2026년 개정 개인정보 보호법 — 9월 11일부터 무엇이 달라졌나

이현섭 변호사(법무법인 세움 파트너) · 기준일 2026-09-11 · 최신판: https://datalaw.kr/guides/pipa-2026-amendment/

핵심 요약 — 법률 제21445호(2026년 3월 10일 공포)가 **2026년 9월 11일** 시행됐습니다. 실무에 곧바로 걸린 변화는 넷입니다. ① 통지·신고 대상인 '유출등'에 **위조·변조·훼손**이 들어왔습니다(제23조 제2항). ② 제34조에 유출등의 **가능성 단계 통지**가 신설되면서 뒤 항이 밀려 **신고의 근거가 제3항에서 제4항으로** 이동했습니다. ③ 중대·반복 위반의 과징금 상한이 전체 매출액의 **100분의 10**이 됐습니다(제64조의2 제2항 신설). ④ 개인정보 보호책임자 지정에 **이사회 의결과 신고** 의무가 붙었고, 미지정·자격미달 지정에 과태료가 신설됐습니다(제31조 제3항, 제75조 제2항 제14호의2\~4). 이를 구체화할 시행령 개정령도 하루 전인 **2026년 9월 10일 대통령령 제36671호로 공포**되어 법률과 같은 날 시행됐습니다. 시행령은 이사회 의결·신고 대상을 연간 매출액등 1,800억 원 초과 등으로, 보호책임자 지정·변경·해제 신고 기한을 6개월(1년 범위 연장 가능)로, 시행 전에 지정한 보호책임자의 신고 기한을 시행일부터 6개월로 정했습니다. 앞서 개인정보위가 8월 21일 「개인정보 유출등 대응 매뉴얼」과 「과징금 투자 감경제도 안내서」의 초안을 공개해 실무 기준선을 먼저 내놓았습니다(의견제출은 9월 3일 마감됐고, 확정본은 9월 11일 현재 공개되지 않았습니다). 시행일에는 시행령이 다시 위임한 고시도 함께 시행됐습니다. 과징금 부과기준 고시(개인정보보호위원회고시 제2026-12호)가 투자감경과 10% 구간의 가중 판단기준을 정하고 인증 감경을 줄였으며, 과태료 부과기준 고시(제2026-14호)가 제정되고 보호책임자 신고서 서식(제2026-11호)이 생겼습니다.

PDF판 — 이 가이드를 PDF로 내려받아 사내·팀에 그대로 전달할 수 있습니다.

개정법은 2026년 9월 11일 시행됐습니다. 이 페이지는 흩어져 있는 글들을 **무엇이 바뀌었고 무엇이 남았는지** 순서대로 묶은 것입니다. 조문 단위 대조가 필요하면 바로 아래 대조표로, 특정 상황에 무엇이 달라졌는지가 궁금하면 해당 항목으로 들어가면 됩니다.

이미 걸린 것과 아직 남은 것

이미 시행된 것

날짜	무엇이	근거
2026년 8월 20일	본인전송요구권 관련 시행령 규정 시행	대통령령 제36121호
2026년 9월 11일	개정 개인정보 보호법 본체 시행	법률 제21445호 부칙 제1조
2026년 9월 11일	개정 시행령 시행 — 보호책임자 신고 절차, 유출 가능성 통지, 과징금 별표 1의5, 과태료 별표 2	대통령령 제36671호(2026. 9. 10. 공포) 부칙 제1조
2026년 9월 11일	개인정보위 고시 시행 — 과징금 부과기준 개정(투자감경·가중 판단기준·감경률 조정), 과태료 부과기준 제정, 보호책임자 지정·변경·해제 신고서 서식 신설	개인정보보호위원회고시 제2026-12호·제2026-14호·제2026-11호(2026. 9. 11.)

아직 남은 것

날짜	무엇이	근거
2027년 2월 20일	매출 1,800억 원 초과 민간 기업이 전송 요구를 받는 시점	시행령
2027년 3월 11일	시행 전에 이미 지정한 개인정보 보호책임자의 지정 신고 기한(이사회 의결·신고 대상 사업자에 한함)	시행령 개정령안 부칙 제2조

날짜	무엇이	근거
2027년 7월 1일	제32조의2 제1항 단서(인증 의무화), 제75조 제2항 제15호(인증 미이수 과태료)	법률 제21445호 부칙 제1조 단서

8월 20일과 9월 11일은 **서로 다른 개정**이었습니다. 앞의 것은 본인전송요구권(마이데이터) 시행령이고, 뒤의 것이 유출·과징금·보호책임자를 바꾼 법률 개정입니다. 둘을 하나로 묶어 두면 지금 무엇이 걸려 있는지가 뒤섞입니다.

조문이 정확히 어떻게 바뀌었나

바뀐 것을 조문 단위로 한자리에 놓으면 다음과 같습니다.

무엇이	2026년 9월 10일까지	2026년 9월 11일부터
유출등의 정의	조문마다 「분실·도난·유출·위조·변조 또는 훼손」을 나열	**제23조 제2항**이 「유출등」으로 정의를 통합. 위조·변조·훼손이 통지·신고 대상에 포함
유출 신고의 근거	제34조 **제3항**	**제34조 제4항** (뒤 항이 한 칸씩 이동)
유출 가능성 통지	없음	**제34조 제2항 신설** — 유출등의 가능성을 알게 된 때에도 통지 의무
유출 통지 기재사항	제34조 제1항 제1호\~제5호	제3호가 「**구체적인** 정보」로 강화되고 **제6호(손해배상·법정손해배상·분쟁조정 등 법적 권리와 행사 방법)·제7호 신설**
피해 최소화 조치	제34조 제2항	제34조 제3항으로 이동하면서 「**회수·삭제 등 피해 확산 방지 조치**」 명시
과징금 상한	전체 매출액의 **3%**	원칙 3%는 유지하되 **제64조의2 제2항 신설**로 세 경우에 **10%** — ① 처분일부터 3년 내 같은 호 재위반(고의·중과실) ② 고의·중과실로 피해 정보주체 1천만 명 이상 ③ 시정조치 명령 불이행
과징금 감경	재량	**제64조의2 제6항 신설** — 예산·인력·설비·장치를 투자·운영한 경우 「감경**한다**」(고의·중과실 제외)
보호책임자(CPO) 업무 조항	제31조 **제3항**	**제31조 제4항** (제3항\~제9항이 제4항\~제10항으로 이동)
CPO 지정 절차	없음	**제31조 제3항 신설** — 대통령령 기준에 해당하면 지정·변경·해제에 **이사회 의결**과 보호위원회 **신고**
CPO 업무 범위	7개 호	**제31조 제4항 제2호·제3호 신설** — 전문 인력 관리·예산 확보, 사업주·대표자 및 이사회 보고
사업주·대표자 책임	없음	**제30조의3 신설** — 개인정보 보호의 최종 책임자가 사업주·대표자임을 명시
CPO 관련 과태료	없음	**제75조 제2항 제14호의2\~제14호의4 신설** — 미지정·자격요건 미달, 이사회 의결 누락, 신고 누락

⚠≣ 위 표에서 **2027년 7월 1일에 시행되는 두 조항은 뺐습니다** — 제32조의2 제1항 단서(인증 의무화)와 제75조 제2항 제15호(인증 미이수 과태료)입니다. 9월 11일에 함께 시행된 것으로 읽으면 틀립니다.

항 번호가 이동한 조문이 여럿이라, 개정 내용을 이해하는 것과 별개로 **인용을 그대로 옮겨 쓰면 사고가 납니다.** 제34조·제64조의2·제31조를 개정 전 조문과 나란히 놓은 전체 대조표는 따로 두었습니다.

→ 2026년 9월 11일 시행 개정 개인정보 보호법 — 신구조문 대조표

시행일이 지났는데 아직 안 한 것이 있다면

시행 전에 준비를 끝내지 못한 회사가 지금 확인할 자리는 여섯입니다. 앞의 셋은 문서를 고치면 끝나고, 뒤의 셋은 의사결정이 필요합니다.

확인할 곳	그대로 두면	어디를 보나
사고대응 절차서·위·수탁 계약서·개인정보 처리방침의 **「법 제34조 제3항에 따른 신고」** 인용	그 인용이 지금은 다른 조항(피해 최소화 조치)을 가리킵니다	신구조문 대조표
같은 문서의 **「법 제31조 제3항」** 인용	보호책임자 업무는 제31조 제4항으로 옮겼습니다. 대법원도 같은 이유로 규칙을 고쳤습니다	아래 「개인정보 보호책임자를 다시 봐야 하나」
유출 **통지문 서식**	제34조 제1항에 제6호(손해배상·법정손해배상·분쟁조정 등 법적 권리와 행사 방법)·제7호가 신설돼 기재 항목이 늘었습니다	유출 사고 대응 가이드
사고대응 절차서의 **가능성 통지 분기**	유출이 확인되지 않아도 가능성을 알게 된 때부터 72시간 안에 통지해야 하는 경우가 생겼습니다(제34조 제2항)	아래 「유출 가능성 통지의 요건과 시계」
시행일에 **끝나지 않았던 위반 상태**	부칙 제3조 제2항이 그 상태에도 새 가중 규정을 적용합니다. 종료 시점이 요건 판단에 직접 걸립니다	과징금 상한이 어떻게 바뀌나
개인정보보호 투자액의 계정 관리	감경은 의무 조항이 됐지만 입증 부담은 회사 쪽입니다. 위반이 있었던 사업연도의 직전 3개 사업연도 이력을 봅니다	아래 「투자 감경은 산정 절차의 어디에 놓입니까」

여기부터는 상황별로 나눕니다.

유출 사고가 나면 무엇이 달라졌나

첫째, 신고·통지의 사정권이 넓어졌습니다. 개정법은 '유출등'의 정의를 제23조 제2항으로 올리면서 **위조·변조·훼손**을 더했습니다. 데이터가 밖으로 나간 정황이 없어도 파일이 훼손된 것만으로 통지·신고 의무가 붙을 수 있다는 뜻입니다. 랜섬웨어가 대표적인 경우입니다.

→ 랜섬웨어로 파일이 암호화만 됐다면 유출 신고를 해야 하나

둘째, 절차 자체는 지금도 같습니다. 개정법이 72시간을 새로 만드는 것이 아닙니다. 시계가 언제부터 도는지, 규모를 모르는 상태에서 무엇을 먼저 해야 하는지는 현행법에서 이미 정해져 있고, 그 절차는 아래 글이 조문 단위로 다룹니다.

→ 개인정보 유출을 인지했습니다 — 72시간 안에 해야 할 일과 하면 안 되는 일

셋째, 본사 플레이북을 쓰는 회사는 간극이 더 벌어집니다. GDPR 기준 절차서는 위험도 평가를 첫 분기점에 두지만, 한국법은 위험 정도를 요건으로 삼지 않습니다. 개정으로 통지 대상이 넓어져 이 차이가 커졌습니다.

→ 본사 인시던트 대응 플레이북을 한국에 그대로 적용할 수 있나

넷째, 실무 기준선은 이미 나와 있습니다. 개인정보위와 한국인터넷진흥원이 2026년 8월 21일 「개인정보 유출등 대응 매뉴얼」 개정 초안(2026. 9.판, 74면)을 공개해 9월 3일까지 의견을 받았습니다. 초안 기준으로 신설되는 가능성 통지가 붙는 상황은 두 가지입니다. 정보시스템에 불법 접근이 확인됐는데 로그가 없어 누구의 정보가 조회됐는지 특정하지 못하는 경우가 하나이고, 다크웹 판매글처럼 일부 유출이 확인됐고 같은 테이블의 다른 정보주체 정보도 유출됐을 수 있는 경우가 다른 하나입니다. 통지 기한은 가능성을 알게 된 때부터 **72시간** 이내인데, 확산 방지를 위한 긴급 조치가 필요하다는 사유로는 통지를 늦출 수 없습니다. 유출등의 통지는 그 사유로 지연할 수 있으므로 이 점이 두 통지의 실무상 차이입니다. 정보주체를 특정할 수 없으면 침해가 미칠 수 있었던 정보주체 전체에게 통지하는 것이 원칙이고, 기한 안에 실제 유출이 확인되면 유출등의 통지로 갈음합니다. 초안은 통지문 예시와 여섯 가지 필수 기재 항목까지 담고 있어, 사고대응 절차서에 가능성 통지 분기를 새로 그릴 때 출발점으로 삼을 만합니다. 다만 개인정보위 스스로 초안의 시행령 관련 문구가 바뀔 수 있다고 밝힌 상태입니다.

과징금은 얼마나, 어떤 경우에 올라가나

원칙은 그대로 전체 매출액의 100분의 3입니다. 새로 생긴 것은 **가중**과 **감경**입니다. 100분의 10은 재위반·대규모 피해·시정조치 불이행 세 경우에만 붙고, 반대로 신설된 제6항은 일정 사유가 있으면 "감경할 수 있다"가 아니라 "**감경한다**"고 적었습니다.

부칙에서 눈여겨볼 것은 제3조 제2항입니다. **9월 11일에 아직 끝나지 않았던 위반 상태는 새 가중 규정의 사정권에 들어옵니다.** 시행일에 종료되지 않은 위반이 남아 있었다면, 그 상태가 1천만 명 요건을 충족하는 순간 10% 구간이 열립니다. 진행 중인 상태를 지금이라도 끊어 두어야 하는 이유가 여기에 있습니다.

→ 2026년 9월 개정으로 과징금 상한이 어떻게 바뀌나 — 매출액 3%에서 10%로

가중이 어디까지 닿는지 못지않게 중요한 것이 감경 쪽입니다. 예방투자에 대한 감경은 고의·중과실이 없는 한 "감경한다"고 적힌 의무 조항이 됐지만, 감경 사유를 주장하고 입증하는 부담은 여전히 조사받는 회사 쪽에 있습니다. 출발점은 지금까지 어떤 사유가 실제로 인정돼 왔는지입니다. 2026년 공개된 결정문 세 건에는 위반으로 이득을 취하지 않은 점, 사전통지 전 시정 완료와 조사 협조, ISMS-P 인증 보유 같은 사유가 구체적인 감경 비율과 함께 기록돼 있습니다.

→ 과징금이 '전체 매출액'으로 바뀐 뒤 실제로 인정된 감경 사유

지금까지 실제로 얼마가 부과됐는지는 결정문 단위로 확인할 수 있습니다. 조문별로 갈라 보면 과징금이 붙는 자리와 과태료에 그치는 자리가 뚜렷하게 나뉩니다.

→ 개인정보 과징금·과태료 사례 건 — 개인정보위 제재 결정문 전수 DB

조문만 보면 무엇이 문제였는지는 알 수 없습니다. 접근통제를 두지 않은 것과 비밀번호를 평문으로 저장한 것과 접속기록을 남기지 않은 것이 모두 제29조 위반입니다. 개인정보위가 결정문의 「위법성 판단」 절에서 실제로 무슨 행위를 적었는지는 행위 유형별로 따로 모아 두었습니다.

→ 개인정보위 제재 위반행위 — 결정문 「위법성 판단」 절 전수 (과징금 부과 건 기준)

부과된 처분을 법원에서 다투면 어떻게 되는지도 판결문 단위로 볼 수 있습니다. 2021년 이후 처분에 대한 1심·2심은 전부 위원회가 이겼지만, 기각 판결 안에도 해설서의 규범력이나 면제 사유에 관해 위원회와 다른 판단이 들어 있고, 그 판시들은 소송보다 조사·의견진술 단계에서 먼저 쓰입니다.

→ 개인정보위 과징금 취소소송, 법원은 어디서 위원회와 갈렸나 — 판결 18건 전수 검토

개인정보 보호책임자를 다시 봐야 하나

자격요건은 새로 생기는 것이 아닙니다. 경력 요건과 지정 대상 범위는 시행령 제32조와 별표 1로 2024년 3월부터 이미 시행 중입니다. 9월 11일에 바뀐 것은 **제재**입니다. 그동안 제31조 위반에는 과태료가 없었는데, 개정법이 미지정·자격미달 지정·이사회 의결 누락·신고 누락을 각각 과태료 대상으로 삼았습니다. 세 호 모두 제26조 제8항에 따라 **수탁자에게 준용**되므로, 업무를 위탁받아 처리하는 회사도 자기 이름으로 같은 의무를 집니다.

이사회 의결·신고의 대상과 절차는 개정 시행령(대통령령 제36671호) 제32조 제3항·제4항이 정합니다. 대상은 연간 매출액등 1,800억 원 초과에 민감정보·고유식별정보 5만 명 또는 개인정보 100만 명 요건이 붙는 사업자, 재학생 2만 명 이상 대학, 상급종합병원, 공공시스템운영기관이고, 신고는 사유 발생일부터 6개월 이내(이사회 소집 곤란 등 사유가 있으면 1년 범위 연장)입니다. 시행 전에 이미 지정한 보호책임자도 시행일부터 6개월 안에 신고해야 합니다(부칙 제2조). 신고서 서식은 시행일에 함께 시행된 「개인정보 보호책임자 지정 및 경력 인정에 관한 고시」(개인정보보호위원회고시 제2026-11호) 제2조와 별지 서식으로 정해졌고, 개인정보위가 9월 10일 공지한 FAQ는 신고를 개인정보 포털(www.privacy.go.kr)의 「CPO 신고」 메뉴로 받는다고 안내합니다.

→ 본사 APAC DPO를 한국 CPO로 올려 두었습니다 — 9월 11일 이후 그대로 둬도 되나

개인정보 보호책임자를 정보보호 최고책임자(CISO)가 겸하고 있는 회사라면 확인할 조문이 하나 더 있습니다. CISO 겸직 제한을 받는 회사에서도 정보통신망법 제45조의3 제4항 제2호 라목이 CPO 업무를 겸직 가능 업무로 열어 두고 있는데, 그 라목이 인용하는 개인정보 보호법 조문을 개정법 부칙 제4조 제2항이 제31조 제2항에서 **제31조 제4항**으로 바꿨습니다. 시행일은 개정법 본체와 같은 9월 11일이었습니다. 겸직 자체는 그대로 가능하지만, 겸직 구조의 근거 조문이 같은 날 함께 움직인 셈입니다.

→ CISO가 CPO를 겸할 수 있나요? 9월 11일부터 근거 조문이 바뀌었습니다

법원도 같은 정비를 마쳤습니다. 대법원은 2026년 7월 29일 대법원규칙 제3272호로 「법원 개인정보 보호에 관한 규칙」을 개정해, 사법부 개인정보 보호책임자의 업무를 정한 제6조 제2항 제3호의 인용을 「법 제31조제3항」에서 **법 제31조 제4항**으로 바꿨고, 시행일 역시 개정법과 같은 2026년 9월 11일로 맞췄습니다. 법원행정처는 개정이유에서, 보호책임자의 수행 업무에 전문인력·예산 확보와 대표자·이사회 보고를 추가한 개인정보 보호법 개정(법률 제21445호)을 반영해 인용 조문을 정비한 것이라고 밝혔습니다. 사고대응 절차서·위·수탁 계약서·개인정보 처리방침에 「법 제31조 제3항」식 인용이 남아 있다면, 법원이 규칙까지 고쳐 따라간 이 항 이동에 맞춰 사내 문서에도 같은 정비가 필요합니다.

위탁사와 수탁사가 같은 사고를 두고 각자 다른 처분을 받는 구조도 이 준용에서 나옵니다. 수탁사에서 유출이 나면 위탁사는 제26조 제4항의 관리·감독으로 걸리고 수탁사는 자기 이름의 안전조치 의무로 걸리는데, 개인정보위가 두 자리를 실제로 어떻게 갈랐는지는 결정문에 남아 있습니다.

→ 수탁사 직원의 실수로 개인정보가 유출됐다 — 위탁사는 어디까지 책임지나

외국계 한국법인이 추가로 볼 것

본사 산출물을 번역해 쓰는 구조에서는 개정 내용보다 **누가 결정하고 무엇을 밖에 알리는지**가 먼저 걸립니다. 이사회 의결이 들어오는 것이 대표적입니다.

→ 본사 프라이버시 정책을 한국 법인에 그대로 옮겼습니다 — 9월 11일 전에 다시 봐야 할 아홉 지점

본사가 참조하는 영문 법률이 몇 년판인지도 함께 확인할 필요가 있습니다. 구판을 기준으로 삼으면 과잉 준수와 미준수가 동시에 생깁니다.

→ 영문 개인정보 보호법에 세 버전이 공존합니다 — 본사가 읽는 판이 현행(법률 제20897호)인지 확인하는 법

국내대리인 구조는 이번 개정이 아니라 **이미 지난 기한**의 문제입니다. 재지정 경과기간은 2026년 4월 2일에 끝났고, 9월 11일부터 대리 업무의 범위가 넓어졌습니다.

→ 한국에 자회사가 있는데 국내대리인은 로펌입니다 — 재지정 기한은 2026년 4월에 이미 지났습니다

8월 20일 본인전송요구권은 별개 일정이었습니다

이쪽은 2026년 8월 20일에 이미 시행됐습니다. 다만 **보내는 쪽과 받는 쪽에 걸리는 날짜가 다릅니다.** 정보를 보내야 하는 기업 상당수는 2027년부터이고, 받아가는 쪽에는 8월 20일부터 의무가 붙습니다.

→ 본인전송요구권 8월 20일 시행 — 우리 회사에 실제로 걸리는 날은 언제인가

요구가 실제로 들어왔을 때의 기한과 거절 사유는 따로 정리했습니다.

→ 본인전송요구가 들어왔습니다: 며칠 안에 보내야 하고, 거절할 수 있나

데이터를 받는 사업을 준비 중이라면 전문기관 지정 대상인지부터 갈라야 합니다. 기준은 규모가 아니라 목적입니다.

→ 마이데이터 사업을 하려면 전문기관 지정을 받아야 하나요

시행령이 답한 것 — 대통령령 제36671호

법률과 시행령이 같은 날 시행됐습니다. 하루 전인 2026년 9월 10일 개정 시행령이 대통령령 제36671호로 공포됐고, 부칙 제1조가 시행일을 법률과 같은 9월 11일로 정했습니다. 아래는 공포된 조문 문언입니다.

다음 세 가지는 모두 대통령령에 위임되어 있었습니다. 이를 담은 시행령 일부개정령은 2026년 6월 2일부터 7월 13일까지 입법예고(공고 제2026-59호)를 거쳐 8월 31일 법제처 심사를 마쳤고, 9월 10일 공포됐습니다. 입법예고안에서 바뀐 대목이 있으므로(뒤에서 보듯 신고 기한이 1개월에서 6개월로 늘었습니다), 입법예고 단계의 자료로 사내 기준을 잡아 두었다면 공포문으로 다시 맞춰야 합니다.

- 제34조 제2항의 **유출등의 가능성** 범위와 그때 알려야 할 사항
- 제64조의2 제6항의 **감경 사유**
- 제31조 제3항의 **이사회 의결·신고 대상 기준**과 신고 방법·절차

이사회 의결·신고 대상과 신고 기한

시행령에서 대상 목록은 하나입니다. 이사회 의결·신고 의무의 대상(제32조 제3항)은 별표 1의 전문 자격을 갖춘 보호책임자를 지정해야 하는 대상과 같은 목록이고, 민간 기업의 금액 기준은 현행 「연간 매출액등 1,500억 원 이상」에서 **1,800억 원 초과로** 오릅니다. 여기에 민감정보·고유식별정보 5만 명 이상 또는 개인정보 100만 명 이상 요건이 함께 걸립니다. 재학생 2만 명 이상 대학, 상급종합병원, 공공시스템운영기관도 대상입니다.

신고 기한은 입법예고안과 공포본이 다릅니다. 입법예고안은 신고 의무 발생일부터 1개월이었으나, 시행령 제32조 제4항은 **사유가 발생한 날부터 6개월 이내**로 늘렸고, 경영상 이유로 이사회 소집이 어려운 경우 등 부득이한 사유가 있으면 보호위원회가 **1년 범위에서 연장**할 수 있게 했습니다. 신고서 서식은 보호위원회 고시로 정하는데, 시행일에 기존 「개인정보 보호책임자 경력 인정에 관한 고시」의 제명을 「개인정보 보호책임자 지정 및 경력 인정에 관한 고시」로 바꾸고 제2조(지정 신고 등)와 별지 서식을 신설하는 방식으로 정해졌습니다(개인정보보호위원회고시 제2026-11호). 신고서를 받은 위원회는 법인등기사항증명서나 사업자등록증을 행정정보 공동이용으로 확인하고, 신고인이 그 확인에 동의하지 않으면 사본을 내야 합니다.

시행 전에 이미 지정해 둔 보호책임자도 신고 대상입니다. 부칙 제2조는 시행 당시 대상 기준에 해당하는 개인정보처리자가 시행 전에 지정한 보호책임자를 **시행일부터 6개월 이내**, 즉 2027년 3월 11일까지 신고하도록 정했습니다. 법률 부칙이 비워 두었던 「기존 지정분」 문제에 시행령이 답한 것입니다. 부칙이 요구하는 것은 신고이고, 기존 지정에 대한 이사회 의결을 다시 거치라는 문언은 없습니다. 개인정보위가 2026년 9월 10일 공지한 「개인정보 보호책임자 지정 신고 관련 주요 FAQ」도 이미 지정해 운영 중인 경우 이사회 의결을 추가로 거칠 필요는 없고 신고 의무만 이행하면 된다고 답했습니다.

유출 가능성 통지의 요건과 시계

시행령 제39조의2는 통지 사유를 두 가지로 정합니다. ① 개인정보처리시스템이나 개인정보취급자의 정보기기에 불법적인 접근이 있어 유출등이 의심되지만 **어느 정보주체의 개인정보인지 특정하기 곤란한 경우**에는 그 불법적 접근을 알게 된 때, ② 일부 개인정보가 제3자에 의해 거래되는 등 유출등이 확인됐고 **다른 정보주체의 개인정보도 유출됐을 수 있다고 인정되는 경우**에는 그 사실을 알게 된 때입니다. 통지 사항은 가능성이 있는 개인정보 항목, 의심되는 시점과 경위, 피해 최소화 방법·대응조치·담당 부서, 그리고 유출 여부가 확정되면 추가 통지하겠다는 사실입니다.

기한은 제39조의3에 따라 위 시점부터 **72시간 이내**입니다. 기한 안에 실제 유출이 확인되면 제34조 제1항의 유출 통지로 갈음하고, 반대로 **실제로 유출되지 않았음이 확인되면 그 사실도 즉시 통지**해야 합니다. 연락처를 알 수 없는 등 정당한 사유가 있으면 홈페이지에 30일 이상 게시하는 것으로 갈음할 수 있습니다. 8월 21일 공개된 「개인정보 유출등 대응 매뉴얼」 초안이 든 두 상황과 같은 구조입니다.

투자 감경은 산정 절차의 어디에 놓입니까

과징금 감경 사유는 원래 별도 공고 제2026-55호로 2026년 6월 1일 입법예고됐으나, 법제처 심사 과정에서 공고 제2026-59호 개정령안에 **통합**됐습니다. 아래 수치는 공포된 제60조의2 제5항과 별표 1의5의 문언입니다.

별표 1의5는 과징금을 기준금액 산정, 투자감경, 1차 조정, 2차 조정, 부과과징금 결정의 순서로 산정합니다. **투자감경은 1차 조정보다 앞에 놓인 독립 단계입니다.** 실무자에게는 상한 숫자보다 이 위치가 더 중요합니다. 감경 사유는 개인정보 보호를 위하여 예산·인력·설비·장치 등을 투자하고 운영하는 경우로서 ① 투자한 규모·비율과 지속성, ② 법 제30조의3에 따른 사업주·대표자의 책임 이행 정도, ③ 보호책임자의 역할·조직·인력 구성 등 보호 체계의 운영 내용과 수준, ④ 그 밖의 안전성 확보 조치 노력을 고려해 보호위원회가 고시하는 기준을 충족하는 경우입니다(제60조의2 제5항). 감경 폭은 기준금액의 **100분의 40 범위**이고, 고의·중과실 위반은 법 제64조의2 제6항 단서에 따라 제외됩니다.

매출액 기준 부과기준율은 다음과 같습니다.

위반행위의 중대성	부과기준율
매우 중대한 위반행위	2.1% 이상 2.7% 이하
중대한 위반행위	1.5% 이상 2.1% 미만
보통 위반행위	0.9% 이상 1.5% 미만
약한 위반행위	0.03% 이상 0.9% 미만

법 제64조의2 제2항의 가중 대상이면 부과기준율에 가중비율을 곱하되, 그 곱한 비율은 **8.91**%를 넘을 수 없습니다. 매출액을 산정하기 어려워 정액으로 기준금액을 정하는 경우(제60조의2 제2항 각 호)에는 중대성에 따라 5백만 원 이상 18억 원 이하이고, 가중금액을 더해도 **45억 원**을 넘을 수 없습니다. 가중비율과 가중금액은 고의·중과실의 내용, 위반 반복 정도, 시정조치 명령 불이행, 피해 정보주체 1천만 명 이상 여부를 고려해 보호위원회 고시가 정하도록 했고, 9월 11일 개정 고시는 이를 새로 만든 별표 2 「위반행위의 가중 판단기준」에 맡겼습니다(제8조의2).

감경이 막히는 자리도 있습니다. 매우 중대한 위반행위에 대해 1차·2차 조정의 감경 전부 또는 일부를 적용하지 않을 수 있다는 규정은 2026년 5월 19일부터 이미 시행 중이고, 개정 시행령에서는 투자감경이 앞에 들어오면서 마목이 됩니다. 과징금 면제 사유(제60조의2 제6항)는 현행 문언이 그대로 유지됩니다. 입법예고안(공고 제2026-55호)에 있던 중소기업·소상공인의 기술 지원 시정 문구는 공포본에 없습니다. 이 문구는 시행령 대신 과징금 부과기준 고시로 옮겨 갔습니다. 고시 제4조 제2항 제2호는 피해가 없거나 경미한 경우로서 위반을 시정하고 유출등의 통지·신고를 위반하지 않았으면 과징금을 부과하지 않을 수 있다고 정하는데, 9월 11일 개정 고시는 이 「시정」에 중소기업·소상공인 등이 법 제34조 제4항에 따라 기술을 지원받아 시정하는 경우를 포함시켰습니다.

입법예고안에서 빠진 것이 하나 더 있습니다. 공고 제2026-55호 부칙 제2조는 투자감경을 시행일 **이후에 발생한 위반행위**부터 적용한다는 적용례를 두었는데, 공포된 부칙에는 그 적용례가 없습니다. 부칙은 시행일(제1조), 보호책임자 신고 특례(제2조), 신용정보법 시행령 정비(제3조) 셋뿐입니다. 문언만 놓고 보면 시행일 이후 부과하는 과징금이면 위반행위 시점과 무관하게 투자감경이 적용된다고 읽힐 여지가 있지만, 명문이 없으므로 확정된 해석은 아닙니다. 게다가 9월 11일 개정된 과징금 부과기준 고시는 부칙 제2조에서 **고시 시행 전에 종료된 행위에는 종전 규정을 적용**한다고 정했습니다. 9월 10일까지 끝난 위반에 투자감경을 어떤 기준으로 볼지는 시행령과 고시의 문언만으로는 정해지지 않습니다.

매출액 산정, 중대성 판단, 투자감경, 1차·2차 조정, 감경 제한, 부과과징금 결정의 세부 기준은 별표 1의5 제3호가 **전부 보호위원회 고시에 다시 위임**했습니다. 그 고시가 시행일에 맞춰 개정됐습니다.

과징금 부과기준 고시가 정한 것 — 제2026-12호

개인정보위는 2026년 7월 16일 「개인정보 보호법 위반에 대한 과징금 부과기준」 일부개정안을 행정예고(공고 제2026-90호, 의견제출 8월 5일까지)했고, 시행일인 9월 11일 개인정보보호위원회고시 제2026-12호로 확정해 같은 날 시행했습니다. 산정 순서는 기준금액, **투자감경**, 1차 조정, 2차 조정, 부과과징금 결정이 되고, 1차 조정의 가중·감경은 기준금액이 아니라 「투자감경을 거친 금액」을 바탕으로 계산합니다.

무엇이	개정 고시(2026. 9. 11. 시행)	종전
투자감경(제8조의3)	① 예산·인력·설비·장치 투자의 규모·비율·지속성·증가 정도 ② 대표자의 제30조의3 책임 이행과 보호책임자의 지정·권한·업무수행 수준 등 보호 체계 ③ 법정 의무를 넘는 보호기술·안전조치를 종합해 **기준금액의 40% 이하** 감경. 위반행위가 있었던 사업연도의 **직전 3개 사업연도** 조치를 본다. 고의·중과실은 제외	없음
10% 구간 기준금액(제6조·제8조의2)	관련 매출액 × 부과기준율 × 가중비율. 가중비율과 가중금액은 별표 2 「위반행위의 가중 판단기준」으로 정한다	없음
반복 위반 가중(제9조 제1항 제2호)	최근 3년 같은 호 과징금 1회 **20%** · 2회 **40%** · 3회 이상 **80%**	1회 15% · 2회 이상 30%
신고·통지 기한 도과 + 피해 확산 방지 조치 불이행(제10조 제1항 제2호)	1차 조정 금액의 30% 이하 **가산 신설**	없음
인증·자율 보호 활동 감경(제10조 제2항 제3호)	인증 **30%** · 자율규제 규약 이행 **20%** · 처리방침 평가 등 **15%** 이하	50% · 40% · 30% 이하
사고 대응 체계(제10조 제2항 제5호)	대응 체계를 갖추고 조기 탐지·신속한 신고·통지·확산 방지로 회복한 경우 1차 조정 금액의 40% 이하 **감경 신설**	「그 밖의 사유」 10% 이하 감경(삭제)
업무 형태·규모 감경(제9조 제2항 제2호)	국가기관·지방자치단체 등과 공공시스템운영기관은 대상에서 제외	공공기관·비영리법인·중소기업자 등
부과과징금 결정(제11조 제1항 제3호)	위반에 비해 현저히 과중하면 2차 조정 금액의 50% 이하 추가 감경 신설, 사유는 의결서에 명시	부담능력·시장 여건 사유만

중대성 판단기준(별표 1)의 개인정보 유형에는 인증정보와 같은 칸에 **연계정보**(서비스 연계를 위해 주민등록번호를 비가역적으로 암호화한 정보)가 들어갔습니다.

부칙 제2조가 중요합니다. **이 고시 시행 전에 종료된 행위에 대한 과징금은 종전 규정에 따릅니다.** 9월 10일까지 끝난 위반이면 옛 감경률(인증 50% 등)로, 9월 11일 이후에도 이어진 위반이면 새 기준으로 산정됩니다. 인증에 기대던 회사라면 감경 폭이 줄었습니다. 반대로 유출 대응 체계를 갖추고 신속하게 신고·통지한 것은 감경 사유로 새로 들어왔고, 기한을 넘기면서 확산 방지 조치까지 하지 않으면 가산됩니다.

과징금이 10% 구간으로 올라가면 공표명령도 가까워집니다. 개인정보위는 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」을 9월 4일 개정해 9월 11일부터 시행했습니다. 공표명령 요건 가운데 과징금 사건에서 중대성이 「매우 중대한 위반행위」인 경우를 정한 제6조 제1항 제3호가 종전에는 법 제64조의2 제1항만 적었는데, 이제 같은 조 제2항에 따라 과징금을 부과받은 경우도 적습니다. 공표명령의 요건과 면제 사례는 따로 정리했습니다.

→ 과태료가 더 많은 쪽은 공표되지 않았습니다 — 개인정보위 결과 공표는 무엇으로 결정되는가

과태료 금액도 오릅니다

개정 시행령은 별표 2의 과태료 금액을 전 구간에서 올렸습니다. 제안이유는 안전조치 의무 위반 과태료를 1차 600만 원·2차 1,200만 원·3차 이상 2,400만 원에서 **900만 원·1,800만 원·3,000만 원**으로 올린다고 적었지만, 별표 2의 개별기준을 보면 48개 항목 전부가 같은 비율로 움직입니다. 법정 상한 5천만 원 구간은 1,500만·3,000만·5,000만 원, 2천만 원 구간은 600만·1,200만·2,000만 원, 1천만 원 구간은 300만·600만·1,000만 원입니다. 개정법이 신설한 보호책임자 미지정·자격미달·이사회 의결 누락·미신고(제75조 제2항 제14호의2부터 제14호의4까지)와 유출 가능성 통지 미이행(같은 항 제17호)도 각각 900만·1,800만·3,000만 원으로 별표에 들어갔습니다.

별표 2의 금액을 실제 부과금액으로 바꾸는 기준도 같은 날 고시가 됐습니다. 위원회 지침이던 과태료 부과기준이 「개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보보호위원회고시 제2026-14호)으로 제정돼 9월 11일 시행됐습니다. 최근 3년간 같은 위반으로 받은 처분 횟수에 해당하는 별표 2 금액을 기준금액으로 삼고, 감경기준(고시 별표 2)과 가중기준(고시 별표 3)에 따라 조정하며, 고지서를 받은 날부터 14일 안에 자진납부하면 부과금액의 20%를 감경합니다. 시행 전에 종료된 위반행위에도 적용되지만 그 경우 감경비율은 종전 부과기준(2023. 9. 11.)을 따릅니다(부칙 제2조·제3조). 행정예고안(공고 제2026-92호)에 있던, 과태료 없이 시정조치·경고만 받은 경우도 처분 횟수에 넣는 괄호 문언은 확정 고시에서 빠졌습니다.

투자 감경의 실무 안내서도 초안이 나왔습니다

개인정보위가 2026년 8월 21일 「과징금 투자 감경제도 안내서」 초안(2026. 9.판, 25면)을 공개해 9월 3일까지 의견을 받았습니다. 초안이 별표 문언에 더해 준 실무 정보는 세 가지입니다.

첫째, 감경 판단의 시간 범위입니다. 위원회는 위반행위가 있었던 사업연도의 **직전 3개 사업연도** 안에서 조치한 사항을 고려하고, 상당하다고 인정하면 위반행위가 있었던 사업연도의 조치도 볼 수 있습니다(사업을 개시한 지 1년이 안 된 기업 등). 감경을 받으려면 사고가 난 해의 긴급 투자가 아니라 그 전 3년의 투자 이력이 필요하다는 뜻입니다.

둘째, 투자액 산출 방법입니다. 개인정보보호 투자액은 정보보호산업법 제13조의 정보보호 공시 기준을 준용해 유·무형자산 감가상각비, 비용, 내부인력 인건비 세 항목의 합으로 산출합니다. 정보보호 공시를 이미 수행하는 기업은 공시 자료를 그대로 소명에 쓸 수 있습니다. 증빙서류는 감사보고서·합계잔액시산표·자산대장·비용원장·인건비 내역·기안서 수준까지 예시되어 있습니다. 감경을 염두에 둔다면 개인정보보호 예산을 지금부터 별도 계정과목으로 관리해 두는 편이 소명에 유리합니다.

셋째, 고시안의 문언입니다. 초안에 실린 고시안 제8조의3은 세 요건을 종합 고려해 기준금액의 **100분의 40 이하** 금액을 감경하도록 정했고, 개인정보처리자의 고의 또는 중대한 과실로 위반한 경우는 제외합니다. 이 고시안의 골격(세 요건 종합 고려, 40% 이하, 고의·중과실 제외)은 9월 11일 확정된 고시 제8조의3에 그대로 들어갔고, 첫째로 본 직전 3개 사업연도 기준도 고시 본문(제8조의3 제2항)이 됐습니다. 둘째로 본 투자액 산출 방법과 증빙 예시는 안내서에만 있고, 안내서 확정본은 9월 11일 현재 공개되지 않았습니다.

한 가지는 구분해 두는 편이 좋습니다.

개인정보보호위원회 제2소위원회가 2026년 8월 12일 원안 동의로 의결한 침해요인 평가(의결 제2026-215-321호)의 대상은 제3자 전송요구의 대상 분야를 고용·교육으로 확대하는 마이데이터 관련 **다른 개정안**(공고 제2026-77호)이었습니다. 9월 11일 시행에 대비한 것은 공고 제2026-59호 개정령이고, 이쪽이 9월 10일 대통령령 제36671호로 공포된 것입니다.

시행령이 위임한 고시 둘은 시행일에 함께 나왔습니다. 보호책임자 지정·변경·해제 신고서 서식(시행령 제32조 제4항)은 개인정보보호위원회고시 제2026-11호, 과징금 투자감경의 세부 기준(제60조의2 제5항, 별표 1의5 제3호)은 제2026-12호입니다. 그래서 대상 여부 판정, 조문 번호 정비, 진행 중인 위반 상태 정리, 보호책임자 지정 구조 점검과 이사회 안건 일정에 더해 신고서 작성과 투자감경 소명 준비도 이제 확정된 문언으로 할 수 있습니다. 남은 것은 투자 감경제도 안내서와 유출등 대응 매뉴얼의 확정본입니다.

자주 묻는 질문

Q. 2026년 9월 11일에 무엇이 시행되나요?

2026년 9월 11일 개정 개인정보 보호법(법률 제21445호) 본체가 시행됐습니다. 바뀐 것은 다섯입니다. ① 통지·신고 대상인 유출등의 정의에 위조·변조·훼손이 추가됐습니다(제23조 제2항). ② 유출등의 가능성 통지가 신설되면서(제34조 제2항) 유출 신고의 근거 조문이 제34조 제3항에서 제4항으로 이동했습니다. ③ 재위반·대규모 피해·시정조치 불이행 세 경우의 과징금 상한이 전체 매출액의 3%에서 10%로 올랐습니다(제64조의2 제2항). ④ 개인정보 보호책임자 지정에 이사회 의결·신고 의무와 과태료가 붙었습니다(제31조 제3항, 제75조 제2항 제14호의2부터 제14호의4까지). ⑤ 개인정보 보호의 최종 책임자가 사업주·대표자임이 명시됐습니다(제30조의3). 다만 제32조의2 제1항 단서와 제75조 제2항 제15호는 2027년 7월 1일에 시행됩니다.

Q. 2026년 9월 11일에 시행된 것은 법률인가요, 시행령인가요?

둘 다입니다. 법률 제21445호가 2026년 3월 10일 공포되어 2026년 9월 11일 시행됐고, 이를 구체화할 개인정보 보호법 시행령 일부개정령도 2026년 9월 10일 대통령령 제36671호로 공포되어 같은 날 함께 시행됐습니다. 시행령은 2026년 6월 2일부터 7월 13일까지 입법예고(개인정보보호위원회 공고 제2026-59호)를 거쳐 8월 31일 법제처 심사를 마친 안이고, 부칙 제1조가 시행일을 법률과 같은 9월 11일로 정했습니다. 과징금 감경 사유는 원래 별도 공고 제2026-55호로 입법예고됐으나 법제처 심사 과정에서 이 개정령에 통합됐습니다. 개인정보위 제2소위원회가 2026년 8월 12일 침해요인 평가에서 원안 동의로 의결한 개정안은 마이데이터 관련 별건(공고 제2026-77호)입니다. 시행령이 다시 위임한 고시 둘도 같은 날 시행됐습니다. 보호책임자 신고서 서식은 개인정보보호위원회고시 제2026-11호, 과징금 투자감경과 가중 판단의 세부 기준은 과징금 부과기준 개정 고시(제2026-12호)에 들어갔습니다.

Q. 사내 문서에서 가장 먼저 고쳐야 할 곳은 어디인가요?

유출 신고의 근거 조문을 적어 둔 곳입니다. 2026년 9월 10일까지 보호위원회 신고는 제34조 제3항이었지만, 개정법이 제2항에 유출등의 가능성 통지를 신설하면서 뒤 항이 한 칸씩 밀려 신고는 제34조 제4항이 됐습니다. 사고대응 절차서, 위·수탁 계약서, 개인정보 처리방침에 '법 제34조 제3항에 따른 신고'라고 적혀 있다면 그 인용은 지금 다른 조항을 가리킵니다.

Q. 과징금 상한 10%는 모든 위반에 적용되나요?

아닙니다. 상한이 올라가는 것은 신설된 제64조의2 제2항이 정한 세 경우뿐이고 원칙 조항은 그대로 남습니다. 세 경우는 재위반, 고의·중과실에 의한 대규모 피해, 시정조치 불이행이며 각각의 요건과 기간은 신구조문 대조표에 조문 그대로 실어 두었습니다.

Q. 시행 전에 준비를 못 했습니다. 지금 무엇부터 해야 하나요?

먼저 문서의 조문 인용부터 고칩니다. 사고대응 절차서·위·수탁 계약서·개인정보 처리방침에 「법 제34조 제3항에 따른 신고」나 「법 제31조 제3항」이 남아 있으면 지금은 다른 조항을 가리킵니다. 다음이 서식입니다. 유출 통지문에는 제34조 제1항 제6호가 신설한 손해배상·법정손해배상·분쟁조정 등 법적 권리와 그 행사 방법이 들어가야 하고, 사고대응 절차서에는 유출이 확인되지 않아도 가능성을 알게 된 때부터 72시간 안에 통지하는 분기가 필요합니다. 의사결정이 필요한 것은 셋입니다. 이사회 의결·신고 대상이라면 시행 전에 지정한 보호책임자도 시행일부터 6개월 안에 신고해야 하고, 시행일에 종료되지 않았던 위반 상태는 부칙 제3조 제2항에 따라 새 가중 규정의 사정권에 들어가며, 과징금 투자 감경을 소명하려면 위반이 있었던 사업연도의 직전 3개 사업연도 투자 이력이 필요합니다.

관련 가이드

- 개인정보 유출 사고 대응 — 인지부터 처분·구상까지
- 위탁·수탁 개인정보 책임 지도 — 우리는 어느 자리에 있나
- AI 서비스 규제 지도 — AI기본법과 개인정보 보호법이 각각 어디에서 걸리나
- IT·개인정보 법령 시행일 캘린더

이 글은 일반적인 정보 제공을 목적으로 하며, 구체적인 사안에 대한 법률자문이 아닙니다. 개별 사안은 사실관계에 따라 결론이 달라질 수 있으므로 별도의 검토가 필요합니다.

참고 자료

- 개정 개인정보 보호법(법률 제21445호, 2026. 3. 10. 공포, 2026. 9. 11. 시행) — 국가법령정보센터 시행예정 법령
- 개인정보 보호법(현행) · 개인정보 보호법 시행령(현행) — 국가법령정보센터
- 개인정보 보호법 시행령 일부개정령안 입법예고(개인정보보호위원회 공고 제2026-59호, 2026. 6. 2. \~ 7. 13.) — 법제처 입법예고. 첨부된 법령안 전문을 확인했습니다
- 개인정보 보호법 시행령(대통령령 제36671호, 2026. 9. 10. 공포, 2026. 9. 11. 시행) — 제32조 제3항·제4항, 제39조의2, 제39조의3, 제60조의2 제5항, 별표 1의5, 별표 2, 부칙 제1조·제2조·제3조를 공포문으로 대조했습니다. 부칙에 투자감경의 적용례는 없습니다
- 개인정보 보호법 시행령 일부개정령안 — 정부입법현황(법제처 심사완료 2026. 8. 31.) — 국민참여입법센터. 공포 전 단계의 의안(제안이유·개정령안·별표 1의5·별표 2·신구조문대비표)입니다. 공고 제2026-55호 안의 과징금 감경 규정이 이 단계에서 통합됐습니다
- 개인정보보호위원회 제2소위원회 의결 제2026-215-321호(2026. 8. 12.) 「개인정보 보호법 시행령」 일부개정안에 대한 개인정보 침해요인 평가에 관한 건 — 개인정보위 위원회 결정문. 주문은 개인정보보호위원회공고 제2026-77호 개정안에 대한 원안 동의입니다
- 개인정보 보호법 시행령 일부개정령안 입법예고(개인정보보호위원회 공고 제2026-55호, 2026. 6. 1. \~ 7. 13.) — 법제처 입법예고. 법 제64조의2 제2항의 기준금액 산정, 같은 조 제6항의 투자 감경, 같은 조 제7항 제4호의 과징금 면제에 관한 개정안이며, 첨부된 법령안 전문과 별표 1의5안을 확인했습니다. 법제처 심사 과정에서 공고 제2026-59호 개정령안에 통합됐습니다
- 개인정보보호위원회 공고 제2026-77호(2026. 6. 30. 관보 게재) 「개인정보 보호법 시행령」 일부개정령안 입법예고 — 제3자 전송요구 대상 분야를 고용·교육으로 확대하는 등 마이데이터 관련 개정안입니다. 위 의결의 대상이며, 공고 제2026-59호 개정안과는 별건입니다
- 법원 개인정보 보호에 관한 규칙 일부개정규칙(대법원규칙 제3272호, 2026. 7. 29. 공포, 2026. 9. 11. 시행) — 국가법령정보센터. 개정문·부칙·개정이유 전문을 확인했습니다. 제6조 제2항 제3호의 「법 제31조제3항」이 「법 제31조제4항」으로 바뀝니다
- 「개인정보 유출등 대응 매뉴얼」 초안 공개 및 의견수렴(개인정보위 공지, 2026. 8. 21.) — 첨부된 초안 전문(74면)을 확인했습니다. 의견제출은 2026. 9. 3. 마감됐습니다
- 「과징금 투자 감경제도 안내서」 초안 공개 및 의견수렴(개인정보위 공지, 2026. 8. 21.) — 첨부된 초안 전문(25면)과 고시안 제8조의3 문언을 확인했습니다. 의견제출은 2026. 9. 3. 마감됐습니다
- 개인정보보호위원회고시 제2026-12호 「개인정보 보호법 위반에 대한 과징금 부과기준」 일부개정(2026. 9. 11. 고시·시행) — 전자관보 게재본으로 개정문·부칙을 대조했습니다. 개정문이 신설한다고 적은 별표 2(위반행위의 가중 판단기준)는 관보 게재본에서 확인되지 않아 그 내용을 옮기지 않았습니다. 현행 조문과의 비교는 국가법령정보센터의 2026. 5. 19. 개정본을 기준으로 했습니다
- 「개인정보 보호법 위반에 대한 과징금 부과기준」 일부개정안 행정예고(개인정보보호위원회 공고 제2026-90호, 2026. 7. 16.) — 공고문·개정문·조문별 제개정 이유서를 확인했습니다. 의견제출은 2026. 8. 5. 마감됐습니다
- 개인정보보호위원회고시 제2026-14호 「개인정보 보호법 위반에 대한 과태료 부과기준」 제정(2026. 9. 11. 고시·시행) — 전자관보 게재본. 행정예고안(공고 제2026-92호, 2026. 7. 16.)과 조문을 대조했습니다
- 개인정보보호위원회고시 제2026-11호 「개인정보 보호책임자 지정 및 경력 인정에 관한 고시」 일부개정(2026. 9. 11. 고시·시행) — 전자관보 게재본. 제명 변경과 제2조(개인정보 보호책임자 지정 신고 등) 신설을 확인했습니다
- 개인정보 보호책임자 지정 신고 관련 주요 FAQ(개인정보위 공지, 2026. 9. 10.) — 첨부 PDF(27문항)를 확인했습니다

- 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」(2026. 9. 4. 개정, 2026. 9. 11. 시행) — 개인정보위 훈령·예규·고시 게시판 첨부본. 직전 판(2025. 7. 1. 시행)과 대조했습니다

자주 묻는 질문

Q. 2026년 9월 11일에 무엇이 시행되나요?

2026년 9월 11일 개정 개인정보 보호법(법률 제21445호) 본체가 시행됐습니다. 바뀐 것은 다섯입니다. ① 통지·신고 대상인 유출등의 정의에 위조·변조·훼손이 추가됐습니다(제23조 제2항). ② 유출등의 가능성 통지가 신설되면서(제34조 제2항) 유출 신고의 근거 조문이 제34조 제3항에서 제4항으로 이동했습니다. ③ 재위반·대규모 피해·시정조치 불이행 세 경우의 과징금 상한이 전체 매출액의 3%에서 10%로 올랐습니다(제64조의2 제2항). ④ 개인정보 보호책임자 지정에 이사회 의결·신고 의무와 과태료가 붙었습니다(제31조 제3항, 제75조 제2항 제14호의2부터 제14호의4까지). ⑤ 개인정보 보호의 최종 책임자가 사업주·대표자임이 명시됐습니다(제30조의3). 다만 제32조의2 제1항 단서와 제75조 제2항 제15호는 2027년 7월 1일에 시행됩니다.

Q. 2026년 9월 11일에 시행된 것은 법률인가요, 시행령인가요?

둘 다입니다. 법률 제21445호가 2026년 3월 10일 공포되어 2026년 9월 11일 시행됐고, 이를 구체화할 개인정보 보호법 시행령 일부개정령도 2026년 9월 10일 대통령령 제36671호로 공포되어 같은 날 함께 시행됐습니다. 시행령은 2026년 6월 2일부터 7월 13일까지 입법예고(개인정보보호위원회 공고 제2026-59호)를 거쳐 8월 31일 법제처 심사를 마친 안이고, 부칙 제1조가 시행일을 법률과 같은 9월 11일로 정했습니다. 과징금 감경 사유는 원래 별도 공고 제2026-55호로 입법예고됐으나 법제처 심사 과정에서 이 개정령에 통합됐습니다. 개인정보위 제2소위원회가 2026년 8월 12일 침해요인 평가에서 원안 동의로 의결한 개정안은 마이데이터 관련 별건(공고 제2026-77호)입니다. 시행령이 다시 위임한 고시 둘도 같은 날 시행됐습니다. 보호책임자 신고서 서식은 개인정보보호위원회고시 제2026-11호, 과징금 투자감경과 가중 판단의 세부 기준은 과징금 부과기준 개정 고시(제2026-12호)에 들어갔습니다.

Q. 사내 문서에서 가장 먼저 고쳐야 할 곳은 어디인가요?

유출 신고의 근거 조문을 적어 둔 곳입니다. 2026년 9월 10일까지 보호위원회 신고는 제34조 제3항이었지만, 개정법이 제2항에 유출등의 가능성 통지를 신설하면서 뒤 항이 한 칸씩 밀려 신고는 제34조 제4항이 됐습니다. 사고대응 절차서, 위·수탁 계약서, 개인정보 처리방침에 '법 제34조 제3항에 따른 신고'라고 적혀 있다면 그 인용은 지금 다른 조항을 가리킵니다.

Q. 과징금 상한 10%는 모든 위반에 적용되나요?

아닙니다. 상한이 올라가는 것은 신설된 제64조의2 제2항이 정한 세 경우뿐이고 원칙 조항은 그대로 남습니다. 세 경우는 재위반, 고의·중과실에 의한 대규모 피해, 시정조치 불이행이며 각각의 요건과 기간은 신구조문 대조표에 조문 그대로 실어 두었습니다.

Q. 시행 전에 준비를 못 했습니다. 지금 무엇부터 해야 하나요?

먼저 문서의 조문 인용부터 고칩니다. 사고대응 절차서·위·수탁 계약서·개인정보 처리방침에 「법 제34조 제3항에 따른 신고」나 「법 제31조 제3항」이 남아 있으면 지금은 다른 조항을 가리킵니다. 다음이 서식입니다. 유출 통지문에는 제34조 제1항 제6호가 신설한 손해배상·법정손해배상·분쟁조정 등 법적 권리와 그 행사 방법이 들어가야 하고, 사고대응 절차서에는 유출이 확인되지 않아도 가능성을 알게 된 때부터 72시간 안에 통지하는 분기가 필요합니다. 의사결정이 필요한 것은 셋입니다. 이사회 의결·신고 대상이라면 시행 전에 지정한 보호책임자도 시행일부터 6개월 안에 신고해야 하고, 시행일에 종료되지 않았던 위반 상태는 부칙 제3조 제2항에 따라 새 가중 규정의 사정권에 들어가며, 과징금 투자 감경을 소명하려면 위반이 있었던 사업연도의 직전 3개 사업연도 투자 이력이 필요합니다.