SHIN&KIM
법무법인(유) 세종

개인정보 유출 사전예방 강화를 위한 개인정보 보호법 시행령 개정안 입법예고

2026.06.04

2026년 3월, 개인정보의 보호를 강화하고 기업의 책임을 명확히 하는 내용으로 「개인정보 보호법」이 개정되어(이하 '**개정법**') 오는 9월 시행을 앞두고 있습니다. 이와 관련하여 개정법에서 위임한 사항을 규정한 「개인정보 보호법 시행령」 개정안(이하 '**시행령 개정안**')이 최근 입법예고(6.1. ~ 7.13.) 되었습니다.

시행령 개정안은 ▲대표자 등의 책임 명확화 및 CPO 역할 강화, ▲개인정보 보호 인증 의무화, ▲유출 가능성 통지제 도입 및 통지 항목 확대, ▲반복·중대 개인정보 침해에 대한 과징금 강화 등을 주요 내용으로 담고 있습니다. 이는 개정법의 취지를 반영하여 개인정보 처리자의 책임성을 강화하고 정보주체의 권익을 실질적으로 보호하기 위한 후속 조치에 해당하는 내용입니다.

1. 대표자 등의 책임 명확화 및 CPO 역할 강화

가. 개정법 내용

개정법은 개인정보 보호책임자(CPO)가 기업 내에서 실질적인 독립성을 갖고 개인정보 보호 업무를 총괄할 수 있도록 법적 기반을 강화했습니다. 특히 CPO가 대표자나 이사회에 직접 보고하고, 그 업무 수행 결과를 평가받도록 함으로써 CPO의 위상을 격상시키는 동시에, 대통령령이 정한 기준에 해당하는 개인정보처리자의 경우 CPO의 지정, 그 지정의 변경·해제의 경우에는 이사회 의결을 거치고 개인정보보호위원회(이하 "개인정보위")에 신고하도록 하였습니다(법 제31조 제3항).

나. 시행령 개정안 내용

시행령 개정안은 CPO의 독립성과 전문성을 보장하기 위한 구체적인 요건을 규정했습니다.

먼저, CPO를 지정하거나 그 지정을 변경·해제하는 경우, **이사회 의결을 거치고 개인정보보호위원회(이하 "개인정보위")에 신고해야 하는 개인정보처리자의 기준을 마련**하였습니다. 구체적으로, 연 매출액·수입이 1,800억원 이상이면서, 5만명 이상 정보주체에 관하여 민감·고유식별정보를 처리하는 자 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자, 재학생 수 2만명 이상인 대학, 상급종합병원, 공공시스템운영기관은 이사회 의결 및 개인정보위 신고가 의무화됩니다. 이는 현행법상 전문 CPO 지정 의무 대상과 동일합니다(개정안 제32조제2항).

또한, **CPO 지정·변경·해제 시 신고 방법·절차를 구체화**하였습니다. 신고 의무 대상자(개인정보처리자)는 의무가 발생한 날로부터 1개월 이내(부득이한 사유시 1개월 연장 가능) 신고서를 개인정보위에 제출하여야 합니다(개정안 제32조제3항).

2. 개인정보 보호 인증 의무화

가. 개정법 내용

개정법은 정보보호 및 개인정보보호 관리체계 인증(ISMS-P)의 법적 근거를 명확히 하고, 일정 기준에 해당하는 개인정보처리자에게 인증 취득을 의무화하면서 그 구체적인 기준을 시행령에서 정하도록 위임하였습니다(법 제32조의2).

나. 시행령 개정안 내용

시행령 개정안은 ISMS-P 인증 의무 대상이 되는 범위를 구체화하고 있습니다. **① 공공시스템운영기관** 중 보호위원회가 정하여 **고시하는 자 ② 이동통신사업자 ③ 본인확인기관 ④ 전년도 매출액이 1조원 이상**이고 **정보통신서비스 부문 전년도 매출액이 100억원 이상**이며 전년도 말 기준 직전 3개월 간 개인정보가 저장·관리되는 **국내 정보주체의 수**가 **일일평균 3천만명 이상**인 자는 **2028년 12월 31일**까지 의무적으로 ISMS-P 인증을 받아야 합니다(개정안 제34조의9).

3. 유출 가능성 통지제 도입 및 통지 항목 확대

가. 개정법 내용

개정법은 개인정보 유출등의 사고 발생 시 통지·신고 의무를 강화하는 한편, 대통령령이 정하는 유출등의 가능성이 있음을 알게 되었을 때에도 통지 및 신고를 하도록 하였습니다(법 제34조 제2항).

나. 시행령 개정안 내용

유출등 가능성 통지의 요건·시기·항목을 구체화하여, ① 개인정보처리시스템에 대한 불법적 접근을 알게 되었거나, ② 개인정보가 불법적으로 거래·유통되고 있음을 알게 된 때에는 72시간 이내에 정보주체에 통지하도록 하였습니다(개정안 제39조의2). 또한, 개정법에서 개인정보의 위조·변조·훼손도 분실·도난·유출과 같은 범주에 포함시켜 통지·신고를 하도록 규정함에 따라 이를 시행령 개정안에도 명시하였습니다(개정안 제30조의2제2항제1호).

4. 반복·중대 개인정보 침해에 대한 과징금 강화

가. 개정법 내용

개정법은 (i) 3년 내 고의·중과실에 의한 과징금 부과 대상 위반행위 반복, (ii) 고의·중과실에 의한 과징금 부과 대상 위반행위로 인한 피해 규모가 1천만명 이상, (iii) 시정명령 불이행으로 인한 개인정보 유출등과 같이 반복적이거나 중대한 개인정보 침해행위에 대한 과징금 상한액을 **'전체 매출액'의 10% 이하**로 대폭 상향하면서 구체적인 산정기준과 산정절차를 대통령령에 위임하였습니다(법 제64조의2 제2항, 제8항). 또한, 개인정보 보호를 위한 투자 등 대통령령으로 정하는 사유가 있는 경우 과징금을 감경하도록 하는 근거를 신설하여 사전적 예방투자를 유도하고자 하였습니다(법 제64조의2 제6항).

나. 시행령 개정안 내용

시행령 개정안은 **개정법의 강화된 제재 규정에 따라 반복·중대 개인정보 침해 사안에 대한 과징금 부과기준을 개선·정비**하였습니다. 구체적으로, 고의·중과실로 3년 내 위반행위 반복 및 1천만 명 이상 대규모 피해가 발생하는 등 법 제64조의2제2항 각 호의 어느 하나에 해당하는 경우, 위반행위의 중대성을 판단한 후 위반행위의 내용 및 정도, 경위 및 피해 규모(1천만 명 이상) 등을 종합 고려하여 가중하는 방식으로 기준금액을 산정하도록 하였습니다. 또한, 이후 가중·감경 등을 통해 전체 매출액의 최대 10%까지 과징금을 부과할 수 있도록 하였습니다(개정안 [별표 1의5] 제2호 가목 4)).

또한, 과징금 감경 사유를 ▲개인정보 보호를 위한 예산·인력·설비·장치 등의 투자 규모 및 지속성, ▲사업주 또는 대표자, 개인정보 보호책임자의 역할, 조직 및 인력 구성 등 개인정보 보호체계 운영 내용 및 수준, ▲개인정보 안전성 확보 조치 강화를 위한 추가 노력으로 구체화하고, 과징금 감경의 상한(40%) 및 법률에 따른 감경 제외 대상(고의 또는 중대한 과실)을 명시하였습니다(개정안 제60조의2제5항, [별표 1의5] 제2호 나목 등).

과징금 면제 사유와 관련하여는, 그 밖에 정보주체에게 피해가 발생하지 아니하였거나 경미한 경우로서 해당 개인정보처리자가 위반행위를 시정하고 개인정보위가 정하여 고시하는 기준에 해당되는 경우에 중소기업·소상공인 등이 법 제34조제4항에 따라 기술을 지원받아 위반행위를 시정하는 경우를 포함하도록 하였습니다(개정안 제60조의2제6항).

5. 시사점

- **(재무적 리스크의 대폭 확대)** 반복·중대 개인정보 침해행위에 관한 과징금 상한이 전체 매출액의 10% 이하로 상향됨에 따라, 향후 더욱 더 개인정보 유출 사고는 기업에 막대한 재무적 부담으로 작용할 수 있습니다. 이제부터라도 기업들은 개인정보 보호를 단순한 컴플라이언스 이슈가 아닌 핵심적인 경영 리스크로 인식할 필요가 있으며, 특히 이미 개인정보 침해행위로 과징금을 부과받은 바 있거나, 1천만 명 이상의 개인정보를 다루는 기업의 경우에는 더욱이 본 조항의 적용을 받지 않을 수 있도록 사전적으로 관리 체계를 재점검하는 것이 필수적입니다.
- **(CPO 역할 및 거버넌스 재정립)** CPO의 독립성 보장 및 자격요건 강화, ISMS-P 인증 의무 대상 확대에 따라 기업 내 개인정보 보호 거버넌스를 전반적으로 검토하면서 CPO를 중심으로 실질적인 보호 체계를 구축해야 합니다.
- **(정보주체 권리 강화에 따른 대응 체계 마련)** 유출 통지·신고 의무가 강화되고 정보주체의 유출 통지청구권이 신설됨에 따라, 기업은 ▲유출 사고 대응 프로토콜 ▲대외 공지 및 피해자 통지 절차 ▲분쟁 및 집단소송 대응 전략 등을 사전에 빠짐없이 마련해 두어야 합니다.
- **(사전 예방적 보호 체계의 중요성 증대)** 서비스 기획·설계 단계부터 개인정보 보호 요소를 내재화하는 '개인정보 보호 중심 설계(Privacy by Design)' 원칙의 중요성이 더욱 커졌습니다. 정보보호 투자 등 사전 예방 노력은 과징금 감경 사유가 될 수 있으므로, 사후 대응이 아닌 선제적인 보호 체계 구축에 집중해야 할 필요도 있습니다.

개정법과 시행령 개정안은 오는 9월부터 시행될 예정이므로, 기업들은 남은 기간 동안 개정 내용을 면밀히 검토하고 개인정보 보호 체계를 전반적으로 점검하여 법 시행에 따른 리스크를 최소화할 필요가 있습니다.

About Shin & Kim's ICT Group

법무법인(유) 세종 ICT그룹은 ICT 분야의 독보적인 전문성과 인적 네트워크를 보유하고 있으며, 고객들로부터 최근 수년간 가장 높은 평가를 받고 있습니다. 방송과 통신, 개인정보, 인터넷 IT 분야에서 축적된 역량을 바탕으로 방송·통신·ICT 규제 동향 파악 및 대관, 법제개선·입법컨설팅, 규제영향력 분석과 기업의 전략 수립 등에 대한 종합적인 법률자문을 제공하고 있습니다. 침해사고 대응 등과 관련하여서도 다양한 업무경험과 전문성을 보유하고 있으므로, 보다 전문적인 내용이나 궁금하신 사항이 있으면 언제든지 연락 주시기 바랍니다.

관련구성원

강신욱
대표변호사

02-316-4059
sokang@shinkim.com

안정호
변호사

02-316-2891
jhahn@shinkim.com

노진홍
변호사

02-316-1639
jhnoh@shinkim.com

윤호상
변호사

02-316-2584
hsyoon@shinkim.com

주해인
변호사

02-316-1825
hiju@shinkim.com

김유빈
변호사

02-316-1968
ybikim@shinkim.com