법무법인(유) 린

Tech Legal Insights

A.P.T. – Personal Information Protection Team 2026. 10.

개인정보 평가·인증의 새로운 의미
- 처리방침 후속점검과 ISMS-P 심사 강화

최근 국정감사에서 2022년부터 올해 상반기까지 개인정보 유출 기업에 부과된 과징금이 7,000억 규모에 이른다는 사실이 드러났습니다. 더욱이 9월 11일 시행된 개정 개인정보 보호법에 따라 반복적이거나 중대한 위반에 대해서는 전체 매출액의 최대 10%까지 과징금이 부과될 수 있게 되어, 침해사고가 기업에 미치는 재무적 부담은 한층 커졌습니다. 특히 최근 개인정보위의 정책 방향은 침해사고 발생 이후의 책임만을 묻는 것이 아니라, 사고 이전에 개인정보 보호체계를 얼마나 충실히 구축·운영하였는지를 평가하는 방향으로 이동하고 있습니다. 개인정보 보호 인증의 보유나 개인정보 보호를 위한 예산·인력 투자와 같이 사고 발생 전에 이미 형성된 사실들이 과징금 감경의 근거가 됩니다. 이번에 발표된 처리방침 후속점검과 ISMS-P 심사제도 개편 역시 이러한 흐름의 연장선상에 있습니다.

이러한 점에서, 개정 개인정보 보호법에 따른 위반 이후 제재 체계의 주요 변경 사항을 살펴본 지난 TLI에 이어, 이번 TLI에서는 사고 이전의 관리 수준이 확인되고 기록으로 남는 처리방침 평가와 ISMS-P 인증·사후심사 단계에서 기업에 요구되는 대응을 짚어봅니다.

1. 평가·인증 이후의 사후점검 강화

개인정보보호위원회(이하 "개인정보위")는 최근 두 건의 조치를 함께 발표했습니다. 2025년 개인정보 처리방침 평가에서 '미흡' 평가를 받은 사업자에 대한 후속점검 결과와 그에 따른 5개 사업자에 대한 개선권고,[1] 그리고 정보보호 및 개인정보보호 관리체계(이하 "ISMS-P") 인증심사 개선을 위한 「개인정보 보호법 시행령」(이하 "시행령") 개정안 입법예고[2]입니다.

두 조치는 대상과 절차를 달리하지만, 평가나 인증이라는 일회적 절차가 종료된 이후에도 감독당국이 개인정보처리자의 실제 운영 상태를 계속 확인한다는 점에서 맥락을 같이합니다. 처리방침 평가제와 ISMS-P는 본래 개인정보처리자의 자율적인 개선을 유도하는 수단으로 설계되었으나, 이제는 후속점검·개선권고, 현장심사·인증취소와 결합되면서 감독 체계의 일부로 기능하고 있습니다.

Contact

구태언 변호사
T. 02-3477-8695
E. tekoo@law-lin.com

안서연 변호사
T. 02-3477-8695
E. syahn@law-lin.com

천희승 변호사
T. 02-3477-8695
E. hscheon@law-lin.com

2. 개인정보 처리방침: 평가 이후의 후속점검

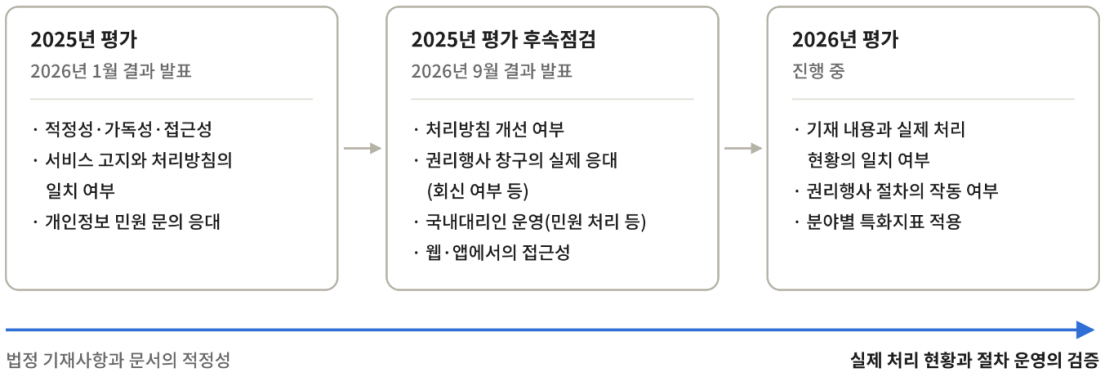
가. 평가에서 후속점검·개선권고로 이어지는 구조

처리방침 평가는 「개인정보 보호법」(이하 "법") 제30조의2에 근거해 2024년부터 매년 실시되고 있습니다. 개인정보 처리방침 평가에 관한 고시는 평가 결과 개선이 필요한 경우 법 제61조제2항에 따른 개선권고와 법 제66조에 따른 결과 공표 등을 명할 수 있도록 하고 있습니다. 이번 발표는 평가 결과에 따른 후속 조치가 실제로 이루어진 사례입니다. 개인정보위는 미흡 사업자에게 결과를 통보하고, 신청한 사업자에게는 평가위원이 현장을 방문해 개선 방법을 안내한 뒤, 처리방침 개선 여부, 정보주체 권리행사 창구 운영, 국내대리인 운영, 웹·모바일 앱에서의 처리방침 접근성 등을 다시 점검해 개선사항의 이행 여부를 확인했습니다.

나. 평가 대상의 확대: 문서 검토에서 실제 운영 점검으로

처리방침 평가는 법 제30조의2에 따라 처리방침이 법정 기재사항을 적정하게 정하고 있는지(적정성), 알기 쉽게 작성되었는지(가독성), 정보주체가 쉽게 확인할 수 있는 방법으로 공개되어 있는지(접근성)를 평가하는 제도입니다. 최근의 평가는 이에 더하여 처리방침의 기재 내용이 실제 개인정보 처리 현황과 부합하는지, 그리고 처리방침에 안내된 권리행사 절차 등이 실효적으로 운영되고 있는지까지 확인하면서 검증의 범위를 넓혀가고 있습니다. 특히 이번 후속점검에서 개선권고의 대상이 된 것은 처리방침의 문구가 아니라 정보주체의 권리행사 창구 운영체계와 국내대리인 운영에 대한 관리·감독이었습니다.

처리방침의 평가 대상이 기재 내용에 더해 실제 운영 실태까지 확대되고 있습니다



麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.

다. 개선권고 사항의 법적 의미

개선권고는 그 자체로 제재 처분은 아닙니다. 그러나 후속점검에서 확인된 사항은 상당 부분 법적 의무와 직접 맞닿아 있는 것들이 있습니다. 예컨대 국내대리인에 대한 관리·감독 의무(법 제31조의2 제3항)를 위반하면 2,000만원 이하의 과태료가, 정보주체의 열람을 부당하게 제한하거나 거절하면(법 제35조제3항) 1회 위반 시 900만원, 3회 이상 위반 시 3,000만원의 과태료가 부과될 수 있습니다(시행령 별표 2). 이처럼 권고의 계기가 된 사실이 법적 의무 위반에 해당할 경우, 개선권고와는 별개로 과태료 부과나 시정조치 명령의 대상이 될 수 있습니다.

아울러 시행령은 처리방침의 수립·변경 및 시행을 개인정보 보호책임자(이하 "CPO")의 업무로 규정하고 있습니다(시행령 제32조제5항제1호). 따라서 처리방침 평가와 후속점검에 대한 대응은 단순한 문서 관리가 아니라 CPO가 책임지는 개인정보 보호 거버넌스의 문제로 다루어야 합니다.

3. ISMS-P: 인증 이후의 상시 검증

가. 법정 인증취소 사유와 집행 현황

법 제32조의2는 인증 이후의 관리 장치를 이미 두고 있습니다. 개인정보위는 인증의 실효성 유지를 위해 연 1회 이상 사후관리를 실시해야 하고(제4항), ① 거짓 등 부정한 방법으로 인증을 받은 경우, ② 사후관리를 거부 또는 방해한 경우, ③ 인증기준에 미달하게 된 경우, ④ 개인정보 보호 관련 법령을 위반하고 그 위반사유가 중대한 경우에는 인증을 취소할 수 있습니다(제3항, ①의 경우 필요적 취소). 그러나 이번 국정감사에서 공개된 자료에 따르면, 2021년부터 2026년 상반기까지 ISMS-P 인증기업에서 발생한 침해사고는 115건에 이르지만 인증이 취소된 사례는 한 건도 없었습니다. 이는 인증제도의 실효성에 대한 문제 제기로 이어졌고, 이번 시행령 개정안 역시 인증 취득 여부뿐 아니라 인증 유지 상태에 대한 사후 검증을 강화하려는 취지로 이해됩니다.

나. 이번 시행령 개정안의 의미

9월 16일 입법예고된 시행령 개정안은 2026년 4월 정부가 발표한 「정보보호 및 개인정보보호 관리체계 인증제 실효성 강화방안」[3] 을 구체화한 것으로, 주요 내용은 다음과 같습니다.

麟舜
서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.

항목	개정안 내용
서면·현장심사 병행	인증심사와 매년 실시하는 사후심사에서 서면심사와 현장심사를 병행할 수 있도록 규정 명확화(시행령 개정안 제34조의2제4항, 제34조의5)
사고 시 기술점검	인증 유효기간 중 침해사고·유출이 발생한 경우 일정 자격[4]을 갖춘 기술인력이 현장에서 점검도구를 활용하여 취약점 진단·모의침투 수행(시행령 개정안 제34조의2제4항 단서)
인증기준 차등 적용	개인정보 처리규모, 사회적 파급력 등을 고려한 인증기준 차등 적용에 대한 근거 마련(시행령 개정안 제34조의2)
인증취소 시 과태료 유예	인증 의무대상자가 인증취소 처분을 받은 경우 인증 취득 의무 위반 과태료를 1년간 유예(거짓·부정한 방법으로 인한 취소는 제외)

특히 과태료 유예 조항은 인증 의무대상자의 인증이 취소될 경우 곧바로 인증 취득 의무 위반에 따른 과태료 부과로 이어지지 않도록 하는 장치입니다. 인증이 취소된 의무대상자에게 1년의 기간 동안 재발방지 대책을 수립하고 새로운 인증을 다시 취득할 기회를 부여하되, 거짓이나 부정한 방법으로 인증을 받아 취소된 경우는 제외했습니다. 2027년 7월 ISMS-P 인증 의무화를 앞두고, 인증취소가 의무대상자에게 미치는 법적 효과를 미리 정리한 것이라는 점에서 의미가 있습니다.

다. 인증 의무화 일정

법 제32조의2 제1항 단서에 따른 ISMS-P 인증 의무화는 기업·기관의 예산 확보에 소요되는 기간을 고려해 2027년 7월 1일부터 시행됩니다. 의무 대상은 매출액, 개인정보의 처리 규모 등을 고려하여 대통령령으로 정하도록 되어 있고, 2026년 6월 입법예고된 시행령 개정안은 이동통신사업자, 본인확인기관, 그리고 전년도 매출액 1조원 이상이면서 정보통신서비스 부문 매출액이 100억원 이상이며 전년도 말 기준 직전 3개월간 개인정보가 저장□ 관리되는 국내 정보주체 수가 일일평균 3천만명 이상인 사업자 등에 2028년 12월 31일까지 인증을 취득할 것을 요구했으나,[5] 9월 10일 공포된 개정 시행령은 이에 대한 규정을 두고 있지 않습니다.

이처럼 인증 의무화의 시행일은 확정되었으나 의무 대상과 취득 기한은 아직 정해지지 않은 상황입니다. 따라서 관련 기업들은 향후 시행령 개정 동향을 지속적으로 확인할 필요가 있습니다. 아울러 인증 준비에는 상당한 기간이 소요되므로, 기준이 확정되기 전이라도 인증 범위와 대응 체계를 미리 점검해 두는 것이 바람직합니다.

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.

4. 사고 이전의 관리 이력이 제재에 미치는 영향

처리방침의 후속점검과 ISMS-P 인증 이후의 사후심사가 기업에 실질적인 의미를 갖는 이유는, 개정법이 과징금 부과 여부를 판단하고 그 금액을 산정하는 각 단계에 사고 이전의 관리 이력을 반영하도록 하고 있기 때문입니다. 9월 11일 시행된 개정법과 시행령 별표 1의5를 기준으로 그 내용을 정리하면 다음과 같습니다.

가. 과징금 부과 여부 판단 및 산정 단계

먼저 유출에 대한 과징금은 개인정보처리자가 법 제29조에 따른 안전성 확보에 필요한 조치를 다한 경우에는 부과되지 않습니다(법 제64조의2 제1항 제9호 단서). 평시의 안전조치 이행 여부가 과징금 부과 여부 자체를 좌우하는 것입니다. 과징금이 부과되는 경우에도 기업이 사고 이전에 갖추어 둔 보호조치와 관리 체계가 각 산정 단계에서 다음과 같이 반영됩니다.

산정 단계	반영되는 사고 이전의 사실	조정 범위
기준금액 산정	암호화 등 안전성 확보 조치 이행 노력	위반행위의 중대성에 따라 부과기준율 0.03%~2.7%(시행령 별표1의5)
투자감경	개인정보 보호 투자 규모·비율·지속성·증가정도, 대표자의 책임 이행 정도(법 제30조의3), CPO의 역할·조직·인력 구성 등 보호 체계 운영 수준, 법상 의무사항 이외의 강화된 보호기술의 적용 등 안전성 확보조치 수준이나 노력 등	기준금액의 40% 이하. 요건 충족 시 감경 의무(고의·중과실 제외)
2차 조정	개인정보 보호 인증, 자율적인 보호 활동	50% 범위에서 가중·감경
감경 제한	'매우 중대한 위반행위'에 해당하면 1·2차 조정 감경의 전부 또는 일부를 적용하지 않을 수 있음	—
징벌적 과징금	과징금 처분일부터 3년 내 같은 호의 위반 반복(고의·중과실), 고의·중과실 위반으로 1천만명 이상 피해, 시정조치 명령 불이행으로 인한 유출	전체 매출액의 10% 이하

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.

위 산정 요소 가운데 투자감경에 관해서는 개인정보위가 개정법 시행에 맞추어 「과징금 투자 감경제도 안내서」를 발간하고, 요건별 세부 기준과 필요 증빙서류를 구체적으로 제시했습니다. 안내서에 따르면, 투자감경은 위반행위가 있었던 사업연도의 직전 3개 사업연도 범위 내에서 조치한 사항을 대상으로 판단하고, 투자 규모는 감사보고서, 자산대장, 비용원장, 인건비 내역 등을 통해 확인합니다. 또한 안전조치에 관한 추가적 노력은 개인정보 유출등이 발생한 시점에 적용·운영되고 있던 안전조치를 중심으로 고려하며, 이러한 조치는 내부 관리계획에 명문화되고 증빙을 통해 확인되어야 합니다.

5. 시사점

앞서 살펴본 조치들은 개인정보 평가·인증과 과징금 제재가 별개의 영역으로 다루어질 수 없음을 보여줍니다. 평가·인증 과정에서 확인된 사실은 그 절차 안에서 끝나지 않고, 침해사고가 발생했을 때 제재의 수준을 판단하는 자료로 다시 활용될 수 있습니다.

이와 함께 개인정보처리자의 관리 수준을 살피는 기준도 달라지고 있습니다. 처리방침 평가, ISMS-P 심사, 과징금 투자감경은 모두 관리 체계를 갖추었는지를 확인하는데 그치지 않고, 그것이 실제로 작동하고 있는지를 묻는 방향으로 나아가고 있습니다. 이러한 흐름에 비추어 보면, 개인정보 보호 업무는 개별 평가나 심사에 사안별로 대응하는 방식으로는 충분하지 않습니다. 평시의 관리 활동이 이후 어느 단계에서든 일관된 근거로 제시될 수 있도록 체계적으로 운영하는 것이 중요합니다.

다만 ISMS-P 인증 의무 대상의 기준과 인증심사 개선을 위한 시행령 개정안의 최종 내용은 아직 확정되지 않았고, 투자감경 역시 실제 적용 사례가 축적되지 않은 상황입니다. 관련 기업들은 제도의 구체적인 운영 방향이 드러나는 과정을 지속적으로 살펴볼 필요가 있습니다.

***

법무법인(유) 린 APT(AI, Platform, Technology) 그룹 개인정보보호팀은 국내 기업들의 규제 이슈에 전략적인 원스톱(One-Stop) 토탈 솔루션(Total Solution)을 제공하고 있습니다.
상기 내용에 대해 문의사항이 있으시면 언제든지 법무법인(유) 린 APT(AI, Platform, Technology) 부문 개인정보보호팀(Tel. 02-3477-8695) 구태언 팀장(tekoo@law-lin.com), 안서연 변호사(syahn@law-lin.com), 천희승 변호사(hscheon@law-lin.com)에게 문의해 주시기 바랍니다.

1. 보도자료 | 개인정보보호위원회 〉〉 위원회 소식〉보도 · 해명 〉 상세보기
2. 보도자료 | 개인정보보호위원회 〉〉 위원회 소식〉보도 · 해명 〉 상세보기
3. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=11976
4. 「정보보호산업의 진흥에 관한 법률 시행규칙」 별표 1에 규정된 기술인력의 자격기준 중 중급 이상
5. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=12137

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.