으로 보임
- 민간 부문의 경우, 전파법에 따른 주요 이동통신사업자(3사), 정보통신망법에 따라 지정받은 본인확인기관(23개), 매출액(1조 이상)·정보통신서비스 부문 매출액(100억원 이상) 및 처리되는 국내 정보주체 수가 3,000만 명 이상인 개인정보처리자(7~45개 추정)가 의무대상이 됨
- 주요 이동통신사업자(3사)의 경우 국민 대부분이 모바일 통신 서비스를 이용하고 있어 해당 개인정보를 두텁게 보호할 필요가 있는 점을 고려하였으며, 본인확인기관의 경우 핵심 개인정보인 주민등록번호를 처리하는 점을 고려하여 의무 대상으로 선정
- ‘매출액(1조 이상)·정보통신서비스 부문 매출액(100억원 이상) 및 처리되는 국내 정보주체 수가 3,000만 명 이상인 개인정보처리자’

는 정보통신망법 제47조제2항에 따른 정보보호 관리체계 인증 (ISMS 인증) 의무대상 기준 중 하나인 ‘정보통신서비스 부문 매출액 100억원 이상인 자’로서 매출액 1조 이상·국내 정보주체 수 3,000만 명 이상 조건을 모두 충족하는 자임.

- 상기 3가지 조건을 충족하는 자는 대규모 개인정보를 처리하는 주요 개인정보처리자로서 7~45개*로 추정**되며, ISMS-P 인증을 의무화하여 국민의 개인정보를 두텁게 보호할 필요가 있음

* 자체 설문조사에 따른 결과이며 세부 내용은 '2. 규제 대안 검토 및 선택 - 선택 근거' 부분 참조

* 추후 자료조사를 실시하여 처리되는 정보주체 규모를 파악 후 확정 예정

- o 의무대상 기준이 비교적 명확하고 예측 가능성 있으며, 중요 개인정보 및 대규모 개인정보를 처리하는 자를 의무 대상으로 지정하여 초기 시행에 따른 부담·혼란을 완화하고자 한 것으로서 목적과 수단간 비례성이 확보된 것으로 판단됨

2. 영향평가 필요성 등 고려사항

영향평가		
기술	경쟁	중기
해당없음	해당없음	해당없음

o 영향평가

- 기술규제영향평가

해당없음

- 경쟁영향평가

해당없음

경쟁영향평가 점검항목	해당 여부
(A) 사업자의 수 또는 범위 제한	없음
(B) 사업자의 경쟁능력 제한	없음
(C) 사업자의 경쟁유인 감소	없음
(D) 소비자에게 제공되는 선택과 정보의 제한	없음

- 중기영향평가

해당없음

- 규제 차등화 예비분석 결과표

① 규제 영역	해당없음
② 규제 방식	해당없음
③ 예비분석모델	해당없음
판단 근거	해당없음
④ 대상 업종	해당없음
⑤ 예비분석내용	해당없음
⑥ 차등화적용 여부	해당없음

o 기타 고려사항

- 고용친화적 규제설계

해당없음

- 시장유인적 규제설계

해당없음

- 일몰설정 여부

해당없음

- 우선허용·사후규제 적용 여부
해당없음

분류	적용여부	적용내용/미적용사유
포괄적 개념 정의		ISMS-P 인증 의무 대상자의 범위를 구체화한 것으로 포괄적 개념 정의에 해당하지 않음
유연한 분류 체계		특정 대상을 ISMS-P 인증 의무화한 것으로 유연한 분류 체계에 해당하지 않음
네거티브 리스트		허용 대상을 한정하거나, 금지 대상을 열거하고 나머지는 허용하는 등의 네거티브 리스트에 해당하지 않음
사후 평가관리		신기술·신산업 관련 사전 심의·검사 또는 사후 평가·관리와 무관한 사안임
규제 샌드박스		규제샌드박스 적용대상이 아님

3. 해외 및 유사입법사례

o 해외사례

- (EU GDPR) 제42조 데이터 관리자 및 데이터 처리자가 GDPR을 준수하여 데이터 처리 작업을 수행함을 입증하는 인증의 목적 및 원칙, 유효기간 등 규정, 제43조 인증단체의 요건 및 역할·책임 등 규정

Article 42 Certification	제42조 인증
1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of dataprotection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account. 2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects. 3. The certification shall be voluntary	1. 회원국, 감독기관, 보호위원회와 집행위원회는 특히 유럽연합 차원에서, 정보 관리자나 처리자에 의한 처리 작업의 본 규정 준수를 입증하기 위한 목적의 정보 보호 인증 메커니즘과 정보보호 인장 및 마크 수립을 장려해야 한다. 중소기업과 중소기업의 특수한 요구가 고려되어야 한다. 2. 본 조 제 5항에 따라 승인된 인증 메커니즘과 인장 및 마크는, 본 규정 적용 대상인 정보 관리자나 처리자에 의한 준수 외에도, 제46조제2항제(f)호에 언급된 조건에 따라 제3국이나 국제기구로의 개인정보 전송 체계 내에서 제3조에 따라 본 규정 적용 대상이 아닌 정보 관리자나 처리자가 제공하는 적절한 보호장치의 존재를 입증하기 위한 목적으로 수립될 수도 있다. 해당 정보 관리자나 처리자는 계약 또는 기타 법적 구속력이 있는 문서를 통해, 정보 주체의 권리와 관련한 것을 포함해 그러한 적절한 보호장치를 적용하겠다는 구속력 있고 집행가능한 약속을 해야 한다. 3. 인증은 자발적이어야 하며 투명한

and available via a process that is transparent. 4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56. 5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal. 6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure. 7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met. 8. The Board shall collate all certification mechanisms and data protection seals and marks in a	과정을 통해 이용 가능해야 한다. 4. 본 조에 따른 인증은 본 규정을 준수해야 할 정보 관리자나 처리자의 책임을 감경하지 않으며, 제55조 또는 제56조에 따라 주무 권한을 가진 감독기관의 업무나 권한에 영향을 미치지 않는다. 5. 본 조에 따른 인증은 제43조에 언급된 인증단체 또는 주무 감독기관에 의해, 제58조제3항에 따라 해당 주무감독기관이 승인하거나 제63조에 따라 보호위원회가 승인한 기준을 바탕으로 발급되어야 한다. 이 기준을 보호위원회가 승인한 경우, 이는 공통 인증인 유럽 정보보호 인장(European Data Protection Seal)이 될 수 있다. 6. 인증 메커니즘에 처리를 제출하는 정보 관리자나 처리자는 해당하는 경우에 따라 제43조에 언급된 인증단체 또는 주무 감독기관에 인증 절차 수행에 필요한 모든 정보와 처리 활동에 대한 접근권을 제공해야 한다. 7. 정보 관리자나 처리자에 대한 인증은 최대 3년의 기간에 대해 발급되고, 관련 요구사항이 계속 충족되는 것을 전제로 동일한 조건으로 갱신될 수 있다. 인증을 위한 요구사항이 충족되지 않거나 더 이상 충족되지 않게 된 경우, 해당하는 경우에 따라 제43조에 언급된 인증단체 또는 주무 감독기관에 의해 인증이 철회된다 8. 보호위원회는 모든 인증 메커니즘과 인장 및 마크를 기록부에 수록하고 적절한 수단을 통해 일반이 이를
---	--

register and shall make them publicly available by any appropriate means.	이용할 수 있도록 해야 한다.
Article 43 Certification bodies	제43조 인증단체
1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following: (a) the supervisory authority which is competent pursuant to Article 55 or 56; (b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56. 2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have: (a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority; (b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;	1. 제57조 및 제56조에 따른 주무 감독기관의 업무나 권한에 미치는 영향 없이, 정보 보호와 관련하여 적절한 수준의 전문성을 갖춘 인증단체는, 감독기관이 필요할 때 제58조제2항제(h)호에 따른 권한을 행사할 수 있도록 감독기관에 미리 알린 후, 인증을 발급 및 갱신해야 한다. 회원국은 그러한 인증단체가 다음 중 하나 또는 양쪽 모두로부터 인가를 받도록 해야 한다. (a) 제55조 또는 제56조에 따라 주무 권한을 가진 감독기관 (b) 유럽의회 및 이사회 규정(EC) No 765/2008에 따라 지명된 국가 인가단체. 이 경우, EN-ISO/IEC 17065/2012 그리고 제55조 또는 제56조에 따라 주무 권한을 가진 감독기관이 수립한 추가 요구사항에 따라 인가가 이루어져야 한다 2. 제1항에 언급된 인증단체는 다음 조건을 갖춘 경우에만 해당 항에 따라 인가를 받는다. (a) 단체의 독립성과 인증의 주제 사안과 관련한 전문성을 주무 감독기관이 만족할 만한 수준으로 입증 (b) 제42조제5항에 언급된 기준으로, 제55조 또는 제56조에 따라 주무 권한을 가진 감독기관이 승인하거나 제63조에 따라 보호위원회가 승인한 기준을 존중하겠다고 약속

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks; (d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and (e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests. 3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies. 4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article. 5. The certification bodies referred to	(c) 정보 보호 인증과 인장 및 마크의 발급, 주기적 검토 및 철회를 위한 절차 수립 (d) 인증 위반 또는 정보 관리자나 처리자의 인증 이행 방식(과거 또는 현재)에 대한 민원을 처리하기 위한 절차 및 구조 수립, 그리고 해당 절차 및 구조를 정보 주체와 일반 대중에게 투명하게 공개하기 위한 절차 및 구조 수립 (e) 해당 단체의 업무와 임무가 이해 충돌을 일으키지 않음을 주무 감독기관이 만족할 만한 수준으로 입증 3. 본 조 제1항 및 제2항에 언급된 인증단체에 대한 인가는 제55조 또는 제56조에 따라 주무 권한을 가진 감독기관이 승인하거나 제63조에 따라 보호위원회가 승인한 기준을 바탕으로 이루어져야 한다. 본 조 제1항제(b)호에 따른 인가의 경우, 그러한 요구사항은 규정(EC) No 765/2008에서 구상된 요구사항과 인증단체의 방법 및 절차를 설명하는 기술 규칙을 보완해야 한다. 4. 제1항에 언급된 인증단체는 인증이나 인증 철회로 이어지는 적절한 평가를 수행할 책임이 있으며, 이는 정보 관리자나 처리자가 본 규정을 준수해야 할 의무에 영향을 미치지 않는다. 인가는 최대 5년의 기간에 대해 발급되고, 인증단체가 본 조에 명시된 요구사항을 충족하는 것을 전제로 동일한 조건으로 갱신될 수 있다. 5. 제1항에 언급된 인증단체는 요청된
---	--

in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification. 6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means. 7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation. 8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1). 9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).	인증의 부여 또는 철회 사유를 주무 감독기관에 제공해야 한다. 6. 본 조 제3항에 언급된 요구사항과 제42조제5항에 언급된 기준은 쉽게 접근할 수 있는 형태로 감독기관에 의해 일반에 공개되어야 한다. 감독기관은 또한 해당 요구사항 및 기준을 보호위원회에 전송해야 한다. 보호위원회는 모든 인증 메커니즘과 정보 보호 인장을 기록부에 수록하고 적절한 수단을 통해 일반이 이를 이용할 수 있도록 해야 한다. 7. 제8장에 미치는 영향 없이, 주무 감독기관이나 국가 인가단체는 인가 조건이 충족되지 않거나 더 이상 충족되지 않게 된 경우, 또는 인증단체가 취한 행동이 본 규정에 위배되는 경우, 본조 제1항에 따른 인증단체의 인가를 철회할 수 있다. 8. 집행위원회는 제42조제1항에 언급된 정보 보호 인증 메커니즘을 위해 고려되어야 할 요구사항을 명시하기 위한 목적으로 제92조에 따라 위임 법령을 채택할 권한을 가져야 한다. 9. 집행위원회는 인증 메커니즘과 정보 보호 인장 및 마크를 위한 기술 표준과 그러한 인증 메커니즘과 정보 보호인장 및 마크의 홍보 및 인식을 위한 메커니즘을 규정하는 실행 법령을 채택할 수 있다. 그러한 실행 법령은 제93조제2항에 언급된 심사 절차에 따라 채택되어야 한다.
---	--

○ 타법사례

- (정보통신망법 및 동법 시행령) 정보통신망법에 따른 '정보보호 관리체계 인증(ISMS 인증)' 의무대상(제47조제2항) 및 인증 시행에 필요한 사항 등에 대하여 규정

<정보통신망법>

제47조(정보보호 관리체계의 인증) ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

1. 「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자(이하 "주요정보통신서비스 제공자"라 한다)

2. 집적정보통신시설 사업자

3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

③ 과학기술정보통신부장관은 제2항에 따라 인증을 받아야 하는 자가 과학기술정보통신부령으로 정하는 바에 따라 국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우에는 제1항에 따른 인증 심사의 일부를 생략할 수 있다. 이 경우 인증 심사의 세부 생략 범위에 대해서는 과학기술정보통신부장관이 정하여 고시한다.

④ 과학기술정보통신부장관은 제1항에 따른 정보보호 관리체계 인증을 위하여 관리적·기술적·물리적 보호대책을 포함한 인증기준 등 그 밖에 필요한 사항을 정하여 고시할 수 있다.

⑤ 제1항에 따른 정보보호 관리체계 인증의 유효기간은 3년으로 한다. 다만, 제47조의5제1항에 따라 정보보호 관리등급을 받은 경우 그 유효기간 동안 제1항의 인증을 받은 것으로 본다.

⑥ 과학기술정보통신부장관은 한국인터넷진흥원 또는 과학기술정보통신부장관이 지정한 기관(이하 "정보보호 관리체계 인증기관"이라 한다)으로 하여금 제1항 및 제2항에 따른 인증에 관한 업무로서 다음 각 호의 업무를 수행하게 할 수 있다.

1. 인증 신청인이 수립한 정보보호 관리체계가 제4항에 따른 인증기준에 적합한지 여부를 확인하기 위한 심사(이하 "인증심사"라 한다)

2. 인증심사 결과의 심의

3. 인증서 발급·관리

4. 인증의 사후관리

5. 정보보호 관리체계 인증심사원의 양성 및 자격관리

6. 그 밖에 정보보호 관리체계 인증에 관한 업무

⑦ 과학기술정보통신부장관은 인증에 관한 업무를 효율적으로 수행하기 위하여 필요한 경우 인증심사 업무를 수행하는 기관(이하 "정보보호 관리체계 심사기관"이라 한다)을 지정할 수 있다.

⑧ 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 과학기술정보통신부장관에게 통보하여야 한다.

⑨ 제1항 및 제2항에 따라 정보보호 관리체계의 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.

⑩ 과학기술정보통신부장관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우에는 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 인증을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증을 받은 경우

2. 제4항에 따른 인증기준에 미달하게 된 경우

3. 제8항에 따른 사후관리를 거부 또는 방해한 경우

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.

⑫ 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관 지정의 기준·절차·유효기간 등에 필요한 사항은 대통령령으로 정한다.

제47조의7(정보보호 관리체계 인증의 특례) ① 과학기술정보통신부장관은 제47조제1항 및 제2항에 따른 인증을 받으려는 자 중 다음 각 호의 어느 하나에 해당하는 자에 대하여 제47조에 따른 인증기준 및 절차 등을 완화하여 적용할 수 있다.

1. 「중소기업기본법」 제2조제2항에 따른 소기업

2. 그 밖에 정보통신서비스의 규모 및 특성 등에 따라 대통령령으로 정하는 기준에 해당하는 자

② 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 제1항에 관련된 비용 및 기술 등 필요한 지원을 할 수 있다.

③ 과학기술정보통신부장관은 제1항에 따른 인증기준 및 절차 등 그 밖에 필요한 사항을 정하여 고시할 수 있다.

<정보통신망법 시행령>

제49조(정보보호 관리체계 인증 대상자의 범위) ① 법 제47조제2항제1호에서 “대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자”란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 「전기통신사업법」 제2조제3호에 따른 전기통신회선설비를 설치·보유하고 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자

2. 「전기통신사업법」 제38조제1항에 따라 기간통신사업자로부터 이동통신서비스를 제공받아 재판매하는 전기통신사업자

② 법 제47조제2항제3호에서 “대통령령으로 정하는 기준에 해당하는 자”란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 전년도 매출액 또는 세입이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자

가. 「의료법」 제3조의4에 따른 상급종합병원

나. 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교

2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.
3. 전년도 일일평균 이용자 수가 100만명 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.

제49조의2(정보보호 관리체계 인증의 특례 대상자의 범위) ① 법 제47조의7제1항제2호에 따른 정보보호 관리체계 인증의 특례 대상은 「중소기업기본법」 제2조제2항에 따른 중기업으로서 다음 각 호의 어느 하나에 해당하는 자로 한다.

1. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 300억원 미만인 자
 2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 300억원 이상인 자 중 주요 정보통신설비를 직접 설치·운영하지 않는 자로서 다음 각 목의 어느 하나에 해당하는 서비스(법 제47조제1항에 따른 인증, 「개인정보 보호법」 제32조의2제1항에 따른 인증 또는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조의2제1항에 따른 인증을 받은 자가 제공하는 서비스로 한정한다)를 이용하는 자
 - 가. 호스팅서비스(인터넷 홈페이지 구축 및 웹서버 관리 등을 해주는 서비스를 말한다)
 - 나. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」 제3조제2호 및 제3호에 따른 클라우드컴퓨팅서비스
- ② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자는 법 제47조의7제1항제2호에 따른 정보보호 관리체계 인증의 특례 대상에서 제외한다.
1. 법 제47조제2항제1호 또는 제2호에 해당하는 자
 2. 제49조제2항제1호 또는 제3호에 해당하는 자
 3. 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제2조제1호하목에 따른 가상자산 사업자
 4. 「전자금융거래법」 제2조제3호에 따른 금융회사

4. 비용편익 분석

<규제대안 1 : ISMS-P 인증 의무화 시행>

① 비용편익분석 : 피규제 기업·소상공인 직접비용 562.34 백만

분석기준년도	규제시행년도	분석대상기간 (년)	할인율(%)	단위
2025	2027	1	4.5	백만원, 현재가치

규제대안 1 : ISMS-P 인증 의무화 시행				
영향집단		비용	편익	순비용
피규제 기업· 소상공인	직접	562.34		562.34
	간접			
피규제 일반국민				
피규제자 이외 기업				

· 소상공인			
피규제자 이외 일반 국민			
정부			
총 합계	562.34		562.34
기업순비용	562.34	연간균등순비용	614.08

III. 규제 의 실효성

1. 규제 의 순응도

○ 피규제자 준수 가능성

- 공공 부문의 경우에는 대상이 되는 시스템 목록이 이미 지정·공개되어 있어 예측 가능성이 높으며, 고시를 통해 초기 의무화 대상을 81개 시스템으로 한정하여 실시할 예정임
- 위 81개에 정부24·주민등록시스템·국민신문고 등 대국민 주요 서비스 시스템이 포함되어 있으며, 국가는 정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책을 마련할 의무가 있으므로 규제의 준수 가능성이 높을 것으로 판단됨
- 민간 부문의 경우, 주요 이동통신사업자는 시장 점유율이 90% 이상*으로 다수 국민의 개인정보를 처리하고 있고, 본인확인기관은 중요 개인정보인 주민등록번호를 처리하고 있으므로 개인정보 보호 수준을 강화할 필요성이 있음
 - * SKT(41.5%), KT(30.5%), LGU+(23.6%) [KOSIS 국가통계포털, '스마트폰 통신사별 점유율(25년)' 참고]
- '매출액(1조 이상)·정보통신서비스 부문 매출액(100억원 이상) 및 처리되는 국내 정보주체 수가 3,000만 명 이상인 자'는 개인정보를 대규모로 처리하므로, 해당 규모의 개인정보처리자라면 ISMS-P 인증을 의무화하여 국민의 개인정보를 두텁게 보호할 필요가 있음
- 따라서, 민간 의무대상자는 처리하는 개인정보 규모·개인정보 중요도 등을 고려했을 때 책임성 강화·규제 필요성에 대한 공감대 형성이 충분히 이루어질 수 있을 것으로 판단됨

2. 규제 의 집행가능성

○ 행정적 집행가능성

개인정보보호위원회 인력 및 업무 위탁기관인 한국인터넷진흥원 인력을 활용하여 행정적 집행 가능

○ 재정적 집행가능성

의무대상자 확인·선정 등을 위한 비용이 필요할 것으로 판단되며,
해당 업무 수행을 위한 예산을 확보하여 집행 가능

IV. 추진계획 및 종합결론

1. 추진 경과

- 개인정보 보호법 개정안(의안번호 16765, 정무위 제안) 국회 본회의 의결('26.2.12.) 및 공포('26.3.10.)
- 정보보호 및 개인정보보호 관리체계 인증제 실효성 강화를 위한 현장 간담회 개최('26.3.12.)
- 「정보보호 및 개인정보보호 관리체계 인증제 실효성 강화방안」 발표(경제관계장관회의, 과기정통부 합동. '26.4.10.)

2. 향후 평가계획

- ISMS-P 인증 의무 대상 설명회를 통해 인증 취득 방법·절차 등 실무적으로 필요한 사항을 안내 하는 등 제도 순응도를 높이기 위한 노력 지속
- ISMS-P 인증 의무 시행으로 인한 애로 사항·개선점 등을 지속적으로 모니터링하고, 공공 부문의 경우에는 관련 사항을 고시(의무 대상자 단계적 확대 실시)에 반영 예정

3. 규제 정비계획

법령명	규제조문	규제 폐지·완화 내용	추진 일정
개인정보보호법 시행령	제34조의9	규제 재검토 기한 도래 시 검토	2029.12.

4. 종합결론

- ISMS-P 인증 취득이 기관·기업의 자율에 맡겨져 있어, 대규모 개인정보 처리 등 핵심 인프라에 대한 관리체계 공백 발생 우려 및 인증체계 강화 필요성에 대한 공감대 형성
 - 매출액, 개인정보의 처리 규모 등을 고려하여 일정 기준에 해당하는 개인정보처리자에 대해 ISMS-P 인증을 의무화하도록 개인정

보 보호법 개정('26.3.10. 공포, '27.7.1. 시행)

- 의무화 시행에 따른 기관·기업의 부담 및 혼선을 최소화하고 변경된 제도의 조기 정착을 위한 합리적 기준 수립 필요
 - 공공·민간 의무 대상자 기준이 비교적 명료·예측 가능하고, 처리하는 개인정보 규모·중요도 등을 고려했을 때 규제 필요성 및 순응도가 높을 것으로 판단되며, 인증 의무화로 국민의 개인정보를 보다 안전하게 보호할 수 있는 편익이 클 것으로 보임
- 개인정보 보호는 비용이 아니라 기업의 미래를 위한 투자라는 인식을 제고하고, 대규모 개인정보 침해·유출 사고 예방에 기여할 것으로 기대

가. 대안별 분석 비교표

분석기준년도	규제시행년도	분석대상기간 (년)	할인율 (%)	단위
2025	2027	1	4.5	백만원, 현재가치
규제대안1 : ISMS-P 인증 의무화 시행				
영향집단		비용	편익	순비용
피규제 기업 · 소상공인	직접	562.34		562.34
	간접			
피규제 일반국민				
피규제자 이외 기업 · 소상공인				
피규제자 이외 일반 국민				
정부				
총 합계		562.34		562.34
기업순비용		562.34	연간균등순비용	614.08

정성분석 내용 및 기타 참고사항

증을 취득한 자는 인증받은 내용을 표시하거나 홍보할 수 있으므로(개인정보 보호법 제32조의2 제6항) 기관·기업 이미지 제고에 기여할 수 있음

- 아울러, 인증 취득 및 사후심사(매 1년 주기)를 통해 개인정보처리시스템·개인정보 처리 조치 등에 대한 일정 기준을 지속적으로 유지한다면, 해킹 등 개인정보 침해·유출 사고를 예방하는데 기여할 수 있고 해당 사고에 따른 과태료·과징금·소송 비용 등을 절감할 수 있음
- 개인정보 침해·유출 사고 등을 예방할 수 있다면 국민의 개인정보를 안전하게 보호하는 것은 물론 개인정보 보호에 대한 국민 신뢰도를 향상시킬 수 있으며, 민간 기업의 경우에는 해당 신뢰도를 바탕으로 매출액 증대를 기대할 수 있음
- 특히 본 시행령을 통한 의무대상자가 공공 및 민간의 주요·대규모 개인정보처리자임을 고려하면 비용 대비 편익이 월등히 높을 것으로 판단됨

나. 각 대안의 활동별 비용·편익 분석 결과

<규제대안1 : ISMS-P 인증 의무화 시행>

①피규제 기업소상공인 :

□ 직접비용

(정량)영향집단명	신설한 개인정보 보호법 시행령 제34조의9 기준을 충족하는 공공·민간의 주요 개인정보처리자		
활동제목	정보보호 및 개인정보보호 관리체계 인증(ISMS-P 인증) 의무 대상자의 범위		
비용항목	기타		
비용	연도	비용	비용(현재가치)
	2027	614,097,000	562,347,016
	합계	614,097,000	562,347,016
일시적/반복적	반복적/비균등/비정률		
산식	연도	산식설명	산식
	2027		
근거설명	○ (전제사항) 매출액 등이 발생하지 않아 직접편익 산출이 어려운 공공 개인정보처리자는 분석에서 제외(직접비용·편익 산출이 가능한 민간 개인정보처리자를 대상으로 분석) ○ (비용산출 근거) ISMS-P 인증심사에 따른 평균 수수료 × ISMS-P 인증 의무 (예상)대상 기관 수 - 평균 수수료: 18,609천원 · '25년 기준, ISMS-P 인증 평균 수수료는 약 18,600천원이며, 최근 5년간 ISMS-P 인증 기업 수 및 수수료 평균은 아래와 같음		
	< 최근 5년간 ISMS-P 인증 기업 수 및 수수료 평균 >		
	구분	인증기업 수	수수료 총합(원)
	'21	111	1,922,693,300
	'22	135	2,633,479,800
	'23	143	2,659,815,500
	'24	158	2,885,753,600
	'25	173	3,219,397,300
	수수료 평균(원) 17,321,561 19,507,258 18,600,108 18,264,263 18,609,233		
	※ 인증수수료는 심사원의 인건비, 출장비 등 실제 비용 위주로 구성되어 있으며, 기관·기업의 자산 및 인력 등 산정, 규모별 투입공수에 따라 수수료 변동 - 인증 의무화 (예상)대상 기관 수: 33개(설문조사 결과, 의무 대상이 확실해 보이는 기업의 수치만 반영) · 이동통신사업자(3개) · 본인확인기관(23개) · 매출액(1조 이상)·정보통신서비스 부문 매출액(100억원 이상)		

	및 처리되는 국내 정보주체의 수가 3,000만 명 이상인 개인정보처리자(7~45개 추정*) * '25년 ISMS의무대상자(정보통신서비스 부문 매출액 100억원 이상 기준을 충족하는 자 포함) 중, 매출액 1조 이상인 116개 기업을 대상으로 설문조사 실시('26.2.). 해당 조사에서 정보주체 수가 3,000만 명 이상이라고 응답한 기업은 9개(이 중, 정보통신서비스 부문 매출액 100억원 이상인 자는 7개)이고, 3,000만 명 미만이라고 응답한 기업은 69개, 미응답 기업은 38개임 → ISMS-P 의무 대상 기준에 부합하는 기업 수는 7~45개 추정 - 총 비용: 614,097천원(18,609천원×33개)
--	--

□직접편익

(정량)영향집단명	신설한 개인정보 보호법 시행령 제34조의9 기준을 충족하는 공공·민간의 주요 개인정보처리자
활동제 목	정보보호 및 개인정보보호 관리체계 인증(ISMS-P 인증) 의무 대상자의 범위
편익항목	과징금 산출액
편익	0
일시적/반복적	일시적
산식	10,121,296,350천원 (306705950000*33)
근거설명	○ (전제사항) 매출액 등이 발생하지 않아 직접편익 산출이 어려운 공공 개인정보처리자는 분석에서 제외(직접비용·편익 산출이 가능한 민간 개인정보처리자를 대상으로 분석) ○ (비용산출 근거) ISMS-P 인증 취득으로 대규모 개인정보 침해·유출 사고를 예방할 수 있다면, 해당 사고로 기업에 부과될 수 있는 과징금을 직접편익으로 산출 가능. 과징금은 개인정보 보호법 제64조의2제1항에 따라 전체 매출액의 100분의3을 산정(최대)*하는 것으로 함 * 실제 과징금은 동조 제2항에 따라 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액을 기준으로 산정하므로 아래 예상 산출액보다 적을 수 있음 - ISMS-P 인증 의무 (예상)대상 각 기관의 매출액×0.03 합계액* * 상기 '직접비용' 분석에서 분류한 33개 기관의 각 매출액[금융감독원 전자공시시스템(dart.fss.or.kr)을 통해 확인한 '24회계연도 매출액 기준)에 0.03을 곱한 값을 합산한 수치임 - . 이동통신사업자(3개): 1,345,499,130천원 - . 본인확인기관(23개): 7,766,006,902천원 - . 매출액(1조 이상)·정보통신서비스 부문 매출액(100억원 이상) 및 처리되는 국내 정보주체의 수가 3,000만 명 이상인 개인정보처리자(설문조사 시 '해당한다'고 응답한 7개 기업): 1,009,790,317천원 - 총 편익: 10,121,296,349천원

	※ 참고: 과태료·소송 비용 등은 기업별 상이하여 산출(일률적 추산)이 불가능하므로 제외하였으며, 유출사고 예방으로 인한 국민의 개인정보 보호 및 기업 신뢰도 향상 편익은 정량적으로 산출불가하나 그 편익이 매우 클 것으로 판단됨
--	---

②피규제 일반국민 :

□편익

(정성)영향집단명	정보주체
활동제목	정보보호 및 개인정보보호 관리체계 인증(ISMS-P 인증) 의무 대상자의 범위
편익항목	개인정보 보호
일시적/반복적	반복적
근거설명	○ ISMS-P 인증 의무대상자 지정으로 대국민 영향력이 큰 개인정보처리시스템에 대한 개인정보 침해·유출사고를 예방할 수 있을 것으로 보이며, 이로 인해 정보주체의 프라이버시 및 개인정보가 보호되고 디지털경제에 대한 신뢰도 향상에 기여하여 일반국민의 편익이 클 것으로 기대됨

< 규제 개요 >

기본 정보	1.규제사무명	개인정보 보호 기본계획 수립을 위한 자료제출		
	2.규제조문	개인정보 보호법 시행령 제13조		
	3.위임법령	개인정보 보호법 제11조제5항		
	4.유형	신설	5.입법예고	2026.06.02~2026.07.13
규제의 필요성	6.추진배경 및 정부개입 필요성	○ 개인정보 보호법 제11조에서는 개인정보위가 개인정보 보호 정책 추진, 성과평가 등을 위해 개인정보처리자 등을 대상으로 개인정보 관리 수준 및 실태파악 등을 위한 조사를 실시할 수 있도록 규정 ○ 다만, 대통령령에서 자료제출 등의 범위를 구체화하고 있지 않아 개인정보 보호 정책 추진, 의무 이행 확인 등을 위한 개인정보처리자의 현황 파악이 곤란한 상황임		
	7.규제내용	○ 개인정보위의 자료제출 요구 등의 범위 구체화 – 개인정보 보호 법령에 따른 의무 대상 여부를 확인하기 위해 필요한 매출액, 개인정보 보유 규모 등에 관한 사항 – 개인정보 보호 정책 추진, 성과평가 등을 위해 필요한 사항		
	8.피규제집단 및 이해관계자	○ 개인정보처리자(관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등		
	9.규제목표	○ 개인정보 보호 정책 추진 및 의무대상자 확인 등을 위해 개인정보처리자의 관리 수준, 실태 파악 등 관련 조사를 원활하게 추진하여 정책 효과성 및 제도 이행력 제고		
규제의 적정성	10.영향평가 여부	기술영향평가	경쟁영향평가	중기영향평가
		해당없음	해당없음	해당없음
	11.비용편익 분석 (정성분석)	○ 법 제11조제2항에 따른 개인정보위의 개인정보처리자 대상 개인정보 관리 수준 및 실태파악을 위한 조사 실시와 관련하여 자료제출 등의 범위를 명확히 규정하는 것으로 추가 발생하는 비용은 없으며 의무 이행 대상 확인을 통한 개인정보 정책 효과성 극대화		
기타	12.규제일몰제	대분류	소분류	
		일몰설정 예외기준	1. 국제조약 등에 따라 동일하게 적용 되어야 하는 규제	미해당
			2. 국가의 질서 유지 및 국민생명·안전과 직접 관련된 규제	미해당
			3. 사회통념상 보편적으로 통용되는 규범적	미해당

			성격의 규제		
		경제규제 여부기준	4. 국민과 기업의 경제활동에 대한 규제		미해당
			5. 경제활동에 직접영향을 주는 규제		미해당
		일몰설정 세부기준	6. 피규제자의 규제부담이 매우 큰 규제		미해당
			7. 한시적 목적을 위한 규제이거나 주기적인 검토가 필요한 규제		미해당
		일몰설정여부		일몰조문	연장여부
		일몰유형		일몰설정기간	일몰주기
	13. 우선허용 · 사후 규제 적용여부	해당없음			

<조문 대비표>

현 행	개 정 안
제13조(자료제출 요구 등의 범위와 방법) ① 보호위원회는 법 제11조제1항에 따라 개인정보처리자에게 다음 각 호의 사항에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다. 1. 해당 개인정보처리자가 처리하는 개인정보 및 개인정보파일의 관리와 고정형 영상정보처리기기 또는 이동형 영상정보처리기기의 설치·운영에 관한 사항 2. 법 제31조에 따른 개인정보 보호책임자의 지정 여부에 관한 사항 3. 개인정보의 안전성 확보를 위한 기술적·관리적·물리적 조치에 관한 사항 4. 정보주체의 열람, 개인정보의 정정·삭제·처리정지의 요구 및 조치 현황에 관한 사항 5. 그 밖에 법 및 이 영의 준수에 관한 사항 등 기본계획의 수립·추진을 위하여 필요한 사항	제13조(자료제출 요구 등의 범위와 방법) ① (현행과 같음)
<신 설>	② 보호위원회는 법 제11조제2항에 따라 개인정

현 행	개 정 안
	<u>보처리자에게 다음 각 호에 따른 자료의 제출이나 의견의 진술 등을 요구할 수 있다.</u> <u>1. 법 및 이 영에 따른 의무 대상 여부를 확인하기 위해 필요한 매출액, 개인정보 보유 규모 등에 관한 사항</u> <u>2. 그 밖에 법 및 이 영의 준수에 관한 사항 등 개인정보 보호 정책 추진, 성과평가 등을 위하여 필요한 사항</u>
② 보호위원회는 제1항에 따라 자료의 제출이나 의견의 진술 등을 요구할 때에는 <u>기본계획을 효율적으로 수립·추진하기 위하여 필요한 최소한의 범위로 한정하여 요구하여야 한다.</u>	③ 보호위원회는 제1항 및 제2항에 따라 자료의 제출이나 의견의 진술 등을 요구할 때에는 <u>기본계획의 효율적 수립·추진과 개인정보관리 수준 및 실태파악 등을 위하여 필요한 최소한의 범위로 한정하여 요구하여야 한다.</u>
③ 법 제11조제3항에 따라 중앙행정기관의 장이 소관 분야의 개인정보처리자에게 자료의 제출 등을 요구하는 경우에는 제1항과 제2항을 준용한다. 이 경우 “보호위원회”는 “중앙행정기관의 장”으로 “법 제11조제1항”은 “법 제11조제3항”으로 본다.	④ (현행과 같음)

I. 규제의 필요성 및 대안선택

1. 추진배경 및 정부개입 필요성

- 현행 개인정보 보호법 제11조는 개인정보위가 개인정보 보호 정책 추진 등을 위해 개인정보처리자 등을 대상으로 개인정보 관리 수준 및 실태파악 등을 위한 조사를 실시할 수 있도록 규정하고 있음
 - 다만, 대통령령에서 자료제출 등의 범위를 구체화하고 있지 않아 개인정보 보호 정책 추진, 의무대상 확인 등을 위한 현황 파악이 곤란
- 이에, 시행령에 위임된 자료제출 등의 범위에 대해 구체적으로 규정하여 법 해석상 혼란을 최소화하고 정책 집행의 효과성 제고

2. 규제 대안 검토 및 선택

① 대안의 내용 및 선택 근거

- 대안의 내용
 - 개인정보위가 개인정보처리자 대상 개인정보관리 수준 및 실태파악 등을 위해 실시할 수 있는 조사 관련 자료제출의 범위* 구체화(안 제11조 제2항)
 - * ①법령에 따른 의무 대상 여부를 확인하기 위해 필요한 매출액, 개인정보 보유 규모 등에 관한 사항, ②그 밖에 개인정보 정책 추진, 성과평가 등을 위해 필요한 사항
- 선택 근거
 - 개인정보 보호 법령에서 개인정보처리자에게 부여하고 있는 의무* 대상 여부 확인에 필요한 매출액, 개인정보 보유규모 등에 관한 사항을 자료제출 범위에 추가하여 원활한 개인정보 정책 추진 도모
 - * 자격요건을 갖춘 CPO 지정, 손해배상책임보장(보험 등) 가입, 국내대리인 지정 등

② 이해관계자 의견수렴

이해관계자명	일시 · 장소 · 방법	제시의견	조치결과
	○ 입법예고 예정 (‘26.06.02.~’26.7.13.)		

3. 규제목표

- 개인정보위가 개인정보 보호 정책 추진을 위해 개인정보처리자에게 요구할 수 있는 자료 제출의 범위를 보다 구체화하여, 정부 규제의 불확실성을 완화하는 한편 정책 수립 및 집행의 효과성 제고

II. 규제의 적정성

1. 목적·수단 간 비례적 타당성

- 개인정보위의 자료제출 요구 범위에 법령에 따른 의무대상 확인을 위한 사항 및 법령 준수와 관련된 사항을 구체화함으로써 합리적이고 예측가능한 법 적용을 도모하여 목적과 수단 간 비례성 확보

2. 영향평가 필요성 등 고려사항

영향평가		
기술	경쟁	중기
해당없음	해당없음	해당없음

○ 영향평가

- 기술규제영향평가

해당없음

- 경쟁영향평가

해당없음

경쟁영향평가 점검항목	해당 여부
(A) 사업자의 수 또는 범위 제한	해당없음
(B) 사업자의 경쟁능력 제한	해당없음
(C) 사업자의 경쟁유인 감소	해당없음
(D) 소비자에게 제공되는 선택과 정보의 제한	해당없음

- 중기영향평가

해당없음

- 규제 차등화 예비분석 결과표

① 규제 영역		해당없음
② 규제 방식		해당없음
③ 예비분석모델		해당없음
	판단 근거	해당없음
④ 대상 업종		해당없음
⑤ 예비분석내용		해당없음
⑥ 차등화적용 여부		해당없음

3. 해외 및 유사입법사례

○ 해외사례

해당없음

○ 타법사례

【정보통신망법】

제64조(자료의 제출 등) ① 과학기술정보통신부장관 또는 방송미디어통신위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 **정보통신서비스 제공자**(국내대리인을 포함한다. 이하 이 조에서 같다)에게 **관계 물품·서류 등을 제출**하게 할 수 있다.

1. 이 법에 위반되는 사항을 발견하거나 혐의가 있음을 알게 된 경우
2. 이 법의 위반에 대한 신고를 받거나 민원이 접수된 경우
- 2의2. 이용자 정보의 안전성과 신뢰성 확보를 현저히 해치는 사건·사고 등이 발생하였거나 발생할 가능성이 있는 경우
3. 그 밖에 **이용자 보호를 위하여 필요한 경우**로서 대통령령으로 정하는 경우

【정보통신망법 시행령】

제68조(자료제출 등) 법 제64조제1항제3호에서 “이용자 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우”란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 법 제41조제1항 각 호의 **청소년보호를 위한 시책의 마련을 위하여 필요한 경우**
2. 법 제42조의3제3항의 **청소년보호책임자의 청소년보호업무 수행 여부를 확인하기 위하여 필요한 경우**

【소비자기본법】

제77조(검사·시료수거와 자료제출 등) ① 중앙행정기관의 장은 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령이 정하는 바에 따라 소속공무원으로 하여금 사업자의 물품·시설 및 제조공정 그 밖의 물건의 검사 또는 필요한 최소한의 시료수거를 하게 하거나 그 사업자에게 그 업무에 관한 보고 또는 관계 물품·서류 등의 제출을 명할 수 있다.

1. 제8조제2항의 규정에 따라 국가가 정한 기준을 사업자가 준수하는지 여부를 시험·검사 또는 조사하기 위하여 필요한 경우
 2. 제13조의 규정에 따라 소비자에게 정보제공을 하기 위하여 필요한 경우
 3. 제16조제1항의 규정에 따라 소비자의 불만 및 피해를 처리하기 위하여 필요한 경우
 4. 이 법의 위반 여부를 확인하기 위하여 필요한 경우
- ② 제1항의 규정에 따른 시료수거는 무상으로 할 수 있다.

- ③ 중앙행정기관의 장은 물품등의 안전성을 의심할 만한 정당한 이유가 있는 경우로서 대통령령이 정하는 사유가 있는 때에는 소속 공무원으로 하여금 사업자의 영업장소, 제조장소, 창고 등 저장소, 사무소 그 밖의 이와 유사한 장소에 출입하여 제1항의 규정에 따른 검사 등을 할 수 있다.

Ⅲ. 규제 의 실효성

1. 규제 의 순응도

○ 피규제자 준수 가능성

- 개인정보위는 법령에 따라 개인정보 보호 정책 추진 및 성과평가 등을 위해 개인정보처리자에게 자료제출을 요구할 수 있으며,
- 이에 따라, 자료제출의 범위를 구체화함으로써 규제의 불확실성 해소 및 피규제자인 개인정보처리자의 예측가능성 제고로 준수 가능성 확보

2. 규제 의 집행가능성

○ 행정적 집행가능성

기존 개인정보위 인력 활용이 가능하여 행정적 집행력 보유

○ 재정적 집행가능성

별도의 재정이 소요되지 않음

< 규제 개요 >

기본 정보	1.규제사무명	개인정보 보호책임자 지정·변경·해제시 준수사항 이행대상자의 범위와 신고절차		
	2.규제조문	개인정보 보호법 시행령 제32조		
	3.위임법령	개인정보 보호법 제31조제3항, 제10항		
	4.유형	신설	5.입법예고	2026.06.02~2026.07.13
규제의 필요성	6.추진배경 및 정부개입 필요성	○ 개인정보 보호법 개정(' 26.3.10. 공포)에 따라 매출액, 개인정보 보유 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자에 대해 개인정보 보호책임자(“CPO”) 지정·변경·해제 시 이사회 의결 및 개인정보위 신고 의무 도입 ○ 이에, 시행령에 위임된 CPO 지정·변경·해제 시 이사회 의결 및 개인정보위 신고 의무기관과 신고 방법·절차 등을 규정하여 CPO의 실질적 권한 제고 및 제도 효과성 확보		
	7.규제내용	○ 개인정보처리자의 매출액, 개인정보의 보유 규모 등을 고려하여 CPO 지정·변경·해제 시 이사회 의결 및 개인정보위 신고 의무 신설		
	8.피규제집단 및 이해관계자	○ 일정 기준 이상 개인정보처리자(기존 전문CPO 지정 의무기관)* * ①연 매출액등이 1,800억원 이상이면서, 5만명 이상 민감·고유식별정보 또는 100만명 이상 개인정보처리자 ②재학생 수 2만명 이상인 대학 ③상급종합병원 ④공공시스템운영기		
	9.규제목표	○ 일정 기준 이상의 개인정보처리자에게 CPO 지정·변경·해제 시 이사회 의결 및 개인정보위 신고 의무를 부여하여 규제의 불확실성을 완화하고, CPO의 실질적 권한을 강화하여 제도의 이행력 제고		
규제의 적정성	10.영향평가 여부	기술영향평가	경쟁영향평가	중기영향평가
		해당없음	해당없음	해당없음
	11.비용편익 분석 (정성분석)	○ 기존 법령에 따라 CPO의 전문성 강화를 위해 자격요건을 갖춘 전문CPO 지정을 의무화한 대규모 개인정보처리자에 대해 지정 절차 및 신고제를 도입하는 것으로 추가 발생하는 비용은 없으며 의무기관의 자격요건 준수 여부 점검을 통해 제도의 이행력 확보 편익 극대화		
기타	12.규제일몰제	대분류	소분류	
		일몰설정 예외기준	1. 국제조약 등에 따라 동일하게 적용 되어야 하는 규제	미해당

			2. 국가의 질서 유지 및 국민생명 · 안전과 직접 관련된 규제	미해당
			3. 사회통념상 보편적으로 통용되는 규범적 성격의 규제	해당
		경제규제 여부기준	4. 국민과 기업의 경제활동에 대한 규제	
			5. 경제활동에 직접영향을 주는 규제	
		일몰설정 세부기준	6. 피규제자의 규제부담이 매우 큰 규제	
			7. 한시적 목적을 위한 규제이거나 주기적인 검토가 필요한 규제	
		일몰설정여부 일몰조문 연장여부		
		일몰유형 일몰설정기간 일몰주기		
	13. 우선허용 · 사후 규제 적용여부	해당 없음		

<조문 대비표>

현 행	개 정 안
제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① 법 제31조제1항 단서에서 “종업원 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 「소상공인기본법」 제2조제1항에 따른 소상공인에 해당하는 자를 말한다.	제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① (현행과 같음)
<신 설>	② 법 제31조제3항 각 호 외의 부분에서 “대통령령으로 정하는 기준에 해당하는 자”를 “대통령령으로 정하는 기준에 해당하는 자 또는 대통령령으로 정하는 기준에 해당하는 자의 대표자”로 한다.

현 행	개 정 안
	령령으로 정하는 기준에 해당하는 개인정보처리자"란 다음 각 호의 어느 하나에 해당하는 개인정보처리자(공공기관의 경우에는 제2조제2호부터 제5호까지에 해당하는 경우로 한정한다)를 말한다. 1. 연간 매출액 등이 1,800억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자(제2조제5호에 따른 각급 학교 및 「의료법」 제3조에 따른 의료기관은 제외한다) 가. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자 나. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자 2. 직전 연도 12월 31일 기준으로 재학생 수(대학원 재학생 수를 포함한다)가 2만명 이상인 「고등교육법」 제2조에 따른 학교 3. 「의료법」 제3조의4에 따른 상급종합병원 4. 공공시스템운영기관 ③ 법 제31조제3항제2호에 따라 개인정보 보호책임자를 지정·변경·해제하고 신고해야 하는 개인정보처리자는 신고의무가 발생한 날부터 1개월 이내에 보호위원회 고시로 정하는 개인정보 보호책임자 지정·변경·해제 신고서를 보호위원회에 제출하여야 한다. 다만, 보호위원회는 본문에 따른 기간 내에 지정·변경·해제 신고서를 제출할 수 없는 부득이한 사유가 있다고 인정하는 때에는 그 사유가 해소된 날로부터 1개월의 범위에서 제출기한을 연장할 수 있다.
② 법 제31조제3항제7호에서 "대통령령으로 정한 업무"란 다음 각 호와 같다. 1. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행 2. 개인정보 처리와 관련된 인적·물적 자원 및 정보의 관리 3. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 ③ 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다. 1. 공공기관: 다음 각 목의 구분에 따른 기준에 해당하	④ 법 제31조제4항제9호에서 "대통령령으로 정한 업무"란 다음 각 호와 같다. 1. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행 2. 개인정보 처리와 관련된 인적·물적 자원 및 정보의 관리 3. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 ⑤ 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다. 1. (현행과 같음)

현 행	개 정 안
는 공무원 등 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관 고위공무원단에 속하는 공무원(이하 "고위공무원"이라 한다) 또는 그에 상당하는 공무원 나. 가목 외에 정무직공무원을 장으로 하는 국가기관, 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상당하는 공무원 다. 가목 및 나목 외에 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관, 4급 이상 공무원 또는 그에 상당하는 공무원 라. 가목부터 다목까지의 규정에 따른 국가기관 외의 국가기관(소속 기관을 포함한다): 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장 마. 시도 및 시도 교육청: 3급 이상 공무원 또는 그에 상당하는 공무원 바. 시군 및 자치구: 4급 이상 공무원 또는 그에 상당하는 공무원 사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람. 다만, 제4항제2호에 해당하는 경우에는 교직원을 말한다. 아. 가목부터 사목까지의 규정에 따른 기관 외의 공공기관: 개인정보 처리 관련 업무를 담당하는 부서의 장. 다만, 개인정보 처리 관련 업무를 담당하는 부서의 장이 2명 이상인 경우에는 해당 공공기관의 장이 지명하는 부서의 장이 된다. 2. 공공기관 외의 개인정보처리자: 다음 각 목의 어느 하나에 해당하는 사람 가. 사업주 또는 대표자 나. 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장) ④ 다음 각 호의 어느 하나에 해당하는 개인정보처리자(공공기관의 경우에는 제2조제2호부터 제5호까지에 해당하는 경우로 한정한다)는 제3항 각 호의 구분에 따른 사람 중 별표 1에서 정하는 요건을 갖춘 사람을 개인정보 보호책임자로 지정해야 한다.	가. ~ 바. (현행과 같음) 사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람. 다만, 제2항제2호에 해당하는 경우에는 교직원을 말한다. 아. (현행과 같음) 2. (현행과 같음) 가. 사업주 또는 대표자 나. 임원(「상법」 제401조의2제1항제3호에 따른자와 같은 법 제408조의2에 따른 집행임원을 포함한다) 다. 나목에 따른 임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장 ⑥ 제2항 각 호의 어느 하나에 해당하는 개인정보처리자(공공기관의 경우에는 제2조제2호부터 제5호까지에 해당하는 경우로 한정한다)는 제5항 각 호의 구분에 따른 사람 중 별표 1에서 정하는 요건을 갖춘 사람을 개인정보 보호책임자로 지정해야 한다.

현 행	개 정 안
1. 연간 매출액 등이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자(제2조제5호에 따른 각급 학교 및 「의료법」 제3조에 따른 의료기관은 제외한다) 가. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자 나. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자 2. 직전 연도 12월 31일 기준으로 재학생 수(대학원 재학생 수를 포함한다)가 2만명 이상인 「고등교육법」 제2조에 따른 학교 3. 「의료법」 제3조의4에 따른 상급종합병원 4. 공공시스템운영기관 ⑤ 보호위원회는 개인정보 보호책임자가 법 제31조제3항의 업무를 원활히 수행할 수 있도록 개인정보 보호책임자에 대한 교육과정을 개설·운영하는 등 지원을 할 수 있다. ⑥ 개인정보처리자(법 제31조제2항에 따라 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우는 제외한다)는 법 제31조제6항에 따른 개인정보 보호책임자의 독립성 보장을 위해 다음 각 호의 사항을 준수해야 한다. 1. 개인정보 처리와 관련된 정보에 대한 개인정보 보호책임자의 접근 보장 2. 개인정보 보호책임자가 개인정보 보호 계획의 수립·시행 및 그 결과에 관하여 정기적으로 대표자 또는 이사회에 직접 보고할 수 있는 체계의 구축 3. 개인정보 보호책임자의 업무 수행에 적합한 조직체계의 마련 및 인적·물적 자원의 제공 제62조의3(규제의 재검토) ① 보호위원회는 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 3년마다(매 3년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 해야 한다. 1. ~ 9. (생략)	1. ~ 4. <삭 제> ⑦ 보호위원회는 개인정보 보호책임자가 법 제31조제4항의 업무를 원활히 수행할 수 있도록 개인정보 보호책임자에 대한 교육과정을 개설·운영하는 등 지원을 할 수 있다. ⑧ 개인정보처리자(법 제31조제2항에 따라 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우는 제외한다)는 법 제31조제7항에 따른 개인정보 보호책임자의 독립성 보장을 위해 다음 각 호의 사항을 준수해야 한다. 1. ~ 3. (현행과 같음) 제62조의3(규제의 재검토) ① 보호위원회는 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 3년마다(매 3년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 해야 한다. 1. ~ 9. (생략) 10. 제32조제2항, 제3항에 따른 개인정보 보호책임자 지정, 변경, 해제시 준수하여야 할 대상자

현 행	개 정 안
	의 범위와 신고절차 : 2027년 1월 1일

I. 규제의 필요성 및 대안선택

1. 추진배경 및 정부개입 필요성

- 현행 개인정보 보호법 제31조 및 동법 시행령 제32조는 개인정보처리자에게 개인정보 보호책임자(이하 “CPO”) 지정 의무를 부과하는 한편, 일정 규모 이상 개인정보처리자에 대해서는 자격을 갖춘 전문CPO를 지정하도록 하여 개인정보 처리에 대한 책임성을 강화하고 있음
- 개인정보 보호법 개정(’26.3.10.공포, ’26.9.11. 시행)에 따라, 매출액·개인정보 보유 규모 등을 고려 대통령령으로 정하는 기준에 해당하는 처리자에 대해 CPO 지정·변경·해제 시 이사회 의결 및 개인정보위 신고 의무 도입
 - 이에, 시행령에 위임된 CPO 지정 절차 준수 및 신고 의무 대상기관, 신고 절차 등을 구체적으로 규정하여 CPO의 실질적 권한 제고 유도

2. 규제 대안 검토 및 선택

① 대안의 내용 및 선택 근거

- 대안의 내용
 - 개인정보처리자의 매출액, 개인정보의 보유 규모를 종합적으로 고려하여 CPO 지정·변경·해제 시 이사회 의결 및 개인정보위 신고의무가 적용되는 대상기관(전문CPO 지정기준과 동일)* 수립(안 제32조제2항)
 - * ①연 매출액 또는 수입이 1,800억원 이상인면서, 5만명 이상 민감·고유식별정보 또는 100만명 이상 개인정보처리자 ②재학생 수 2만명 이상인 대학 ③상급종합병원 ④공공시스템운영기관
 - CPO 지정·변경·해제 시 신고방법·신고절차 마련(안 제32조제3항)
 - 신고의무가 발생한 날부터 1개월 이내(부득이한 사유가 있는 경우 그 사유가 해소된 날로부터 1개월 연장 가능) 개인정보위에 신고서 제출
- 선택 근거
 - (대상기관) 전문CPO를 지정하도록 旣 의무화(’24.3.15.)한 대규모 개인정보처리자를 대상으로 CPO 자격요건 충족 여부 등 이행점검 및 CPO 역할 강화를 위한 추가적 사항을 부여하여 제도의 효과성 확보

- (이행절차) 법률에서 정한 **CPO 지정절차** 및 지정신고 등에 필요한 사항을 구체화하여 개인정보처리자의 **예측 가능성 제고**

② 이해관계자 의견수렴

이해관계자명	일시 · 장소 · 방법	제시의견	조치결과
	○ 입법예고 예정 (‘26.6.2.~’26.7.13.)		

3. 규제목표

- 일정기준 이상의 개인정보처리자에게 CPO 지정·변경·해제 시 **이사회 의결** 및 개인정보위 신고 의무를 부여하여, 규제의 불확실성을 **완화**하고 개인정보처리자의 개인정보 처리 책임성 및 투명성 제고

II. 규제의 적정성

1. 목적·수단 간 비례적 타당성

- 동 제도는 자격요건을 갖춘 전문CPO를 지정해야 하는 대상기관에 대해 CPO 지정·변경·해제 시 이사회 의결 및 개인정보위 신고 의무를 부여하여 대규모 처리자의 개인정보 처리 책임성을 강화하기 위함임
 - 매출액, 개인정보 보유 규모가 일정 기준(①연간 매출액 또는 수입 등이 1,500억원 이상, ②100만명 이상의 정보주체, 5만명 이상의 민감정보 또는 고유 식별정보) 이상인 개인정보처리자에 대해서는 학력 및 개인정보 보호 관련 경력을 요구하는 자격요건*을 신설하여 전문CPO를 지정하도록 하여 CPO의 전문성을 강화
 - 이러한 전문CPO 제도의 실효성 및 이행력 강화를 위해서는 지정·변경·해제시 이사회 의결 및 개인정보위 신고 의무를 부여할 필요
 - 전문CPO 제도 도입의 취지를 고려할 때, 이사회 의결 및 개인정보위 신고 의무 부여 대상을 전문CPO 지정 대상기관보다 넓게 정하면 과도한 규제가 될 수 있고, 더 좁게 정하면 전문CPO 지정 대상임에도 실효성 확보가 불충분할 수 있어, 전문CPO 지정 대상기관과 범위를 동일하게 정할 필요
- 또한, 보호법 개정(시행 '26.9.11.)에 따른 CPO 지정 신고제 도입과 관련 의무 이행을 위한 신고절차 및 방법 등을 구체화함으로써 합리적이고 예측가능한 법 적용을 도모하여 목적과 수단 간 비례성 확보

2. 영향평가 필요성 등 고려사항

영향평가		
기술	경쟁	중기
해당없음	해당없음	해당없음

○ 영향평가

- 기술규제영향평가

해당없음

- 경쟁영향평가

해당없음

경쟁영향평가 점검항목	해당 여부
(A) 사업자의 수 또는 범위 제한	해당없음
(B) 사업자의 경쟁능력 제한	해당없음
(C) 사업자의 경쟁유인 감소	해당없음
(D) 소비자에게 제공되는 선택과 정보의 제한	해당없음

- 중기영향평가

해당없음

- 규제 차등화 예비분석 결과표

① 규제 영역	해당없음
② 규제 방식	해당없음
③ 예비분석모델	해당없음
판단 근거	해당없음
④ 대상 업종	해당없음
⑤ 예비분석내용	해당없음
⑥ 차등화적용 여부	해당없음

○ 기타 고려사항

- 고용친화적 규제설계

해당없음

- 시장유인적 규제설계

해당없음

- 일몰설정 여부

설정(일몰유형 신규, 일몰조문 제62조의3, 일몰주기 3년, 일몰설정기간 2027.1.1.~2029.12.31.)

- 우선허용·사후규제 적용 여부
해당없음

분류	적용여부	적용내용/미적용사유
포괄적 개념 정의		인허가 또는 지원사항을 규정한 것이 아니므로 포괄적 개념 정의 불필요
유연한 분류 체계		인허가 또는 지원사항을 규정한 것이 아니므로 유연한 분류 체계에 미해당
네거티브 리스트		신사업 관련 허용대상을 한정 열거하는 사항이 아님
사후 평가관리		신사업 관련 사전 심의·검사 또는 사후 평가·관리와 무관
규제 샌드박스		신기술을 활용한 서비스 창출과 무관

3. 해외 및 유사입법사례

o 해외사례

- EU 개인정보 보호법(GDPR)은 제37조부터 제39조까지 개인정보처리자와 수탁처리자를 대상으로 '개인정보 보호담당관(Data Protection Officer)'의 지정과 지위 및 수행업무 전반에 관한 사항을 규정

【EU GDPR】

제37조(개인정보보호 담당관의 지정) ① 다음 각 호에 해당하는 경우, 개인정보처리자와 수탁처리자는 개인정보보호 담당관을 지정해야 한다.

- (a) 법원이 사법 권한을 행사하는 경우를 제외한 공공당국 또는 기관이 처리를 하는 경우
 - (b) 개인정보처리자나 수탁처리자의 핵심 활동이 처리의 성격, 범위 또는 목적에 의해 개인정보주체에 대한 정기적이고 체계적인 대규모의 모니터링을 요하는 처리 작업들로 구성되는 경우
 - (c) 개인정보처리자 또는 수탁처리자의 핵심 활동이 제9조에 따른 특정 범주의 개인정보와 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보를 대규모로 처리하는 것으로 구성되는 경우
- ② 사업체 집단은 단일의 개인정보보호 담당관을 지정할 수 있는데 각 사업장이 해당 개인정보보호 담당관을 쉽게 이용할 수 있는 경우에 그러하다.
- ③ 개인정보처리자 또는 수탁처리자가 공공당국이나 기관인 경우, 조직의 구조나 규모를 고려하여 다수의 그러한 당국이나 기관을 위해 단일의 개인정보보호 담당관이 지정될 수 있다.
- ④ 제1항에 규정된 것 이외의 경우, 개인정보처리자나 수탁처리자의 각 범주를 대표하는 협회 또는 기타 기관은 유럽연합 또는 회원국 법률이 요구하는 경우 개인정보보호 담당관을 지정할 수 있거나 지정해야 한다. 개인정보보호 담당관은 개인정보처리자 또는 수탁처리자를 대변하는 해당 협회 및 기타 기관을 대행할 수 있다.
- ⑤ 개인정보보호 담당관은 직무상의 자질, 특히 개인정보보호법과 실무에 대한 전문적 지식과 제39조에 규정된 업무를 수행할 수 있는 능력에 근거하여 지정되어야 한다.
- ⑥ 개인정보보호 담당관은 개인정보처리자 또는 수탁처리자의 직원일 수 있거나 서비스계약에 근거하여 업무를 수행할 수 있다.
- ⑦ 개인정보처리자 또는 수탁처리자는 개인정보보호 담당관의 상세 연락처를 공개하며 이를 감독기관에 통보하여야 한다.

제38조(개인정보보호 담당관의 지위) ① 개인정보처리자 및 수탁처리자는 개인정보보호 담당관이 개인정보 보호와 관련된 모든 문제에 적절하고 시의적절하게 관여하도록 해야 한다.

- ② 개인정보처리자 및 수탁처리자는 개인정보보호 담당관이 제39조의 업무를 수행하고 개인정보 및 처리 작업을 열람하며 전문지식을 유지하는 데 필요한 자원을 제공함으로써 그의 업무 수행을 지원해야 한다.
- ③ 개인정보처리자 또는 수탁처리자는 개인정보보호 담당관이 그 업무의 수행에 있어 어떠한 지시도 받지 않도록 보장해야 한다. 개인정보보호 담당관은 본인의 업무 수행을 이유로 개인정보처리자나 수탁처리자에 의해 해임 또는 처벌받아서 안된다. 개인정보보호 담당관은 개인정보처리자 또는 수탁처리자의 최고 경영진에게 직접 보고해야 한다.
- ④ 개인정보주체는 본인의 개인정보 처리 및 본 규정에 따른 권리 행사와 관련한 모든 사안에 관해 개인정보보호 담당관에게 연락을 취할 수 있다.
- ⑤ 개인정보보호 담당관은 유럽연합이나 회원국 법률에 따라 본인의 업무 수행에 관해 비밀 또는 기밀 유지의 의무를 준수해야 한다.
- ⑥ 개인정보보호 담당관은 기타 업무 및 직무를 수행할 수 있다. 개인정보처리자나 수탁처리자는 이러한 업무 및 직무가 이해의 상충을 초래하지 않도록 해야 한다.

제39조(개인정보보호 담당관의 업무) ① 개인정보보호 담당관은 최소한 다음 각 호의 업무를 수행하여야 한다.

- (a) 개인정보처리자나 수탁처리자, 그리고 처리를 수행하는 직원에게 본 규정과 유럽연합 또는 회원국의 개인정보보호 규정에 따른 의무에 대해 고지 및 권고
- (b) 책임 할당, 인식 제고, 처리 작업에 관련된 직원 교육 및 관련 감사 등 본 규정, 기타 유럽연합 또는 회원국의 개인정보보호 규정, 개인정보 보호와 관련한 개인정보처리자 또는 수탁처리자의 정책이 준수되는지 모니터링
- (c) 요청이 있을 경우, 제35조에 따라 개인정보보호 영향평가에 관한 자문 제공 및 평가의 이행을 모니터링
- (d) 감독기관과 협력
- (e) 제36조에 규정된 사전 자문 등 처리에 관련한 현안에 대해 감독기관의 연락처 역할 수행 및 적절한 경우 기타 사안에 대한 자문 제공
- ② 개인정보보호 담당관은 업무를 수행할 때 처리의 성격과 범위, 상황, 목적을 참작하여 처리 작업과 연계된 위험을 충분히 고려해야 한다.

o 타법사례

- 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3 및 동법 시행령 제36조의8은 정보통신서비스 제공자를 대상으로 정보 보호 최고책임자(CISO) 지정·신고 의무 및 신고 절차·방법 등을 규정

【정보통신망법】

제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임원(「상법」 제401조의2제1항제3호에 따른 자와 같은 법 제408조의2에 따른 집행임을 포함한다)을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 하되, 「중소기업기본법」 제2조제2항에 따른 중기업의 정보보호 최고책임자의 지정에 대해서는 대통령령으로 정한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다.

② 제1항에 따른 신고의 방법 및 절차 등에 대해서는 대통령령으로 정한다.

③ 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자(자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우로 한정한다)는 제4항의 업무 외의 다른 업무를 겸직할 수 없다. <신설 2018. 6. 12.>

(이하 생략)

【정보통신망법 시행령】

제36조의8(정보보호 최고책임자의 신고 방법 및 절차) 법 제45조의3제1항에 따라 정보보호 최고책임자를 지정하고 신고해야 하는 정보통신서비스 제공자는 신고의무가 발생한 날부터 6개월 이내에 과학기술정보통신부령으로 정하는 정보보호 최고책임자 지정신고서를 과학기술정보통신부장관에게 제출해야 한다. 다만, 과학기술정보통신부장관은 제36조의7 제2항 각 호의 어느 하나에 해당하는 자가 본문에 따른 기간 내에 지정신고서를 제출할 수 없는 부득이한 사유가 있다고 인정하는 때에는 제출기한을 1년의 범위에서 연장할 수 있다.

Ⅲ. 규제 의 실효성

1. 규제의 순응도

○ 피규제자 준수 가능성

- 자격요건을 갖춘 전문 CPO 지정 의무기관을 대상으로 CPO 지정·변경·해제 시 이사회 의결 및 개인정보위 신고 의무를 부여하여 국민의 중요 개인정보를 대량으로 처리하는 개인정보처리자의 책임성 강화를 통해 국민의 개인정보를 보다 두텁게 보호하기 위한 취지임
- 또한, 개인정보처리자의 매출액과 개인정보의 보유 규모를 고려, 의무 대상을 합리적 선정함으로써 제도 정합성 및 규제 준수 가능성 제고

2. 규제의 집행가능성

○ 행정적 집행가능성

- 기존 개인정보위 인력 및 시스템 활용이 가능하여 행정적 집행력 보유

○ 재정적 집행가능성

- 별도의 재정이 소요되지 않음

IV. 추진계획 및 종합결론

1. 추진 경과

- 「개인정보 보호법」 개정안 및 공포(3.10.)
- 「개인정보 보호법 시행령」 개정안 전체위원회 보고(4.22.)

2. 향후 평가계획

- CPO 지정 및 신고 현황 등 실태파악을 통해 적용대상 기관의 CPO 지정(자격·직위) 요건 및 지정 절차(이사회 의결) 준수여부를 지속 모니터링

3. 종합결론

- 개인정보 보호법 개정(공포 3.10., 시행 9.11.)에 따라 도입된 **CPO 지정 의결 절차** 및 **CPO 지정 신고제** 시행과 관련 대통령령에 위임된 의무 기관과 관련 절차를 구체화하여 개인정보처리자의 규제 불확실성 해소
- 자격요건을 갖춘 전문**CPO** 지정 의무기관을 대상으로 CPO 지정·변경·해제 시 **이사회 의결** 및 개인정보위 신고 의무를 부여하는 것은 CPO 지정 현황 파악을 통해 제도의 실효성을 제고하고 CPO 중심으로 기업·기관의 내부 통제를 강화하기 위한 취지임

< 규제 개요 >

기본 정보	1.규제사무명	개인정보 유출등 발생시 정보주체에게 통지하여야 하는 정보		
	2.규제조문	개인정보 보호법 시행령 제39조		
	3.위임법령	개인정보 보호법 제34조제1항		
	4.유형	강화	5.입법예고	2026.06.02~2026.07.13
규제의 필요성	6.추진배경 및 정부개입 필요성	○ 추진배경 - 디지털 서비스 이용이 확대됨에 따라 함께 개인정보 유출사고 발생 시 단순 정보 유출을 넘어 계정 탈취, 계정 도용, 스미싱 등 추가 피해가 연계되는 사례 증가 - 현행 제도는 개인정보 유출 통지 항목을 아래와 같이 규정하고 있으나, 정보주체가 실제로 취하여야 하는 계정 보호조치에 관한 안내 범위는 명확하지 않아 개인정보처리자별 안내 수준 차이가 발생하고 있음 - 특히 일부 개인정보처리자는 단순 유출 사실만 통지하고 비밀번호 변경 등 구체적인 대응 방법은 충분히 안내하지 않아 정보주체의 신속한 피해 예방에 한계가 있다는 지적이 있음 ○ 정부개입 필요성 - 개인정보 유출 시 정보주체의 즉각적인 대응 여부가 추가 피해 방지에 중요한 점을 고려할 때, 정보주체 보호를 위한 최소한의 사항을 대통령령으로 명확히 규정할 필요가 있음 - 또한, 개인정보 유출 통지는 법령상 의무사항으로 이미 운영 중인 제도이므로, 통지 항목의 구체화는 기존 제도의 실효성을 강화하기 위한 최소한의 규제 강화에 해당함		
	7.규제내용	○ 개인정보 유출통지 항목으로 그 밖에 개인정보가 유출등이 된 정보주체의 보호를 위하여 대통령령으로 정하는 사항의 범위를 구체화(개인정보 보호법 시행령 제39조제4항 신설) - 비밀번호 변경 방법 등 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 계정 보호조치를 규정		
	8.피규제집단 및 이해관계자	기업 및 소상공		
	9.규제목표	개인정보 유출등 발생 시 정보주체가 비밀번호 변경 등 필요한 계정 보호조치를 신속히 이행할 수 있도록 하여 계정 탈취, 명의도용 등 2차 피해를 예방하고 정보주체 보호를 강화		
규제의	10.영향평가	기술영향평가	경쟁영향평가	중기영향평가

적정성	여부			
		해당없음	해당없음	해당없음
	11.비용편익 분석 (정성분석)	개인정보처리자는 이미 개인정보 유출통지 체계를 운영하고 있어, 통지 항목에 계정 보호보치 사항을 추가하는 것은 기술적·현실적으로 이행 가능한 조치 사항으로 별도 비용이 발생하지 않을 것으로 판단되며, 유출통지 안내 강화를 통해 유출등으로 인하여 발생할 수 있는 피해를 최소화하는 등 개인정보가 보다 두텁게 보호되는 편익 발생		
기타	12.규제일몰제	대분류	소분류	
		일몰설정에외기준	1. 국제조약 등에 따라 동일하게 적용 되어야 하는 규제	미해당
			2. 국가의 질서 유지 및 국민생명·안전과 직접 관련된 규제	미해당
			3. 사회통념상 보편적으로 통용되는 규범적 성격의 규제	해당
		경제규제 여부기준	4. 국민과 기업의 경제활동에 대한 규제	
			5. 경제활동에 직접영향을 주는 규제	
		일몰설정 세부기준	6. 피규제자의 규제부담이 매우 큰 규제	
			7. 한시적 목적을 위한 규제이거나 주기적인 검토가 필요한 규제	
		일몰설정여부	일몰조문	연장여부
		일몰유형	일몰설정기간	일몰주기
	13. 우선허용·사후 규제 적용여부	해당없음		

<조문 대비표>

현 행	개 정 안
제39조(개인정보 <u>유출</u> 등의 통지) ① ~ ③ (생 략)	제39조(개인정보 <u>유출</u> 등의 통지) ① ~ ③ (현행과 같음)
<신 설>	④ 법 제34조제1항제7호에서 “그

현 행	개 정 안
	<u>밖에 개인정보가 유출등이 된 정보</u> <u>주체의 보호를 위하여 대통령령으로</u> <u>정하는 사항</u>” 이란 “비밀번호 변경 <u>방법 등 유출등으로 인하여 발생할</u> <u>수 있는 피해를 최소화하기 위하여</u> <u>정보주체가 할 수 있는 계정 보호조</u> <u>치 “를 말한다.</u>

I. 규제의 필요성 및 대안선택

1. 추진배경 및 정부개입 필요성

- (추진 배경) 디지털 서비스 이용이 확대됨에 따라 함께 개인정보 유출 사고 발생 시 단순 정보 유출을 넘어 계정 탈취, 계정 도용, 스미싱 등 추가 피해가 연계되는 사례 증가
- 현행 제도는 개인정보 유출 통지 항목을 아래와 같이 규정하고 있으나, 정보주체가 실제로 취하여야 하는 계정 보호조치에 관한 안내 범위는 명확하지 않아 개인정보처리자별 안내 수준 차이가 발생하고 있음
 1. 유출등이 된 개인정보의 항목
 2. 유출등이 된 시점과 그 경위
 3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
 4. 개인정보처리자의 대응조치 및 피해 구제절차
 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- 특히 일부 개인정보처리자는 단순 유출 사실만 통지하고 비밀번호 변경 등 구체적인 대응 방법은 충분히 안내하지 않아 정보주체의 신속한 피해 예방에 한계가 있다는 지적이 있음
- (정부개입 필요성) 개인정보 유출 시 정보주체의 즉각적인 대응 여부가 추가 피해 방지에 중요한 점을 고려할 때, 정보주체 보호를 위한 최소한의 사항을 대통령령으로 명확히 규정할 필요가 있음
- 또한, 개인정보 유출 통지는 법령상 의무사항으로 이미 운영 중인 제도이므로, 통지 항목의 구체화는 기존 제도의 실효성을 강화하기 위한 최소한의 규제 강화에 해당함

2. 규제 대안 검토 및 선택

① 각 대안의 활동별 비용편익 분석 결과

<규제대안1 : >

①피규제 기업소상공인 :

☐ 간접비용

(정성)영향집단명	개인정보처리자(유출등 사고 발생을 인지한 개인정보처리자)
활동제목	개인정보 유출등 통지 항목 확대
비용항목	해당없음
일시적/반복적	일시적
근거설명	개인정보처리자는 이미 개인정보 유출통지 체계를 운영하고 있어, 통지 항목에 계정 보호조치 사항을 추가하는 것은 기술적·현실적으로 이행 가능한 조치 사항으로, 별도 비용은 발생하지 않을 것으로 예상

②피규제 일반국민 :

☐ 편익

(정성)영향집단명	국민
활동제목	개인정보 유출등 통지 항목 확대
편익항목	피해 최소화 등 정보주체 권리 강화
일시적/반복적	일시적
근거설명	개인정보 유출등 발생 시 정보주체가 비밀번호 변경 등 필요한 계정 보호조치를 신속히 이행할 수 있도록 하여 계정 탈취, 명의도용 등 2차 피해를 예방하고 정보주체 보호를 강화

② 대안의 내용 및 선택 근거

- (현행유지안) 현행 개인정보 유출통지 항목 유지
- 현행과 같이 계정 보호조치 안내 여부를 개인정보처리자가 자율적으로 결정하도록 함
- (대안 1) 유출 통지 항목에 비밀번호 변경 등 계정 보호조치 사항 안내 의무 명확화(선택안)
- 유출 통지 시 비밀번호 변경 방법 등 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 계정 보호조치를 함께 안내하도록 함

o 선택 근거

- 개인정보 유출 시 정보주체의 즉각적인 대응 여부가 추가 피해 방지에 중요한 요소이나, 현행 제도에서는 개인정보처리자별 안내 수준에 차이가 발생하고 있음
- 따라서 정보주체의 보호를 위한 최소한의 계정 보호조치 사항을 명확히 하는 것이 개인정보처리자에게 발생하는 추가 부담은 제한적인 반면 정보주체 보호 효과는 큰 것으로 판단

② 이해관계자 의견수렴

이해관계자명	일시 · 장소 · 방법	제시의견	조치결과
	입법예고 예정 (2026.6.2.~2026.7.13.)		

3. 규제목표

개인정보 유출등 발생 시 정보주체가 비밀번호 변경 등 필요한 계정 보호조치를 신속히 이행할 수 있도록 하여 계정 탈취, 명의도용 등 2차 피해를 예방하고 정보주체 보호를 강화
아울러 유출 통지 사항을 명확히 함으로써 개인정보처리자별 통지 수준 편차를 완화하고 통지 제도의 실효성 제고

II. 규제의 적정성

1. 목적·수단 간 비례적 타당성

- o 개인정보 유출등 발생 시 정보주체 보호를 강화하기 위한 것으로, 이미 운영 중인 개인정보 통지 의무에 최소한의 안내 사항을 추가하는 수준에 그침
- o 정보주체의 실질적 피해 예방이라는 공익이 크고, 개인정보처리자에게 요구되는 사항도 일반적으로 이미 수행 중인 안내 수준이라는 점에서 과도한 규제로 보기 어려움

2. 영향평가 필요성 등 고려사항

영향평가		
기술	경쟁	중기
해당없음	해당없음	해당없음

o 영향평가

- 기술규제영향평가

해당없음

- 경쟁영향평가

해당없음

경쟁영향평가 점검항목	해당 여부
(A) 사업자의 수 또는 범위 제한	해당없음
(B) 사업자의 경쟁능력 제한	해당없음
(C) 사업자의 경쟁유인 감소	해당없음
(D) 소비자에게 제공되는 선택과 정보의 제한	해당없음

- 중기영향평가

해당없음

- 규제 차등화 예비분석 결과표

① 규제 영역	해당없음
② 규제 방식	해당없음
③ 예비분석모델	해당없음
판단 근거	해당없음
④ 대상 업종	해당없음
⑤ 예비분석내용	해당없음
⑥ 차등화적용 여부	해당없음

o 기타 고려사항

- 고용친화적 규제설계

해당없음

- 시장유인적 규제설계

해당없음

- 일몰설정 여부

해당없음

- 우선허용·사후규제 적용 여부

해당없음

분류	적용여부	적용내용/미 적용사유
포괄적 개념 정의		해당없음
유연한 분류 체계		해당없음
네거티브 리스트		해당없음
사후 평가관리		해당없음
규제 샌드박스		해당없음

3. 해외 및 유사입법사례

○ 해외사례

- EU GDPR(General Data Protection Regulation)의 경우 개인정보 침해 발생 시 개인정보 침해로 인한 부작용을 완화하기 위한 조치 등에 관한 정보를 제공하도록 규정하고 있음
- 또한 가이드라인에서 접근 권한이 침해된 경우 비밀번호 재설정과 같이 침해로 인한 부정적 결과로부터 개인을 보호하기 위한 구체적인 조언을 제공해야 한다고 규정하고 있음
- 미국 캘리포니아 소비자 개인정보 보호법의 경우 개인정보 침해 통지에 정보가 유출된 사람들이 자신을 보호하기 위해 취할 수 있는 조치에 대한 조언이 포함될 수 있다고 규정하고 있음

○ 타법사례

- 정보통신망법에서도 침해사고 대응 시 신속한 이용자 통지 의무 규정 신설('26.10.1 시행)

* 제48조의3(침해사고의 신고 등) ④ 정보통신서비스 제공자는 대통령령으로 정하는 침해사고가 발생하면 지체 없이 그 사실을 해당 이용자에게 통지하여야 한다. 이 경우 정보통신서비스 제공자가 이미 다른 법률에 따른 침해사고 통지를 하였으면 전단에 따른 통지를 한 것으로 본다.

⑤ 제1항에 따른 신고의 방법 및 절차와 제4항에 따른 통지의 대상, 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

Ⅲ. 규제 의 실효성

1. 규제 의 순응도

○ 피규제자 준수 가능성

- 개인정보처리자는 이미 개인정보 유출통지 체계를 운영하고 있어, 통지 항목에 계정 보호보치 사항을 추가하는 것은 기술적·현실적으로 이행 가능한 조치 사항으로 판단

2. 규제 의 집행가능성

○ 행정적 집행가능성

개인정보보호위원회의 조사인력 및 전문기관 등 기존 조사·점검 체계를 통해 집행 가능

○ 재정적 집행가능성

별도 예산이 소요되지 않음

IV. 추진계획 및 종합결론

1. 추진 경과

- 개인정보 보호법 개정 시행일에 맞추어('26.3.10. 공포, '26.9.11. 시행) 시행령 개정 추진
- 기 배포 중인 “개인정보 유출 등 사고대응 매뉴얼”을 개정하여 표준 통지 예시 등을 함께 마련할 계획

2. 향후 평가계획

- 제도 시행 이후 유출통지 실태, 정보주체 보호 효과 등 지속 모니터링
- 제도 운영상 미비점 발견 시 개선 추진

3. 종합결론

- 본 개정안은 개인정보 유출등 발생 시 정보주체가 즉시 필요한 계정 보호조치를 할 수 있도록 통지 항목을 구체화하는 것으로,
 - 정보주체 보호 강화 및 개인정보 유출통지 제도의 실효성 제고에 기여할 것으로 기대

가. 대안별 분석 비교표

분석기준년도	규제시행년도	분석대상기간 (년)	할인율 (%)	단위
2026	2026	5	4.5	백만원, 현재가치

규제대안1 :				
영향집단		비용	편익	순비용
피규제 기업 · 소상공인	직접			
	간접			
피규제 일반국민				
피규제자 이외 기업 · 소상공인				
피규제자 이외 일반 국민				
정부				
총 합계				
기업순비용			연간균등순비용	

정성분석 내용 및 기타 참고사항
개인정보처리자는 이미 개인정보 유출통지 체계를 운영하고 있어, 통지 항목에 계정 보호보치 사항을 추가하는 것은 기술적·현실적으로 이행 가능한 조치 사항으로 별도 비용이 발생하지 않을 것으로 판단되며, 유출통지 안내 강화를 통해 유출등으로 인하여 발생할 수 있는 피해를 최소화하는 등 개인정보가 보다 두텁게 보호되는 편익 발생

나. 각 대안의 활동별 비용·편익 분석 결과

<규제대안1 : >

①피규제 기업소상공인 :

□간접비용

(정성)영향집단명	개인정보처리자(유출등 사고 발생을 인지한 개인정보처리자)
활동제목	개인정보 유출등 통지 항목 확대
비용항목	해당없음
일시적/반복적	일시적
근거설명	개인정보처리자는 이미 개인정보 유출통지 체계를 운영하고 있어, 통지 항목에 계정 보호보치 사항을 추가하는 것은 기술적·현실적으로 이행 가능한 조치 사항으로, 별도 비용은 발생하지 않을 것으로 예상

②피규제 일반국민 :

□편익

(정성)영향집단명	국민
활동제목	개인정보 유출등 통지 항목 확대
편익항목	피해 최소화 등 정보주체 권리 강화
일시적/반복적	일시적
근거설명	개인정보 유출등 발생 시 정보주체가 비밀번호 변경 등 필요한 계정 보호조치를 신속히 이행할 수 있도록 하여 계정 탈취, 명의도용 등 2차 피해를 예방하고 정보주체 보호를 강화

< 규제 개요 >

기본 정보	1.규제사무명	정보주체에게 정보유출 가능성이 있음을 통지해야 하는 범위 와 정보		
	2.규제조문	개인정보 보호법 시행령 제39조		
	3.위임법령	개인정보 보호법 제34조		
	4.유형	신설	5.입법예고	2026.06.02~2026.07.13
규제의 필요성	6.추진배경 및 정부개입 필요성	○ 추진배경 - 현행 제도는 개인정보 유출 통지 의무를 “유출 등이 되었음 을 알게 된 때” 로 한정하고 있음 - 이에 따라 해킹 등 침해사고 초기 단계에서 신속히 대응하기 어려운 한계 존재 - 특히, 유출 가능성이 상당한 경우에도 “최종 확인 전” 이라는 사유로 통지를 지연하거나 축소하는 사례가 발생하여 정보주체의 피해 예방 기회가 제한됨 ○ 정부개입 필요성 - 개인정보 유출은 초기 대응 여부에 따라 피해 규모가 확대되 는 특성이 있어, 유출 여부 확정 이전 단계에서도 정보 제공 필 요 - 해킹, 다크웹 유통 등 최근 침해 양상은 사전 대응의 중요성이 커지고 있어 현행 사후적 통지 체계만으로는 한계 - 해외 주요국도 정보주체 권리·이익 침해 가능성을 기준으로 유출 가능성 단계 통지를 인정하고 있어 제도 정비 필요		
	7.규제내용	○ 대통령령으로 정하는 유출등의 가능성 요건과 피해를 최소화하 기 위한 정보 등 대통령령으로 정하는 사항 구체화(개인정보 보호 법 시행령 제39조의2 신설) - 객관적·합리적 기준 하에 유출 가능성이 높은 경우에도 통지 의무 부과		
	8.피규제집단 및 이해관계자	기업 및 소상공		
	9.규제목표	개인정보 유출 가능성 단계에서의 신속한 통지를 통해 정보주체의 대응 기회를 보장하고 피해 확산을 최소화		
규제의 적정성	10.영향평가 여부	기술영향평가	경쟁영향평가	중기영향평가
		해당없음	해당없음	해당없음

	11.비용편익 분석 (정성분석)	해당없음		
기타	12.규제일몰제	대분류	소분류	
		일몰설정 예외기준	1. 국제조약 등에 따라 동일하게 적용 되어야 하는 규제	미해당
			2. 국가의 질서 유지 및 국민생명 · 안전과 직접 관련된 규제	미해당
			3. 사회통념상 보편적으로 통용되는 규범적 성격의 규제	해당
		경제규제 여부기준	4. 국민과 기업의 경제활동에 대한 규제	
			5. 경제활동에 직접영향을 주는 규제	
		일몰설정 세부기준	6. 피규제자의 규제부담이 매우 큰 규제	
			7. 한시적 목적을 위한 규제이거나 주기적인 검토가 필요한 규제	
		일몰설정여부	일몰조문	연장여부
		일몰유형	일몰설정기간	일몰주기
	13. 우선허 용 · 사후 규제 적용여부	해당없음		

<조문 대비표>

현 행	개 정 안
<신 설>	제39조의2(개인정보 유출등의 가능성에 대한 통지) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 서면등의 방법으로 다음 각 호의 구분에 따른 때부터 72시간 이내에 정보주체에게 알려야 한다. 다만, 제39조제1항제2호에 해당하는 경우에는 해당 사유가 해소된 후 지체 없이 정보주체에게 알릴 수 있다. 1. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 불법적인 접근을 알게 된 경우로서 개인정보가 유출등이 된 객관적인 정황이 있거나 유출등이 된 정보주체를 특정하기 곤란한 경우 : 불법적인 접근을 알게 된 때 2. 개인정보처리자가 처리하는 개인정보가 불법적으로 거래·유통되고 있다는 사실이 객관적으로 확인된 경우로서 유출등이 확인된 정보주체 이외의 정보주체에 관한 개인

현 행	개 정 안
	정보도 유출등의 가능성이 높다고 인정되는 경우 : 개인정보처리자가 처리하는 개인정보가 불법적으로 거래·유통되고 있다는 사실을 알게 된 때 ② 제1항에도 불구하고 객관적으로 유출등의 가능성이 없는 경우에는 정보주체에게 알리지 않을 수 있다. ③ 법 제34조제2항에서 “피해를 최소화하기 위한 정보 등 대통령령으로 정하는 사항”이란 다음 각 호의 사항을 말한다. 이 경우 정보주체에게 불필요한 혼란이나 과도한 불안을 초래하지 아니하도록 통지 취지와 한계를 명확히 밝혀야 한다. 1. 유출등의 가능성이 있는 개인정보의 항목 2. 유출등의 가능성이 있는 시점과 그 경위 3. 법 제34조제1항제3호부터 제5호까지의 사항 4. 유출등의 여부가 확정될 경우의 추가 통지를 하겠다는 사실

현 행	개 정 안
	④ 개인정보처리자는 제1항에 따라 유출등의 가능성을 정보주체에게 알린 후 유출등이 되었는지 여부를 알게 되었을 때에는 다음 각 호의 구분에 따라 정보주체에게 알려야 한다. 1. 유출등이 된 사실이 확인된 경우: 법 제34조제1항에 따른 통지 2. 유출등이 되지 않은 사실이 확인된 경우: 유출등이 되지 않았다는 사실을 포함하는 정정 통지 ⑤ 제1항에 따른 통지 기한 내에 법 제34조제1항에 따른 통지 요건에 해당하게 된 경우에는 법 제34조제2항에 따른 통지를 하지 않을 수 있다. ⑥ 제1항부터 제5항까지에도 불구하고 개인정보처리자는 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 제3항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항부터 제5항까지에 따른 통지를 갈음할

현 행	개 정 안
	수 있다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 제3항 각 호의 사항을 30일 이상 게시하는 것으로 제1항부터 제4항까지에 따른 통지를 갈음할 수 있다.

I. 규제의 필요성 및 대안선택

1. 추진배경 및 정부개입 필요성

- (추진 배경) 현행 제도는 개인정보 유출 통지 의무를 “유출 등이 되었음을 알게 된 때”로 한정하고 있음
 - 이에 따라 해킹 등 침해사고 초기 단계에서 신속히 대응하기 어려운 한계 존재
 - 특히, 유출 가능성이 상당한 경우에도 “최종 확인 전”이라는 사유로 통지를 지연하거나 축소하는 사례가 발생하여 정보주체의 피해 예방 기회가 제한됨
- (정부개입 필요성) 개인정보 유출은 초기 대응 여부에 따라 피해 규모가 확대되는 특성이 있어, 유출 여부 확정 이전 단계에서도 정보 제공 필요
 - 해킹, 다크웹 유통 등 최근 침해 양상은 사전 대응의 중요성이 커지고 있어 현행 사후적 통지 체계만으로는 한계
 - 해외 주요국도 정보주체 권리·이익 침해 가능성을 기준으로 유출 가능성 단계 통지를 인정하고 있어 제도 정비 필요

2. 규제 대안 검토 및 선택

① 대안의 내용 및 선택 근거

- (현행유지안) 현행 개인정보 유출통지 제도 유지
 - 유출 확정 시에만 통지 의무 부과
- (대안 1) 유출 가능성 통지제도 도입(선택안)
 - 객관적·합리적 기준 하에 유출 가능성이 높은 경우에도 통지 의무 부과
- (선택 근거)
 - 개인정보 유출 가능성 단계에서의 신속 대응을 통해 정보주체 피해 확산 방지 및 최소화 가능
 - 단순 추측이 아닌 “객관적 정황” 기준을 명시하여 과도한 규제

확대 우려 최소화

- 아울러 통지 시기(72시간) 등을 기존 체계와 정합적으로 설계

② 이해관계자 의견수렴

이해관계자명	일시 · 장소 · 방법	제시의견	조치결과
	입법예고 예정(2026.6.2.~7.13.)		

3. 규제목표

개인정보 유출 가능성 단계에서의 신속한 통지를 통해 정보주체의 대응 기회를 보장하고 피해 확산을 최소화

II. 규제의 적정성

1. 목적·수단 간 비례적 타당성

- 개인정보 유출등 발생 시 정보주체 보호를 강화하기 위한 것으로, 개인정보 침해의 특성상 사전 대응이 핵심이므로, 유출 가능성 단계 통지는 목적 달성을 위한 적절한 수단
 - 대규모 피해를 초래하는 사고 발생 초기부터 정보주체가 신속하게 대응할 수 있도록 유출 가능성이 있는 경우도 통지 의무화하는 것은 목적에 부합
- 단순 가능성이 아닌 “객관적·합리적 판단 기준”을 적용하여 규제 범위의 과도한 확대를 방지
 - 정보주체 관점에서 신속 통지가 필요한 해킹 및 다크웹 공개 등으로 2차 피해 우려 등 유출의 파급효과가 큰 경우를 중심으로 규율
- 통지 시기(72시간), 방법(개별 통지), 예외(가능성 없는 경우 제외) 등을 기존 체계와 정합적으로 설계
 - 기존 유출통지 제도에 비추어 볼 때 유출 원인 등 파악에 소요되는 시간은 유출통지 제도와 비슷하고,
 - 해외사업자 등도 피규제 대상자임을 고려 시 EU(72시간) 등 글로벌 스탠다드와의 정합성 고려가 필요하고,
 - 기존 유출등 통지와 유출등 가능성 통지 기한을 같이 하는 것이 기업의 부담 최소화 가능
 - 기업 부담을 최소화하면서도 정보주체의 보호 효과를 확보하는 균형적 규제

2. 영향평가 필요성 등 고려사항

영향평가		
기술	경쟁	중기
해당없음	해당없음	해당없음

○ 영향평가

- 기술규제 영향평가

해당없음

- 경쟁영향평가

해당없음

경쟁영향평가 점검항목	해당 여부
(A) 사업자의 수 또는 범위 제한	해당없음
(B) 사업자의 경쟁능력 제한	해당없음
(C) 사업자의 경쟁유인 감소	해당없음
(D) 소비자에게 제공되는 선택과 정보의 제한	해당없음

- 중기영향평가

해당없음

- 규제 차등화 예비분석 결과표

① 규제 영역		해당없음
② 규제 방식		해당없음
③ 예비분석모델		해당없음
	판단 근거	해당없음
④ 대상 업종		해당없음
⑤ 예비분석내용		해당없음
⑥ 차등화적용 여부		해당없음

○ 기타 고려사항

- 고용친화적 규제설계

해당없음

- 시장유인적 규제설계

해당없음

- 일몰설정 여부

해당없음

- 우선허용·사후규제 적용 여부

해당없음

분류	적용여부	적용내용/미 적용사유
포괄적 개념 정의		해당없음
유연한 분류 체계		해당없음
네거티브 리스트		해당없음
사후 평가관리		해당없음
규제 샌드박스		해당없음

3. 해외 및 유사입법사례

o 해외사례

- EU GDPR(General Data Protection Regulation)의 경우 정보주체의 권리와 자유에 대한 위협 발생 가능성을 기준으로 통지. 아울러 72시간 기한을 규정
 - 일본의 경우 개인정보가 유출된 경우 뿐만 아니라 개인정보 유출 우려가 있는 경우로서 권리·이익 침해 우려가 큰 경우 통지
- “위험 기반 접근”으로 유출 가능성 단계 통지 인정

관련 국제기준	일치여부	불일치 사유(불일치 시에 한함)
해당없음		

o 타법사례

정보통신망법에서도 침해사고 대응 시 신속한 이용자 통지 의무 규정 신설(26.10.1 시행)

- * 제48조의3(침해사고의 신고 등) ④ 정보통신서비스 제공자는 대통령령으로 정하는 침해사고가 발생하면 지체 없이 그 사실을 해당 이용자에게 통지하여야 한다. 이 경우 정보통신서비스 제공자가 이미 다른 법률에 따른 침해사고 통지를 하였으면 전단에 따른 통지를 한 것으로 본다.
- ⑤ 제1항에 따른 신고의 방법 및 절차와 제4항에 따른 통지의 대상, 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

Ⅲ. 규제 의 실효성

1. 규제 의 순응도

○ 피규제자 준수 가능성

- 개인정보처리자는 이미 개인정보 유출통지 체계를 운영하고 있어, 기존 유출 통지 체계를 기반으로 가능성 통지 추가로, 제도 적응 가능성 높음
- 객관적 판단 기준 제시로 기업의 예측 가능성 확보

2. 규제 의 집행가능성

○ 행정적 집행가능성

개인정보보호위원회의 조사인력 및 전문기관 등 기존 조사·점검 체계를 통해 집행 가능

○ 재정적 집행가능성

별도 예산이 소요되지 않음

IV. 추진계획 및 종합결론

1. 추진 경과

- 개인정보 보호법 개정 시행일에 맞추어('26.3.10. 공포, '26.9.11. 시행) 시행령 개정 추진
- 기 배포 중인 “개인정보 유출 등 사고대응 매뉴얼”을 개정하여 유출 가능성 예시 등을 함께 마련할 계획

2. 향후 평가계획

- 제도 시행 이후 유출통지 실태, 정보주체 보호 효과 등 지속 모니터링
- 제도 운영상 미비점 발견 시 개선 추진

3. 종합결론

- 유출 가능성 통지제 도입은 정보주체 보호 강화를 위한 필수적 조치
 - 과도한 규제 확대를 방지하면서도 실효성 있는 개인정보 보호체계 구축 가능