



제438회국회(임시회)
제2차 정무위원회

개인정보 보호법 일부개정법률안

검 토 보 고

〈 개인정보처리시스템 접속권한 관리 규정의
법률 상향 및 과태료 부과 근거 마련 〉

■ 조지연의원 대표발의(의안번호 제2217377호)

2026. 8.

정 무 위 원 회

수석전문위원 곽 현 준

목 차

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

I. 제안경위

1. 제 안 자: 조지연의원 등 10인
2. 제 안 일: 2026. 3. 11.
3. 회 부 일: 2026. 3. 12.

II. 제안이유 및 주요내용

현행법상 개인정보처리자는 개인정보가 안전하게 관리될 수 있도록 개인정보취급자의 범위를 최소한으로 제한하고, 이들에 대한 적절한 관리·감독을 하도록 규정하고 있음.

그런데 최근 퇴직자 등이 기존에 부여받은 개인정보처리시스템 접근 권한을 이용하여 개인정보를 유출하는 사고 등 개인정보 침해 사고가 발생함에 따라 개인정보 접근 권한에 대한 사항을 법률로 명확하게 정하여야 할 필요가 있다는 의견이 있음.

이에 개인정보보호위원회의 고시로 정하고 있던 개인정보취급자의 개인정보처리시스템 접근 권한에 대한 사항을 법률로 상향하고, 위반 시 과태료를 부과하도록 하여 개인정보 보호와 관리·감독의 실효성과 책임성을 강화하려는 것임(안 제28조제3항 및 제4항 신설 등).

Ⅲ. 검토의견

- 개정안은 현재 개인정보보호위원회의 고시에서 규정하고 있는 개인정보취급자의 개인정보처리시스템 접속권한 관리에 대한 사항을 법률에 상향하여 규정하고 이를 위반하는 경우 과태료를 부과하려는 것임(안 제63조의2 및 제66조제1항).

현행	개정안
제28조(개인정보취급자에 대한 감독) ① · ② (생략) <u><신설></u>	제28조(개인정보취급자에 대한 감독) ① · ② (현행과 같음) ③ <u>개인정보처리자는 개인정보취급자의 업무 또는 개인정보취급자가 변경되었을 경우 지체 없이 데이터 베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성된 시스템에 대한 접근 권한을 변경 또는 말소하여야 한다.</u> ④ <u>개인정보처리자는 제3항에 따라 접근 권한이 변경·말소된 개인정보취급자에 대한 현황을 3년 이내의 범위에서 대통령령으로 정하는 바에 따라 보관·관리하여야 한다.</u>
제75조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다. 1. · 2. (생략) <u><신설></u>	제75조(과태료) ① ----- ----- ----- 1. · 2. (현행과 같음) 3. <u>제28조제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반</u>

현행	개정안
② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다. 1. ~ 12. (생략) <u><신설></u> 13. ~ 27. (생략) ③ ~ ⑤ (생략)	<u>하여 개인정보취급자의 접근 권한을 변경 또는 말소하지 아니한 자</u> ② ----- -----. 1. ~ 12. (현행과 같음) <u>12의2. 제28조제4항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 접근 권한이 변경·말소된 개인정보취급자에 대한 현황을 보관·관리하지 아니한 자</u> 13. ~ 27. (현행과 같음) ③ ~ ⑤ (현행과 같음)

□ 현행법은 개인정보처리자에게 개인정보를 처리함에 있어 개인정보가 안전하게 관리될 수 있도록 개인정보취급자의 범위를 최소한으로 제한하고, 적절히 관리·감독하며, 정기적으로 필요한 교육을 실시하여야 한다고 규정하고 있고,¹⁾

시행령에서는 개인정보처리시스템에 대한 접근 권한의 부여·변경·말소 등에 관한 기준을 수립·시행하도록 하고 있음.²⁾

1) 「개인정보 보호법」

제28조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자(이하 “개인정보취급자”라 한다)의 범위를 최소한으로 제한하고, 개인정보취급자에 대하여 적절한 관리·감독을 하여야 한다.

② 개인정보처리자는 개인정보의 적절한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

○ 그리고 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시)을 통해 개인정보처리자에게 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하고, 그 내역을 기록하여 최소 3년간 보관하도록 규정하고 있음.³⁾

□ 그런데 최근 쿠팡에서 근무하던 당시 대체 인증⁴⁾을 직접 개발했던 전직 직원('24년말 퇴사)이 대체 인증 서명키를 획득한 이후 사전 유출 테스트 과정('25.1.)을 거쳐 '25년 4월부터 11월까지 회원정보 수정 페이지, 배송지 관리 및 주문목록 페이지 등을 조회하며 대량의 개인정보를 유출하는 일이 발생함에 따라 엄격한 접근권한 관리 등 안전조치 강화가 필요하다는 지적이 제기되고 있음.

2) 「개인정보 보호법 시행령」

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.

2. 개인정보에 대한 접근 권한을 제한하기 위한 다음 각 목의 조치

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

3) 「개인정보의 안전성 확보조치 기준」

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.

② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.

⑥ 개인정보처리자는 정당한 권한을 가진 자만이 개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 한다.

4) 쿠팡은 이용자가 ID/PW 등을 통해 로그인한 이후, 별도 재인증 절차 없이 서비스를 이용할 수 있도록 인증토큰을 발급하는 인증 체계를 운영하면서, 시스템의 가용성 및 신뢰성 확보를 위해 백업 인증 목적으로 대체 인증을 개발·운영('24.4.)

- 이에 개정안은 현재 개인정보보호위원회의 고시에서 규정하고 있는 개인정보취급자의 개인정보처리시스템 접근 권한 관리에 대한 사항을 법률에 상향하여 규정하고 이를 위반하는 경우 과태료를 부과하려는 것으로, 개인정보 보호와 관리·감독의 실효성과 책임성을 강화하여 개인정보를 보다 두텁게 보호하려는 긍정적인 취지로 보임.
- 다만, 개인정보보호위원회는 현재도 안전조치 의무 위반 시 3천만원 이하의 과태료가 부과되고 있는 상황에서 개정안을 적용할 경우 3천만원 또는 5천만원의 과태료가 추가로 부과될 수 있어 개인정보처리자에게 과도한 부담을 초래할 우려가 있으므로 신중한 검토가 필요하다는 의견을 제출한바, 해당 의견을 고려할 필요가 있을 것으로 보임.
- 개정안에 대하여 한국온라인쇼핑협회 및 한국인터넷기업협회는 현행 고시의 법적 구속력 및 실효성이 충분하여 개정이 불필요하고, 세부적인 안전조치 기준을 법률에 직접 규정하는 것은 법체계의 정합성을 저해하고 기술환경 변화에 대한 규제 경직성을 초래할 수 있다는 입장임.

문 의 처

02)6788-5108