



제433국회(임시회)
제1차 정무위원회

개인정보 보호법 일부개정법률안

검 토 보 고

〈개인정보 유출 시 보호계획 제출 의무화 등〉
■ 김승원의원 대표발의(의안번호 제221555호)

2026. 3.

정 무 위 원 회

수석전문위원 정명호

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	2

I. 제안경위

1. 제 안 자 : 김승원의원 등 20인
2. 제 안 일 : 2025. 12. 23.
3. 회 부 일 : 2025. 12. 24.

II. 제안이유 및 주요내용

현행법은 개인정보처리자가 개인정보 유출등을 알게 된 경우 정보주체에게 통지하고, 개인정보보호위원회 또는 전문기관에 신고하도록 정하고 있음.

그런데 통지 및 신고 이후의 개인정보처리자의 사후 대응 과정에 대해서는 별도의 보고의무가 정해져 있지 않아 피해 확산 방지, 복구 조치 이행 등이 제대로 관리되지 않고 있고, 사고 원인 분석과 재발 방지 대책 마련에도 한계가 있다는 지적이 있음.

이에 개인정보 유출등이 발생한 경우 개인정보처리자가 보호계획을 수립하고, 개인정보보호위원회에 그 계획을 제출하도록 의무화하여 사후 대응의 책임성과 투명성을 높여 개인정보 유출등에 따른 대응체계를 강화하려는 것임(안 제34조의2 신설 등).

Ⅲ. 검토의견

□ 개정안은 개인정보 유출등이 발생하여 개인정보보호위원회 또는 한국인터넷진흥원에 유출 신고를 행한 개인정보처리자로 하여금 유출등이 된 개인정보의 정보주체에 대한 지원사항 등 법정 사항을 포함한 보호계획을 수립하여 보호위원회에 제출하도록 의무화하고, 보호위원회는 제출받은 계획을 검토하여 그 내용이 미흡한 경우 보완 요구를 할 수 있도록 규정하려는 것임(안 제34조의2 신설).

○ 또한 보호계획 미제출 시 3천만원 이하의 과태료를 부과하고, 보호계획 보완 요구 미이행 시 2천만원 이하의 과태료를 부과하려는 것임(안 제75조제2항 및 제3항).

현행	개정안
제26조(업무위탁에 따른 개인정보의 처리 제한) ① ~ ⑦ (생략)	제26조(업무위탁에 따른 개인정보의 처리 제한) ① ~ ⑦ (현행과 같음)
⑧ 수탁자에 관하여는 제15조부터 제18조까지, 제21조, 제22조, 제22조의2, 제23조, 제24조, 제24조의2, 제25조, 제25조의2, 제27조, 제28조, 제28조의2부터 제28조의5까지, 제28조의7부터 제28조의11까지, 제29조, 제30	⑧ ----- ----- ----- ----- ----- ----- -----

조, 제30조의2, 제31조, 제33조, 제34조, <u>제34조의2</u> , 제35조, 제35조의2, 제36조, 제37조, 제37조의2, 제38조, 제59조, 제63조, 제63조의2 및 제64조의2를 준용한다. 이 경우 “개인정보처리자”는 “수탁자”로 본다.	----- ----- <u>제34조의2</u> , <u>제34조의3</u> ----- ----- ----- ----- -----.
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 “국내대리인”이라 한다)를 지정하여야 한다. 이 경우 국내대리인의 지정은 문서로 하여야 한다.	제31조의2(국내대리인의 지정) ① ----- ----- ----- ----- ----- ----- ----- ----- -----.
1. 2. (생략) <u><신설></u>	1. 2. (현행과 같음) <u>2의2. 제34조의2에 따른 개인정보 유출 등의 보호계획 제출</u>
3. (생략) ② ~ ⑤ (생략)	3. (현행과 같음) ② ~ ⑤ (현행과 같음)
제34조(개인정보 유출 등의 통지·신고) ① 개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조에서 “유출등”이라	제34조(개인정보 유출 등의 통지·신고) ① ----- ----- ---“ <u>유출등</u> ”이라 한다-----

한다)되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.

1. ~ 5. (생략)

② ~ ④ (생략)

<신설>

-----개별적으로 알려
야-----.

1. ~ 5. (현행과 같음)

② ~ ④ (현행과 같음)

제34조의2(개인정보 유출 등의 보호계획 제출) ① 제34조제3항 본문에 따라 보호위원회 또는 대통령령으로 정하는 전문기관에 개인정보 유출등의 신고를 한 개인정보처리자는 유출등이 된 개인정보의 유형·규모 등을 고려하여 대통령령으로 정하는 바에 따라 다음 각 호의 사항이 포함된 보호계획을 보호위원회에 제출하여야 한다.

1. 유출등이 된 개인정보의 해당 정보주체에 대한 지원사항

2. 유출등의 재발 방지를 위한

	<u>기술적·관리적 및 물리적 보호조치 강화 계획</u> <u>3. 그 밖에 보호위원회가 정하는 사항</u> <u>② 보호위원회는 제1항에 따라 제출받은 계획을 검토하고, 그 내용이 미흡하다고 인정할 때에는 개인정보처리자에게 일정한 기한을 정하여 보완을 요구할 수 있다. 이 경우 개인정보처리자는 정당한 사유가 없으면 이에 따라야 한다.</u>
<u>제34조의2(노출된 개인정보의 삭제·차단) (생략)</u>	<u>제34조의3(노출된 개인정보의 삭제·차단) (현행 제34조의2와 같음)</u>
제75조(과태료) ① (생략)	제75조(과태료) ① (현행과 같음)
② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.	② ----- ----- -----.
1. ~ 18. (생략)	1. ~ 18. (현행과 같음)
<u><신설></u>	<u>18의2. 제34조의2제1항(제26조 제8항에 따라 준용되는 경우를 포함한다)을 위반하여 보호계획을 보호위원회에 신고하지 아니한 자</u>
19. ~ 27. (생략)	19. ~ 27. (현행과 같음)

③ 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다. 1. ~ 4. (생략) <u><신설></u> ④·⑤ (생략)	③ ----- ----- -----. 1. ~ 4. (현행과 같음) 5. <u>제34조의2제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 보호위원회의 보호계획 보완 요구를 따르지 아니한 자</u> ④·⑤ (현행과 같음)
--	--

□ 현행법은 개인정보처리자가 개인정보의 유출등이 있음을 알게 되었을 때 지체 없이 해당 정보주체에게 유출등이 된 개인정보의 항목 등 법정 사항을 통지하도록 하고, 해당 사항을 개인정보보호위원회(이하 “보호위원회”라 함) 또는 대통령령으로 정하는 전문기관인 한국인터넷진흥원¹⁾에 신고하도록 하고 있음²⁾.

-
- 1) 「개인정보 보호법 시행령」 제40조(개인정보 유출 등의 신고) ③ 법 제34조제3항 전단 및 후단에서 “대통령령으로 정하는 전문기관”이란 각각 한국인터넷진흥원을 말한다.
- 2) 「개인정보 보호법」 제34조(개인정보 유출 등의 통지·신고) ① 개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조에서 “유출등”이라 한다)되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.
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
- ② 개인정보처리자는 개인정보가 유출등이 된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.
- ③ 개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의

○ 그런데 유출등 사실에 대한 통지 및 신고가 이루어진 이후 개인 정보처리자의 사후 대응과정에 대한 별도의 보고의무가 마련되어 있지 않아, 피해확산 및 재발 방지 등을 위한 사후관리방안이 미비하다는 지적이 제기됨.

○ 이에 개정안은 개인정보 유출등이 발생한 경우 개인정보처리자가 ① 유출등이 된 개인정보의 해당 정보주체에 대한 지원사항 ② 유출등의 재발 방지를 위한 기술적·관리적 및 물리적 보호 조치 강화 계획 ③ 그 밖에 보호위원회가 정하는 사항이 포함된 ‘보호계획’을 수립하여 보호위원회에 제출하도록 의무화하고, 계획 내용이 미흡한 경우 보완 요구를 할 수 있도록 하려는 것임.

○ 개정안에 따르면 유출 사실 신고 후에도 개인정보처리자가 실제로 취약점을 보완하고 정보주체에 대한 실효적 구제를 실시하고 있는지 등에 대한 정부당국 차원의 사후 관리가 강화되는 긍정적인 효과가 있을 것으로 기대됨.

□ 다만, 개정안과 관련하여서는 입법 필요성 외에 다음 의견들을 종합적으로 고려한 입법정책적 결정이 필요할 것으로 보임.

○ **보호위원회**는 개인정보처리자의 피해확산 방지 책임을 강화하

경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각 호의 사항을 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

④ 제1항에 따른 유출등의 통지 및 제3항에 따른 유출등의 신고의 시기, 방법, 절차 등에 필요한 사항은 대통령령으로 정한다.

려는 개정 취지에는 공감하나, 개정안에 따른 보호계획 제출제도는 현행법상의 유출신고 의무³⁾, 피해 최소화 의무⁴⁾, 안전조치 의무⁵⁾과 유사·중복되는 측면이 있으므로 현행 체계와 차별성이 크지 않고, 유출 이후 법 위반에 대한 조사·처분을 통해 안전조치의무 위반에 대한 시정 등 사후 관리가 이루어지고 있어⁶⁾ 신중한 검토가 필요하다는 의견을 제출하였음.

-
- 3) 「개인정보 보호법」 34조에서 이미 개인정보 유출 시 개인정보처리자가 정보주체 및 당국에 “유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보”, “개인정보처리자의 대응조치 및 피해 구제절차” 등을 통지하도록 하고 있음.
- 4) 「개인정보 보호법」 제34조(개인정보 유출 등의 통지·신고) ② 개인정보처리자는 개인정보가 유출등이 된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.
- 5) 「개인정보 보호법」 제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.
- 6) 「개인정보 보호법」 제63조의2(사전 실태점검) ① 보호위원회는 제63조제1항 각 호에 해당하지 아니하는 경우로서 개인정보 침해사고 발생의 위험성이 높고 개인정보 보호의 취약점을 사전에 점검할 필요성이 인정되는 개인정보처리자에 대하여 개인정보 보호실태를 점검할 수 있다.
- ② 보호위원회는 제1항에 따른 실태점검을 실시하여 이 법을 위반하는 사항을 발견한 경우 해당 개인정보처리자에 대하여 시정방안을 정하여 이에 따를 것을 권고할 수 있다.
- ③ 제2항에 따른 시정권고를 받은 개인정보처리자는 이를 통보받은 날부터 10일 이내에 해당 권고를 수락하는지 여부에 관하여 보호위원회에 통지하여야 하며, 그 이행 결과를 보호위원회가 고시로 정하는 바에 따라 보호위원회에 알려야 한다.
- ④ 제2항에 따른 시정권고를 받은 자가 해당 권고를 수락한 때에는 제64조제1항에 따른 시정조치 명령(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회의 경우에는 제64조제3항에 따른 권고를 말한다)을 받은 것으로 본다.
- ⑤ 보호위원회는 제2항에 따른 시정권고를 받은 자가 해당 권고를 수락하지 아니하거나 이행하지 아니한 경우 제63조제2항에 따른 검사를 할 수 있다.
- ⑥ 보호위원회는 관계 중앙행정기관의 장과 합동으로 제1항에 따른 개인정보 보호실태를 점검할 수 있다.

제64조(시정조치 등) ① 보호위원회는 이 법을 위반한 자(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 제외한다)에 대하여 다음 각 호에 해당하는 조치를 명할 수 있다.

1. 개인정보 침해행위의 중지
 2. 개인정보 처리의 일시적인 정지
 3. 그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치
- ② 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관이 이 법을 위반하였을 때에는 제1항 각 호에 해당하는 조치를 명할 수 있다.
- ③ 보호위원회는 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회가 이 법을 위반하였을 때에는 해당 기관의 장에게 제1항 각 호에 해당하는 조치를 하도록 권고할 수 있다. 이 경우 권고를 받은 기관은 특별한 사유가 없으면 이를 존중하여야 한다.

- 또한 인터넷기업협회는 보호계획 포함 사항 중 피해자 지원 관련 사항은 기업의 법적 책임이 확정되기 이전에 사실상의 금전적 보상이나 서비스 제공을 강제하는 효과를 가질 수 있어 기업의 방어권을 침해할 수 있다는 점에서 제외할 필요가 있고, 현행 유출신고 등 제도 이외에 보호계획 제출 및 이행 강제까지 추가될 경우 기업의 사고대응 역량이 분산되어 개인정보 유출등에 따른 대응체계 강화라는 본래 입법 취지가 약화될 가능성이 있다는 입장을 제출하였음.

문 의 처
02)6788-5108