

개인정보 보호법 일부개정법률안

(김상훈의원 대표발의)

의안 번호	15056
----------	-------

발의연월일 : 2025. 12. 10.

발 의 자 : 김상훈 · 윤한홍 · 이현승
김선교 · 고동진 · 안철수
김은혜 · 강대식 · 이달희
이인선 의원(10인)

제안이유

최근 주요 기업에서 개인정보 유출사고가 전방위로 발생함에 따라 개인정보 보호에 대한 신뢰가 저하되고 있음. 그럼에도 불구하고 일부 기업들은 개인정보 보호를 비용으로만 인식하여 개인정보 보호 체계가 충분히 작동하지 못하고 있다는 문제점이 드러나고 있음. 이에 따라 기업의 책임을 한층 강화해야 한다는 사회적 요구가 높아지고 있음.

이에 반복적이거나 중대한 개인정보 침해행위에 대해서는 보다 강력한 과징금 제도를 마련하여 현행 제재수단의 한계를 보완하고, 사업주 또는 대표자의 책임을 명확히 하며, 개인정보 보호책임자의 권한과 독립성을 강화하고 일정 규모 이상의 개인정보처리자에 대한 개인정보 보호 인증 의무화 등 개인정보 보호 체계를 정비하려는 것임.

주요내용

가. 사업주 또는 대표자의 책임 명확화 및 개인정보 보호책임자의 역할 강화(안 제31조)

사업주 또는 대표자를 개인정보 처리 및 보호에 관한 최종 책임자로 명확히 규정하고, 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 개인정보 보호책임자 지정에 관한 사항을 신고하도록 의무화하고 개인정보 보호에 필요한 인력관리 및 예산확보 등 역할을 강화함.

나. 개인정보 보호 인증 의무화(안 제32조의2)

매출액, 개인정보 처리 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 개인정보 보호 인증을 의무적으로 받도록 함으로써 개인정보 관리 체계의 신뢰성과 안전성을 제고함.

다. 반복적이거나 중대한 개인정보 침해에 대한 과징금 강화(안 제64조의2제2항 신설 등)

고의 또는 중대한 과실로 3년 이내 반복적 위반, 고의 또는 중대한 과실로 1천만명 이상 대규모 피해 발생, 시정조치 명령에 따르지 아니하여 유출이 발생한 행위에 대해서는 전체 매출액의 10% 범위 내에서 과징금을 부과할 수 있도록 하고, 예산·인력·설비·장치 등의 투자 및 운영 등 대통령령으로 정하는 사유가 있는 경우에는 과징금을 감경하도록 하여 기업의 사전적 예방투자를 유도함.

개인정보 보호법 일부개정법률안

개인정보 보호법 일부를 다음과 같이 개정한다.

제31조의 제목 “(개인정보 보호책임자의 지정 등)”을 “(사업주 또는 대표자의 책임 및 개인정보 보호책임자의 지정 등)”으로 하고, 같은 조 제1항 본문 중 “처리에”를 “처리 및 보호에”로, “책임질”을 “담당할”로 하며, 같은 조 제3항부터 제9항까지를 각각 제5항부터 제11항까지로 하고, 같은 조에 제3항 및 제4항을 각각 다음과 같이 신설한다.

③ 개인정보처리자의 사업주 또는 대표자는 개인정보의 안전한 처리 및 정보주체의 권리 보호에 관한 최종책임자로서 개인정보 보호분야의 전문성을 갖춘 인력과 충분한 예산의 지원 등 총괄적인 관리 조치를 실효성 있게 하여야 한다.

④ 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 다음 각 호의 사항을 준수하여야 한다.

1. 개인정보 보호책임자 임면시 이사회 의결 및 해임시 이사 총수의 3분의 2 이상의 찬성으로 의결
2. 보호위원회에 개인정보 보호책임자 지정에 관한 사항의 신고

제31조제5항(중전의 제3항)제2호부터 제7호까지를 각각 제4호부터 제9

호까지로 하고, 같은 항에 제2호 및 제3호를 각각 다음과 같이 신설하며, 같은 조 제6항(종전의 제4항) 및 제8항(종전의 제6항) 중 “제3항”을 각각 “제5항”으로 하고, 같은 조 제10항(종전의 제8항) 중 “제7항”을 “제9항”으로 하며, 같은 조 제11항(종전의 제9항) 중 “제3항에 따른 업무 및 제6항”을 “제4항에 따른 신고의 대상, 방법 및 절차, 제5항에 따른 업무 및 제8항”으로 한다.

2. 개인정보 보호에 필요한 인력 관리 및 예산 확보

3. 대표자 및 이사회에 대한 개인정보 보호 현황 및 주요 사항의 보고

제31조의2제1항제1호 중 “제31조제3항제3호”를 “제31조제5항제5호”로 한다.

제32조의2제1항에 단서를 다음과 같이 신설한다.

다만, 매출액, 개인정보의 처리 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 본문에 따른 인증을 받아야 한다.

제64조의2제5항부터 제10항까지를 각각 제7항부터 제12항까지로 하고, 같은 조 제2항부터 제4항까지를 각각 제3항부터 제5항까지로 하며, 같은 조에 제2항을 다음과 같이 신설하고, 같은 조 제3항(종전의 제2항), 같은 조 제4항(종전의 제3항), 같은 조 제5항(종전의 제4항) 각 호 외의 부분 중 “제1항”을 각각 “제1항 및 제2항”으로 하며, 같은 조에 제6항을 다음과 같이 신설하고, 같은 조 제8항(종전의 제6항) 중 “제1항”

을 “제1항 및 제2항”으로, “제2항부터 제5항까지”를 “제3항부터 제7항까지”로 하며, 같은 조 제9항(중전의 제7항) 전단 중 “제1항”을 “제1항 및 제2항”으로 하고, 같은 조 제10항(중전의 제8항) 중 “제1항”을 “제1항 및 제2항”으로, “제7항”을 “제9항”으로 하며, 같은 조 제11항(중전의 제9항) 중 “제1항”을 “제1항 및 제2항”으로 하고, 같은 조 제12항(중전의 제10항) 중 “제9항”을 “제11항”으로 한다.

② 제1항에도 불구하고 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보처리자에게 전체 매출액의 100분의 10을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 50억원을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다.

1. 고의 또는 중대한 과실로 이 조에 따른 과징금을 부과받은 자가 3년 이내에 제1항 각 호의 구분에 따른 같은 위반행위를 반복한 경우
2. 고의 또는 중대한 과실로 제1항 각 호의 어느 하나에 해당하는 위반행위를 하고 정보주체의 피해 규모가 1천만명 이상인 경우
3. 제64조제1항에 따른 시정조치 명령에 따르지 아니하여 개인정보 처리자가 처리하는 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우

⑥ 보호위원회는 개인정보 보호를 위한 예산·인력·설비·장치 등

의 투자 및 운영 등 대통령령으로 정하는 사유가 있는 경우에는 과징금을 감경한다. 다만, 개인정보처리자의 고의 또는 중대한 과실로 위반행위를 한 경우에 이를 적용하지 아니한다.

제75조제2항에 제14호의2 및 제14호의3을 각각 다음과 같이 신설하고, 같은 항 제15호 중 “제32조의2제6항”을 “제32조의2제1항 단서를 위반하여 개인정보 보호 인증을 받지 아니하거나, 같은 조 제6항”으로 하며, 같은 조 제4항제9호를 삭제한다.

14의2. 제31조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 보호책임자를 지정하지 아니한 자(제31조제11항에 따른 개인정보 보호책임자의 자격요건을 갖추지 아니한 자를 개인정보 보호책임자로 지정한 경우를 포함한다)

14의3. 제31조제4항제1호(제26조제8항에 따라 준용되는 경우를 포함한다)의 개인정보 보호책임자의 임면 및 해임절차를 거치지 아니하거나 제31조제4항제2호의 개인정보 보호책임자의 지정을 신고하지 아니한 자

부 칙

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. 다만, 제32조의2의 개정규정은 2027년 7월 1일부터 시행한다.

제2조(과징금 부과에 관한 경과조치 등) ① 이 법 시행 전에 종료된

위반행위에 대한 과징금의 부과는 제64조의2의 개정규정에도 불구하고 종전의 규정에 따른다.

② 이 법 시행 당시 종료되지 아니한 위반행위에 대한 과징금의 부과는 제64조의2의 개정규정에 따른다.

신·구조문대비표

현행	개정안
제31조(개인정보 보호책임자의 지정 등) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다. 다만, 종업원 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 개인정보처리자의 경우에는 지정하지 아니할 수 있다.	제31조(사업주 또는 대표자의 책임 및 개인정보 보호책임자의 지정 등) ① ----- ----- 처리 및 보호에 ----- - 담당할 ----- . - ----- ----- ----- -----.
② (생략) <신설>	② (현행과 같음)
<신설>	③ 개인정보처리자의 사업주 또는 대표자는 개인정보의 안전한 처리 및 정보주체의 권리 보호에 관한 최종책임자로서 개인정보 보호 분야의 전문성을 갖춘 인력과 충분한 예산의 지원 등 총괄적인 관리 조치를 실효성 있게 하여야 한다.
<신설>	④ 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 다음 각 호의 사항을 준수하여야 한다.

③ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다. 1. (생략) <u><신설></u> <u><신설></u> 2. ~ 7. (생략) ④ 개인정보 보호책임자는 제3항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다. ⑤ (생략) ⑥ 개인정보처리자는 개인정보	1. 개인정보 보호책임자 임면시 <u>이사회 의결 및 해임시 이사총수의 3분의 2 이상의 찬성으로 의결</u> 2. <u>보호위원회에 개인정보 보호책임자 지정에 관한 사항의 신고</u> ⑤ ----- -----. 1. (현행과 같음) 2. <u>개인정보 보호에 필요한 인력 관리 및 예산 확보</u> 3. <u>대표자 및 이사회에 대한 개인정보 보호 현황 및 주요 사항의 보고</u> 4. ~ 9. (현행 제2호부터 제7호까지와 같음) ⑥ ----- 제5항 ----- ----- ----- ----- ----- ----- --. ⑦ (현행 제5항과 같음) ⑧ -----
---	--

보호책임자가 제3항 각 호의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 되며, 개인정보 보호책임자가 업무를 독립적으로 수행할 수 있도록 보장하여야 한다.

⑦ (생략)

⑧ 보호위원회는 제7항에 따른 개인정보 보호책임자 협의회의 활동에 필요한 지원을 할 수 있다.

⑨ 제1항에 따른 개인정보 보호책임자의 자격요건, 제3항에 따른 업무 및 제6항에 따른 독립성 보장 등에 필요한 사항은 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정한다.

제31조의2(국내대리인의 지정)

① 국내에 주소 또는 영업소가 없는 개인정보처리자로서 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 자는 다음 각 호의 사항을 대리하는 자(이하 “국내대

제5항

⑨ (현행 제7항과 같음)

⑩ 제9항

⑪

제4항에 따른 신고의 대상, 방법 및 절차, 제5항에 따른 업무 및 제8항

제31조의2(국내대리인의 지정)

①

리인”이라 한다)를 지정하여야 한다. 이 경우 국내대리인의 지정은 문서로 하여야 한다. 1. <u>제31조제3항제3호</u>에 따른 개인정보 처리와 관련한 불만의 처리 및 피해 구제 업무 2. ~ 3. (생략) ② ~ ⑤ (생략) 제32조의2(개인정보 보호 인증) ① 보호위원회는 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관하여 인증할 수 있다. <u><단서 신설></u> ② ~ ⑧ (생략) 제64조의2(과징금의 부과) ① (생략) <u><신설></u>	-----. -----. 1. <u>제31조제5항제5호</u>----- ----- 2. (현행과 같음) ② ~ ⑤ (현행과 같음) 제32조의2(개인정보 보호 인증) ① ----- ----- ----- -----. <u>다만, 매출액, 개인정보의 처리 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 본문에 따른 인증을 받아야 한다.</u> ② ~ ⑧ (현행과 같음) 제64조의2(과징금의 부과) ① (현행과 같음) ② <u>제1항에도 불구하고 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 해당</u>
---	--

개인정보처리자에게 전체 매출액의 100분의 10을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 50억원을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다.

1. 고의 또는 중대한 과실로 이 조에 따른 과징금을 부과 받은 자가 3년 이내에 제1항 각 호의 구분에 따른 같은 위반행위를 반복한 경우

2. 고의 또는 중대한 과실로 제1항 각 호의 어느 하나에 해당하는 위반행위를 하고 정보주체의 피해 규모가 1천 만명 이상인 경우

3. 제64조제1항에 따른 시정조치 명령에 따르지 아니하여 개인정보처리자가 처리하는 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우

② 보호위원회는 제1항에 따른

③ ----- 제1항 및 제2

과징금을 부과하려는 경우 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액을 기준으로 과징금을 산정한다.

③ 보호위원회는 제1항에 따른 과징금을 부과하려는 경우 개인정보처리자가 정당한 사유 없이 매출액 산정자료의 제출을 거부하거나 거짓의 자료를 제출한 경우에는 해당 개인정보처리자의 전체 매출액을 기준으로 산정하되 해당 개인정보처리자 및 비슷한 규모의 개인정보처리자의 개인정보 보유 규모, 재무제표 등 회계자료, 상품·용역의 가격 등 영업현황 자료에 근거하여 매출액을 추정할 수 있다.

④ 보호위원회는 제1항에 따른 과징금을 부과하는 경우에는 위반행위에 상응하는 비례성과 침해 예방에 대한 효과성이 확보될 수 있도록 다음 각 호의 사항을 고려하여야 한다.

1. ~ 11. (생략)

항-----

-----.

④ ----- 제1항 및 제2항-----

-----.

⑤ ----- 제1항 및 제2항-----

-----.

1. ~ 11. (현행과 같음)

<신 설>

⑤ (생 략)

⑥ 제1항에 따른 과징금은 제2항부터 제5항까지를 고려하여 산정하되, 구체적인 산정기준과 산정절차는 대통령령으로 정한다.

⑦ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니하면 납부기한의 다음 날부터 내지 아니한 과징금의 연 100분의 6에 해당하는 가산금을 징수한다. 이 경우 가산금을 징수하는 기간은 60개월을 초과하지 못한다.

⑧ 보호위원회는 제1항에 따른

⑥ 보호위원회는 개인정보 보호를 위한 예산·인력·설비·장치 등의 투자 및 운영 등 대통령령으로 정하는 사유가 있는 경우에는 과징금을 감경한다. 다만, 개인정보처리자의 고의 또는 중대한 과실로 위반행위를 한 경우에 이를 적용하지 아니한다.

⑦ (현행 제5항 및 제6항과 같음)

⑧ 제1항 및 제2항----- 제3항부터 제7항까지-----

-----.

⑨ ----- 제1항 및 제2항-----

-----.

-----.

⑩ ----- 제1항 및 제2

과징금을 내야 할 자가 납부기
한까지 내지 아니한 경우에는
기간을 정하여 독촉하고, 독촉
으로 지정한 기간 내에 과징금
과 제7항에 따른 가산금을 내
지 아니하면 국세강제징수의
예에 따라 징수한다.

⑨ 보호위원회는 법원의 판결
등의 사유로 제1항에 따라 부
과된 과징금을 환급하는 경우
에는 과징금을 낸 날부터 환급
하는 날까지의 기간에 대하여
금융회사 등의 예금이자율 등
을 고려하여 대통령령으로 정
하는 이자율을 적용하여 계산
한 환급가산금을 지급하여야
한다.

⑩ 보호위원회는 제9항에도 불
구하고 법원의 판결에 따라 과
징금 부과처분이 취소되어 그
판결이유에 따라 새로운 과징
금을 부과하는 경우에는 당초
납부한 과징금에서 새로 부과
하기로 결정한 과징금을 공제
한 나머지 금액에 대해서만 환
급가산금을 계산하여 지급한

항-----

제9항-----

⑪ -----

제1항 및 제2항---

⑫ ----- 제11항-----

다.

제75조(과태료) ① (생 략)

② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

1. ~ 14. (생 략)

<신 설>

<신 설>

15. 제32조의2제6항을 위반하여 인증을 받지 아니하였음에도 거짓으로 인증의 내용

제75조(과태료) ① (현행과 같음)

② -----

-----.

1. ~ 14. (현행과 같음)

14의2. 제31조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 보호책임자를 지정하지 아니한 자(제31조제11항에 따른 개인정보 보호책임자의 자격요건을 갖추지 아니한 자를 개인정보 보호책임자로 지정한 경우를 포함한다)

14의3. 제31조제4항제1호(제26조제8항에 따라 준용되는 경우를 포함한다)의 개인정보 보호책임자의 임면 및 해임 절차를 거치지 아니하거나 제31조제4항제2호의 개인정보 보호책임자의 지정을 신고하지 아니한 자

15. 제32조의2제1항 단서를 위반하여 개인정보 보호 인증을 받지 아니하거나, 같은 조

을 표시하거나 홍보한 자	<u>제6항</u> ----- ----- ----- -----
16. ~ 27. (생 략)	16. ~ 27. (현행과 같음)
③ (생 략)	③ (현행과 같음)
④ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이 하의 과태료를 부과한다.	④ ----- ----- -----.
1. ~ 8. (생 략)	1. ~ 8. (현행과 같음)
9. <u>제31조제1항(제26조제8항에 따라 준용되는 경우를 포함 한다)을 위반하여 개인정보 보호책임자를 지정하지 아니 한 자</u>	<u><삭 제></u>
9의2. ~ 12. (생 략)	9의2. ~ 12. (생 략)
⑤ (생 략)	⑤ (현행과 같음)