



제433회국회(임시회)
제1차 정무위원회

개인정보 보호법 일부개정법률안

검 토 보 고

〈 안전성 확보조치의 내용 법률 명시 등 〉

■ 민형배의원 대표발의(의안번호 제2215086호)

2026. 3.

정 무 위 원 회

수석전문위원 정 명 호

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III. 검토의견	3
1. 안전성 확보조치의 구체적 내용을 법률에 명시	3
2. 개인정보 유출등에 따른 후속조치 규정	8

I. 제안경위

1. 제 안 자: 민형배의원 등 14인
2. 제 안 일: 2025. 12. 10.
3. 회 부 일: 2025. 12. 11.

II. 제안이유 및 주요내용

대형 온라인플랫폼에서 반복되는 대규모 개인정보 유출을 막고, 시민 피해를 최소화하고자 합니다.

최근 쿠팡 등에서 수천만 명의 개인정보가 유출되는 사고가 발생했습니다. 이름과 연락처는 물론 통관번호, 주소, 현관 출입 정보 등 일상과 안전에 직결된 정보까지 유출되는 심각한 위험이 현실이 되었습니다.

그럼에도 현행법은 핵심적인 안전조치의 구체적 내용과 대규모 사업자에게 요구되는 추가 조치를 주로 하위 법령에 맡기고 있어, 책임과 의무가 법률에 충분히 반영되어 있지 않습니다. 이로 인해 피해 사실 확인, 비밀번호 변경, 계정 보호 조치 등 대부분의 부담이 여전히 개별 이용자에게 전가되고 있습니다. 사전 대비를 소홀히 한 사업자가

유출 이후에도 적극적인 조치를 취하지 않는다는 비판이 커지고 있습니다.

이에 개인정보 보호조직의 구성·운영, 접근권한 관리, 접속기록의 보관 및 위·변조 방지 등 안전조치 의무의 기본 틀을 법률에 명확히 규정하고자 합니다. 대통령령으로 정하는 기준에 해당하는 개인정보처리자에게는 유출된 개인정보의 온라인 조회 수단 제공, 상담·피해구제 전담 창구 설치 등 추가적인 이용자 보호 조치를 이행하도록 하는 규정을 신설하려는 것입니다(제29조 및 제34조).

Ⅲ. 검토의견

1. 안전성 확보조치의 구체적 내용을 법률에 명시(안 제29조)

- 안 제29조는 개인정보 보호조직의 구성·운영, 접근 권한 관리, 접속기록의 보관 및 위·변조 방지 등 안전조치의무의 기본적인 사항을 법률에 명시하는 내용임.

현행	개정안
제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 <u>내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라</u> 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.	제29조(안전조치의무) ----- ----- ----- <u>다음 각 호에</u> <u>해당하는</u> ----- <u>확보</u> ----- ---.
<신설>	1. 제31조에 따른 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 조치
<신설>	2. 개인정보에 대한 접근 권한을 제한하기 위한 조치
<신설>	3. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
<신설>	4. 그 밖의 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치

□ 현행법 제29조에 따르면, 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 하고,

시행령 제30조에서 내부관리계획의 수립, 개인정보처리시스템에 대한 접근권한의 부여·변경·말소, 접속기록의 보관 및 위조·변조 방지 조치 등에 관한 사항 등을 구체적으로 정하고 있음.

「개인정보 보호법 시행령」

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다. <개정 2023. 9. 12.>

1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부 관리계획의 수립·시행 및 점검

가. 법 제28조제1항에 따른 개인정보취급자(이하 “개인정보취급자”라 한다)에 대한 관리·감독 및 교육에 관한 사항

나. 법 제31조에 따른 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항

다. 제2호부터 제8호까지의 규정에 따른 조치를 이행하기 위하여 필요한 세부 사항

2. 개인정보에 대한 접근 권한을 제한하기 위한 다음 각 목의 조치

가. 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템(이하 “개인정보처리시스템”이라 한다)에 대한 접근 권한의 부여·변경·말소 등에 관한 기준의 수립·시행

나. 정당한 권한을 가진 자에 의한 접근인지를 확인하기 위해 필요한 인증수단 적용 기준의 설정 및 운영

다. 그 밖에 개인정보에 대한 접근 권한을 제한하기 위하여 필요한 조치

3. 개인정보에 대한 접근을 통제하기 위한 다음 각 목의 조치

가. 개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치

나. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등으로서 보호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷망의 차단. 다

만, 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 이용자 수가 일일평균 100만명 이상인 개인정보처리자만 해당한다.

다. 그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치

4. 개인정보를 안전하게 저장·전송하는데 필요한 다음 각 목의 조치

가. 비밀번호의 일방향 암호화 저장 등 인증정보의 암호화 저장 또는 이에 상응하는 조치

나. 주민등록번호 등 보호위원회가 정하여 고시하는 정보의 암호화 저장 또는 이에 상응하는 조치

다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 통하여 정보주체의 개인정보 또는 인증정보를 송신·수신하는 경우 해당 정보의 암호화 또는 이에 상응하는 조치

라. 그 밖에 암호화 또는 이에 상응하는 기술을 이용한 보안조치

5. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 다음 각 목의 조치

가. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독

나. 개인정보처리시스템에 대한 접속기록의 안전한 보관

다. 그 밖에 접속기록 보관 및 위조·변조 방지를 위하여 필요한 조치

6. 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대해 컴퓨터바이러스, 스파이웨어, 랜섬웨어 등 악성프로그램의 침투 여부를 항상 점검·치료할 수 있도록 하는 등의 기능이 포함된 프로그램의 설치·운영과 주기적 갱신·점검 조치

7. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

8. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치

② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

□ 개정안은 현재 시행령에서 정하고 있는 안전조치 의무의 일부 내용을 법률에 상향하여 규정하려는 것으로, 개인정보 처리의 안전에 관한 중요한 사항을 법률에서 직접 정하는 것은 수범자의 예측가능성과 명확성 제고 측면에서 긍정적이라 할 것임. 현행법상 안전성 확보에 필요한 조치를 하지 않은 경우에는 과태료¹⁾가 부과되고, 안전성 확보 조치를 한 경우에는 과징금 면제 사유에 해당²⁾하는 등 제재 규정과도 연계되어 있으므로, 안전조치의 내용을 법률에 명시하는 것은 의미가 있음.

다만, 개인정보 침해 수단과 유형이 갈수록 다양해지고, 보안 환경과 기술의 변화 또한 빠르게 이루어지고 있으므로, 개인정보 보호를 위한 안전성 확보 조치의 구체적이고 세부적인 내용은 하위 법령으로 위임하여 규정할 필요성이 인정될 수 있다는 점도 함께 고려하여 논의할 필요가 있음. 현행법과 유사하게 안전조치의 구체적인 내용을 하위 법령에 위임하고 있는 입법례³⁾도 있음.

1) 「개인정보 보호법」

제75조(과태료) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

5. 제23조제2항·제24조제3항·제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·제29조(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자

2) 「개인정보 보호법」

제64조의2(과징금의 부과) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보처리자에게 전체 매출액의 100분의 3을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 20억원을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다.

9. 개인정보처리자가 처리하는 개인정보가 분실·도난·유출·위조·변조·훼손된 경우. 다만, 개인정보가 분실·도난·유출·위조·변조·훼손되지 아니하도록 개인정보처리자가 제29조(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

3) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제23조의6(연계정보의 안전조치 의무 등) ① 본인확인기관이 연계정보를 생성·처리하는 경우 「개인정보

□ 이와 관련하여 보호위원회는 개정 취지에는 공감하나, 조치의무의 세부적인 사항은 하위 법령에서 정하는 것이 적절하다는 입장이고,

한국인터넷기업협회는 세부적이고 기술적인 기준을 법률에 직접 규정할 경우 급변하는 보안 환경에 신속하게 대응하기 어려울 것이라는 우려를 제기함.

보호법」 제29조에 따른 조치 외에 연계정보 생성·처리의 안전성 확보를 위한 물리적·기술적·관리적 조치를 하여야 한다.

② 연계정보 이용기관은 제23조의5제1항 각 호에 따른 서비스를 제공하는 경우 「개인정보 보호법」 제29조에 따른 조치 외에 연계정보를 주민등록번호와 분리하여 보관·관리하고 연계정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 조치(이하 “안전조치”라 한다)하여야 한다.

③ 방송미디어통신위원회는 생성·처리하는 연계정보의 규모, 매출액 등이 대통령령으로 정하는 기준에 해당하는 본인확인기관의 물리적·기술적·관리적 조치 및 연계정보 이용기관의 안전조치에 대한 운영·관리 실태를 점검할 수 있다.

④ 방송미디어통신위원회는 제3항에 따른 점검에 관한 업무를 대통령령으로 정하는 전문기관에 위탁할 수 있다.

⑤ 제1항에 따른 물리적·기술적·관리적 조치와 제2항에 따른 안전조치에 관하여 필요한 사항은 대통령령으로 정한다.

「전자금융거래법」

제21조(안전성의 확보의무) ① 금융회사등은 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다.

② 금융회사등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치, 소요경비 등의 정보기술부문, 전자금융업무 및 「전자서명법」에 의한 인증서의 사용 등 인증방법에 관하여 금융위원회가 정하는 기준을 준수하여야 한다.

③ 금융위원회는 제2항의 기준을 정할 때 특정 기술 또는 서비스의 사용을 강제하여서는 아니 되며, 보안 기술과 인증기술의 공정한 경쟁이 촉진되도록 노력하여야 한다.

④ 대통령령으로 정하는 금융회사 및 전자금융업자는 안전한 전자금융거래를 위하여 대통령령으로 정하는 바에 따라 정보기술부문에 대한 계획을 매년 수립하여 대표자의 확인·서명을 받아 금융위원회에 제출하여야 한다.

「의료법」

제38조의2(수술실 내 폐쇄회로 텔레비전의 설치·운영) ④ 제1항에 따라 폐쇄회로 텔레비전이 설치된 의료기관의 장은 제2항에 따라 촬영한 영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 보건복지부령으로 정하는 바에 따라 내부 관리계획의 수립, 저장장치와 네트워크의 분리, 접속기록 보관 및 관련 시설의 출입자 관리 방안 마련 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

2. 개인정보 유출등에 따른 후속 조치 규정 (안 제34조제2항 후단 신설)

- 개정안은 개인정보가 유출등이 된 경우 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자에게 유출된 개인정보의 온라인 조회 수단 제공, 피해예방 방법의 안내, 상담·피해구제 전담 창구 설치 및 상담원 배치 등 추가적인 조치를 하도록 하는 내용임.

현 행 (2026. 3. 10. 개정, 2026. 9. 22. 시행 예정)	개 정 안
제34조(개인정보 유출 등의 통지·신고) ① (생략) ③ 개인정보처리자는 개인정보가 유출등이 된 경우에는 해당 개인정보의 회수·삭제 등 피해 확산을 방지하기 위한 조치를 포함하여 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다. <후단 신설> <신 설> <신 설>	제34조(개인정보 유출 등의 통지·신고) ① (현행과 같음) ② 개인정보처리자는 개인정보가 유출등이 된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다. <u>이 경우 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 다음 각 호의 조치를 하여야 한다.</u> <u>1. 유출등이 된 개인정보의 정보주체가 온라인을 통하여 자신의 개인정보 유출 여부 및 유출등이 된 항목을 확인할 수 있는 수단의 제공</u> <u>2. 유출등이 된 개인정보의 내용 및 특성을 고려한 비밀번호 변경, 계</u>

현 행 (2026. 3. 10. 개정, 2026. 9. 22. 시행 예정)	개 정 안
<u><신 설></u> ③ · ④ (생 략)	<u>정 보호, 금융사기 예방 등을 위한</u> <u>구체적인 피해 예방 방법의 안내</u> <u>및 지원</u> 3. <u>유출등이 된 개인정보와 관련한</u> <u>상담 · 피해 구제 신청을 전담하는</u> <u>창구의 개설 및 상담요원의 배치</u> ③ · ④ (현행과 같음)

□ 법 제34조⁴⁾는 개인정보가 유출등이 되었음을 알게 된 경우 정보주체에게 유출등이 된 개인정보의 항목, 경위, 피해 최소화를 위해 취할

4) 「개인정보 보호법」 (2026. 3. 10. 개정, 2026. 9. 11. 시행 예정)

제34조(개인정보 유출등의 통지·신고) ① 개인정보처리자는 개인정보가 유출등이 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. <개정 2023. 3. 14., 2026. 3. 10.>

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 구체적인 정보
 4. 개인정보처리자의 대응조치 및 피해 구제절차
 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
 6. 개인정보 유출등으로 인한 제39조에 따른 손해배상과 제39조의2에 따른 법정손해배상의 청구 및 제43조에 따른 분쟁조정 등 피해를 입은 정보주체의 법적 권리와 그 행사 방법 등에 관한 정보
 7. 그 밖에 개인정보가 유출등이 된 정보주체의 보호를 위하여 대통령령으로 정하는 사항
- ② 제1항에도 불구하고 개인정보의 유형, 정보주체에게 미치는 영향 및 유출등의 위험 정도를 고려하여 대통령령으로 정하는 유출등의 가능성이 있음을 알게 되었을 때에는 지체 없이 유출등의 가능성이 있는 모든 정보주체에게 피해를 최소화하기 위한 정보 등 대통령령으로 정하는 사항을 알려야 한다. <신설 2026. 3. 10.>
- ③ 개인정보처리자는 개인정보가 유출등이 된 경우에는 해당 개인정보의 회수·삭제 등 피해 확산을 방지하기 위한 조치를 포함하여 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다. <개정 2023. 3. 14., 2026. 3. 10.>
- ④ 개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 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. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4., 2023. 3. 14., 2026. 3. 10.>
- ⑤ 제1항·제2항에 따른 통지 및 제4항에 따른 유출등의 신고의 시기, 방법, 절차 등에 필요한 사항은 대통령령으로 정한다. <개정 2023. 3. 14., 2026. 3. 10.>

수 있는 방법, 신고 접수 부서 및 연락처, 손해배상 청구 및 분쟁조정 등 정보주체의 권리와 행사 방법 등에 관한 정보 등을 통지하도록 하고 있으며, 법 제75조5)에 따라 이를 위반한 경우에는 3천만원 이하의 과태료가 부과됨.

법 제34조제2항에서는 개인정보 유출등의 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하도록 하고 있으나, 그 구체적인 내용에 대해서는 법률에서 정하고 있지 않음.

이에 개정안은 일정 규모 이상의 개인정보처리자에 대해서는 유출 정보의 온라인 조회 수단 제공, 피해예방 방법의 안내, 상담·피해구제 전담 창구 설치 및 상담원 배치 등의 조치를 하도록 법률에 명시함으로써, 개인정보 유출등에 따른 피해에 대한 원활한 대응 및 신속하고 충분한 피해구제를 도모하려는 것으로 그 취지는 긍정적임.

□ 다만, 개정안에 대해서는 현행법의 내용과의 중복성 등을 고려하여 논의할 필요가 있음.

개정안 제34조제2항 각 호에서는 개인정보의 유출등이 있는 경우 개인정보처리자가 취해야 할 조치를 정하고 있고, 현행법 제34조제1항에서는 개인정보 유출등의 경우 개인정보처리자가 정보주체에게 통지해야

5) 「개인정보 보호법」 (2026. 3. 10. 개정, 2026. 9. 11. 시행 예정)

제75조(과태료) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

17. 제34조제1항 또는 같은 조 제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 제34조제1항 각 호의 사항 또는 같은 조 제2항의 피해를 최소화하기 위한 정보 등의 사실을 알리지 아니한 자

하는 항목을 규정하고 있음.

법 제34조제1항6)에 따른 통지 항목	개정안 제34조제2항 각 호에 따른 후속조치 항목
1. 유출등이 된 개인정보의 항목 2. 유출등이 된 시점과 그 경위	1. 유출등이 된 개인정보의 정보주체가 온라인을 통하여 자신의 개인정보 유출 여부 및 유출등이 된 항목을 확인할 수 있는 수단의 제공
3. 유출등으로 인하여 발생할 수 있는 피 해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 구체적인 정 보	2. 유출등이 된 개인정보의 내용 및 특성 을 고려한 비밀번호 변경, 계정 보호, 금융사기 예방 등을 위한 구체적인 피 해 예방 방법의 안내 및 지원
4. 개인정보처리자의 대응조치 및 피해 구제절차	
5. 정보주체에게 피해가 발생한 경우 신 고 등을 접수할 수 있는 담당부서 및 연락처	3. 유출등이 된 개인정보와 관련한 상담 · 피해 구제 신청을 전담하는 창구의 개설 및 상담요원의 배치
6. 개인정보 유출등으로 인한 제39조에 따른 손해배상과 제39조의2에 따른 법 정손해배상의 청구 및 제43조에 따른 분쟁조정 등 피해를 입은 정보주체의 법적 권리와 그 행사 방법 등에 관한 정보 <2026. 3. 10. 신설>	
7. 그 밖에 개인정보가 유출등이 된 정보 주체의 보호를 위하여 대통령령으로 정 하는 사항 <2026. 3. 10. 신설>	

법 제34조제1항은 개인정보 유출등의 경우 개인정보처리자가 통지해야
할 항목을 정하고 있고, 개정안 제34조제2항은 개인정보처리자가 취해

6) 2026. 3. 10. 개정, 2026. 9. 11. 시행 예정 법률

야 할 각종 조치 의무를 부과하려는 것으로서 차이가 있으나,

현행법 제75조에 따르면 제34조제1항을 위반하여 같은 항 각 호의 사실을 알리지 않은 경우 과태료가 부과되므로, 개인정보처리자에게는 통지 항목에 포함된 사항을 조치하여 통지할 의무가 있는 것이어서, 사실상 조치 의무가 포함되어 있으므로, 개정안의 내용과 현행법의 규정이 중복되는 측면이 있음.

- 또한, 2026. 3. 10. 개정으로 개인정보 유출등의 가능성이 있는 경우에도 유출등의 가능성이 있는 모든 정보주체를 대상으로 피해 최소화를 위한 정보를 알리도록 통지 의무가 강화되고, 피해 최소화 대책에 ‘해당 개인정보의 회수·삭제 등 피해 확산을 방지하기 위한 조치’를 포함하도록 하는 등 일부 보완이 이루어졌다는 점도 참고할 필요가 있음.

개정 전	2026. 3. 10. 개정내용
제34조(개인정보 유출등의 통지·신고) <신 설> ② 개인정보처리자는 개인정보가 유출등이 된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.	제34조(개인정보 유출등의 통지·신고) ② <u>제1항에도 불구하고 개인정보의 유형, 정보주체에게 미치는 영향 및 유출등의 위험 정도를 고려하여 대통령령으로 정하는 유출등의 가능성이 있음을 알게 되었을 때에는 지체 없이 유출등의 가능성이 있는 모든 정보주체에게 피해를 최소화하기 위한 정보 등 대통령령으로 정하는 사항을 알려야 한다.</u> ③ 개인정보처리자는 개인정보가 유출등이 된 경우에는 <u>해당 개인정보의 회수·삭제 등 피해 확산을 방지하기 위한 조치를 포함하여</u> 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

□ 한편, 개정안에서는 피해 상담 및 구제 신청을 ‘전담’하는 창구 개설 및 상담요원 배치를 하도록 정하고 있음. 해당 사건만 ‘전담’하는 창구와 인력을 운영하도록 하는 것은 개인정보처리자의 여건에 따라 부담이 될 수 있으나, 개정안은 일정 규모 이상의 개인정보처리자로 한정하여 의무를 부여하려는 것이라는 점, 개인정보 유출등이 있는 경우 다수의 피해자가 발생하는 것이 일반적이므로 사고 초기에 집중되는 신고 처리 및 상담에 대응하기 위해서는 상담 창구 운영이 사실상 필수적일 것이라는 점에서 개정안의 취지는 타당해 보임. 현행법 제34조에서도 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처를 피해자에게 통지하도록 하고 있음.

다만, 이에 대해 한국인터넷기업협회는 사실관계가 확정되지 않은 초기 단계에서는 기존 통지 내용 이상의 정보를 제공하기 어려운 구조적 한계가 있고, 원인 분석 및 추가 유출 차단, 보안 취약점 보완 등 사고 대응과 복구에 집중할 인력과 자원이 분산될 우려가 있으며, 상당한 비용과 행정적 부담이 우려된다는 의견을 제시함.

문 의 처
02)6788-5104