개인정보 유출 사고 대응 — 인지부터 처분·구상까지

이현섭 변호사(법무법인 세움 파트너) · 기준일 2026-09-12 · 최신판: https://datalaw.kr/guides/data-breach-response/

핵심 요약 — 개인정보 유출 사고는 ① 인지 ② 72시간 내 통지·신고 ③ 원인 규명 ④ 개인정보위 조사 ⑤ 처분과 공표 ⑥ 기업 간 책임 배분 순으로 진행되고, 단계마다 근거 조문과 판단 기준이 다릅니다. 이 페이지는 각 단계에서 어느 글을 읽어야 하는지를 정리한 지도이며, 인지 후 72시간에 무엇을 해야 하고 무엇을 하면 안 되는지는 이 페이지 2단계에서 조문 단위로 다룹니다. 유출 항목도 경위도 모르는 상태에서 확인된 내용만으로 우선 통지·우선 신고하는 것이 시행령이 정한 기본 절차이고(시행령 제39조 제2항, 제40조 제2항), 그 72시간의 기록은 과징금 고려사항(법 제64조의2 제4항)과 손해배상액 고려사항(법 제39조 제4항)에서 다시 쓰입니다. 원인이 해킹인지 직원 실수인지는 처분 여부를 가르지 않습니다(제64조의2 제1항 제9호). 처분 금액과 결과 공표는 별개의 판단이고, 공표는 법 제66조 제1항에 따른 재량입니다. 2026년 9월 11일부터는 통지·신고 대상인 '유출등'에 위조·변조·훼손이 추가됩니다.

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

사고가 났을 때 가장 흔한 실수는 **순서를 바꾸는 것**입니다. 원인을 규명한 다음 알리려다 기한을 넘기고, 그 지연이 나중에 처분 사유로 남습니다. 이 페이지는 글들을 사고 진행 순서대로 묶었습니다.

1단계 — 이것이 신고 대상 사고인가

먼저 **무엇이 '유출등'인지**를 확정해야 합니다. 개정 전 '유출등'은 분실·도난·유출 세 가지였습니다. 2026년 9월 11일 시행 개정법은 여기에 **위조·변조·훼손**을 더했습니다. 데이터가 밖으로 나간 것이 확인되지 않아도 파일이 훼손된 상태만으로 시계가 돌 수 있다는 뜻입니다.

→ 랜섬웨어로 파일이 암호화만 됐다면 유출 신고를 해야 하나

2단계 — 인지 후 72시간

유출을 인지하는 경로는 보안 관제 업체의 연락일 수도 있고, 고객센터에 접수된 항의일 수도 있고, 외부 제보 메일일 수도 있습니다. 어느 경로든 첫 회의에서는 몇 명분인지, 어떤 항목이 나갔는지, 언제부터였는지를 모릅니다. 이때 거의 반드시 나오는 결론이 "일단 막고, 정확히 파악한 다음에 알리자"인데, 이 판단은 개인정보 보호법(이하 "법")과 시행령이 설계해 둔 시계와 정면으로 충돌합니다. 법은 파악이 끝나지 않은 상태 그대로 72시간 안에 움직이라고 정하고 있습니다.

규모도 원인도 모르는 상태에서 무엇을 먼저 알려야 하나

"확정되면 알리겠다"는 법이 허용하지 않는 선택지입니다. 시행령 제39조 제2항은 유출된 항목이나 시점·경위의 구체적인 내용을 확인하지 못한 경우, 유출 사실과 그때까지 확인된 내용, 그리고 피해 최소화 방법·대응조치·담당부서 안내를 먼저 통지하고, 추가로 확인되는 내용은 확인되는 즉시 통지하도록 정하고 있습니다. 신고도 같은 구조입니다(시행령 제40조 제2항). 법은 "모르는 상태에서의 우선 통지·우선 신고"를 예외가 아니라 기본 절차로 설계해 두었습니다.

통지에는 법 제34조 제1항 각 호의 사항, 즉 유출된 항목, 시점과 경위, 피해 최소화를 위해 정보주체가 할 수 있는 방법, 회사의 대응조치와 피해 구제절차, 피해 신고 접수 부서와 연락처가 들어가야 합니다. 연락처를 알 수 없는 정보주체가 있으면 홈페이지에 30일 이상 게시하는 방법이 있습니다(시행령 제39조 제3항).

통지와 신고의 유예 사유는 어떻게 다른가

72시간을 넘길 수 있는 예외는 좁고, 통지와 신고가 다릅니다. 통지는 접속경로 차단, 취약점 점검·보완, 유출된 개인정보의 회수·삭제 같은 긴급한 조치가 필요한 경우와 천재지변 등 부득이한 사유가 있는 경우에 미룰 수 있지만(시행령 제39조 제1항 제1호·제2호), 신고를 미룰 수 있는 사유는 천재지변이나 그 밖에 부득이한 사유뿐입니다(시행령 제40조 제1항 단서). 긴급 조치가 진행 중이라는 이유로 신고까지 미룰 수는 없다는 뜻이고, 어느 쪽이든 사유가 해소되면 지체 없이 알려야 합니다. "내부 보고 라인

이 길어서", "법무 검토가 안 끝나서"는 여기에 들어가지 않습니다.

시행령 제40조 제1항 단서에는 유출 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우 신고하지 않을 수 있다는 규정도 있습니다. 이 문은 좁습니다. 경로가 확인되었을 것, 회수·삭제 등의 조치가 있었을 것, 그 결과 권익 침해 가능성이 현저히 낮아졌을 것, 세 가지가 모두 충족되어야 합니다. 경로를 추정만 하고 있는 단계, 회수했지만 사본 확산 가능성이 남아 있는 상태라면 이 단서에 기대기 어렵습니다. 그리고 이 단서는 신고에 관한 것일 뿐이어서, 정보주체에 대한 통지 의무는 이 단서로 면제되지 않습니다.

한 명분이 나가도 알려야 하는 쪽이 있습니다

가장 흔한 오해가 "1천 명 미만이니 아무것도 안 해도 된다"는 판단입니다. 통지와 신고는 대상이 다른 별개의 의무입니다.

구분	근거 조문	대상	기한
정보주체 통지	법 제34조 제1항, 시행령 제39조 제1항	모든 유출등 (규모·유형 무관)	알게 된 때부터 72시간 이내
보호위원회·전문기관 신고	법 제34조 제3항, 시행령 제40조 제1항	① 1천 명 이상 유출 ② 민감정보 또는 고유식별정보 유출 ③ 외부로부터의 불법적인 접근에 의한 유출	알게 된 때부터 72시간 이내

통지문에 무엇을 적을지는 법 제34조 제1항이 다섯 가지로 정해 두었고, 2026년 9월 11일 시행 개정법이 손해배상·분쟁조정 등 권리 안내를 여섯째로 더했습니다. 다른 회사들이 그 칸을 실제로 어떻게 채웠는지는 공개 통지문 모음에 모아 두었습니다 — 새로 들어간 여섯째 칸은 지금까지의 문안에서 거의 확인되지 않습니다.

정보주체 통지는 단 한 명분이 유출되어도 적용되고, 통지하지 않으면 3천만 원 이하의 과태료 대상입니다(법 제75조 제2항 제17호). 신고는 시행령 제40조 제1항의 세 경우 중 하나에 해당할 때 의무가 되는데, 각 요건을 뜯어보면 신고 대상이 아닌 사고가 오히려 드뭅니다. 민감정보나 고유식별정보(주민등록번호 등)는 1건이 유출되어도 신고 대상이고, 해킹처럼 외부의 불법적인 접근으로 유출되었다면 규모와 무관하게 신고 대상입니다. 신고를 받는 전문기관은 한국인터넷진흥원입니다(시행령 제40조 제3항).

의무자가 누구인지는 데이터를 어디에서 받았는지로 갈리지 않습니다. 제휴사 API를 통해 넘어와 우리 서버에 남아 있던 개인정보가 유출됐다면 통지·신고 의무는 그것을 보유한 쪽에 있습니다. 그 구조는 3단계의 제휴 API 글에서 조문 단위로 정리했습니다.

석 달 전 침입인데 시계는 오늘부터 돕니다

기산점은 유출이 발생한 시점이 아니라 유출을 "알게 되었을 때"입니다. 법 제34조 제1항은 유출등을 알게 되었을 때 지체 없이 정보주체에게 알리도록 하고, 시행령 제39조 제1항과 제40조 제1항이 그 기한을 알게 된 때부터 72시간 이내로 구체화하고 있습니다. 침입이 석 달 전에 있었더라도 시계는 회사가 인지한 순간부터 돌기 시작하고, 반대로 원인 규명이 끝나야 시계가 시작되는 것도 아닙니다.

실무에서 먼저 해야 할 일은 인지 시점의 기록입니다. 누가, 몇 시에, 무엇을 근거로 유출을 인지했는지를 문서로 남겨 두어야 합니다. 72시간 준수 여부는 결국 기산점을 어디로 보느냐의 문제인데, 인지 경위에 대한 기록이 없으면 이후 조사 과정에서 회사 스스로 기산점을 설명할 수단이 없어집니다.

초기 72시간에 하면 안 되는 일 세 가지

첫째, 성급한 원인 단정입니다. 확인되지 않은 원인이나 규모를 초기 공지에 단정적으로 쓰는 경우가 있습니다. "외부 침입 흔적은 없습니다", "유출 규모는 ○건에 한정됩니다" 같은 문장이 뒤에 뒤집히면, 정정 자체가 이후 조사와 분쟁에서 회사 설명 전체의 신뢰성 문제로 남습니다. 시행령 제39조 제2항이 "그때까지 확인된 내용"을 알리고 추가 확인분은 즉시 통지하는 2단 구조를 마련해 둔 이유가 여기에 있습니다. 확인된 것과 확인 중인 것을 구분해서 쓰는 것이 법이 예정한 방식입니다.

둘째, 축소 통지입니다. 통지 대상을 임의로 좁히거나, 법 제34조 제1항 각 호 중 일부(특히 유출 항목이나 경위)를 빼고 알리는 것입니다. 통지 의무 위반은 3천만 원 이하의 과태료 대상이지만(법 제75조 제2항 제17호), 과태료만의 문제가 아닙니다. 2026년 9월 11일부터 통지 사항에 손해배상·법정손해배상 청구와 분쟁조정 등 정보주체의 법적 권리와 행사 방법 안내가 추가됐습니다(개정 법 제34조 제1항 제6호). 통지문이 사과문이 아니라 정보주체의 권리 행사 안내문의 성격을 갖게 되는 것이고, 축소 통지는 그 출발점부터 어긋난 문서가 됩니다.

셋째, 로그 미보전입니다. 침해 대응을 서두르다 서버를 초기화·재설치하거나 접속기록을 덮어써 버리는 경우입니다. 개인정보처리시스템 접속기록은 1년 이상, 5만 명 이상의 정보주체를 처리하거나 고유식별정보·민감정보를 처리하는 시스템 등은 2년 이상 보관해야 하고(「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2026-9호) 제8조 제1항), 위·변조·도난·분실되지 않도록 안전하게 보관할 의무도 있습니다(같은 조 제3항). 더 중요한 것은 방어의 관점입니다. 유출에 대한 과징금 규정에는 안전성 확보에 필요한 조치를 다한 경우에는 부과하지 않는다는 단서가 있고(법 제64조의2 제1항 제9호 단서), 과징금 산정 시 암호화 등 안전성 확보 조치 이행 노력이 고려 요소로 열거되어 있습니다(같은 조 제4항 제4호). 그 조치를 다했다는 사실을 보여줄 수 있는 것이 로그입니다. 로그를 지우는 것은 의무 위반을 하나 추가하면서, 동시에 방어의 재료를 스스로 없애는 일입니다.

72시간 안에 한 일이 나중에 과징금에 어떻게 반영되나

개인정보가 유출된 경우 전체 매출액의 3%를 초과하지 않는 범위에서 과징금이 부과될 수 있습니다(법 제64조의2 제1항 제9호. 매출액이 없거나 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 20억 원 이내). 법 제64조의2 제5항은 과징금 부과 시 고려할 사항을 열거하고 있는데, 그중에는 안전성 확보 조치 이행 노력(제4호), 피해의 회복 및 피해 확산 방지 조치의 이행 여부(제6호), 보호위원회와의 협조 등 위반행위를 시정하기 위한 조치 여부(제11호)가 들어 있습니다. 위반의 내용·정도가 경미한 경우 등에는 과징금을 부과하지 않을 수 있다는 규정도 있습니다(같은 조 제5항 제3호·제4호).

다만 2026년 9월 11일 개정으로 이 조문의 구조가 바뀌었으므로 개정 전 자료를 인용할 때 주의해야 합니다. 3년 내 반복 위반, 피해 정보주체 1천만 명 이상, 시정명령 불이행 후 유출 같은 경우에 전체 매출액의 100분의 10(매출액 산정이 곤란하면 50억 원)까지 부과할 수 있는 가중 규정이 제2항으로 신설되면서, 종전 제4항의 고려사항은 제5항으로, 과징금을 부과하지 않을 수 있는 사유는 제7항으로 밀렸고, 개인정보 보호를 위한 예산·인력·설비 투자와 운영 실적이 있는 경우의 감경 규정이 제6항으로 신설됐습니다(법률 제21445호).

민사 쪽도 같은 구조입니다. 손해배상액을 정할 때 법 제39조 제4항은 유출된 개인정보를 회수하기 위해 노력한 정도(제7호)와 피해구제를 위해 노력한 정도(제8호)를 고려하도록 합니다. 초기 72시간의 행위(확산 방지 조치, 통지·신고, 조사 협조)는 그 자체로 법이 과징금과 배상액 판단에서 고려하도록 정해 둔 항목들입니다. 결과가 어떻게 될지는 개별 사안마다 다르고 누구도 예측할 수 없지만, 무엇이 고려 대상인지는 조문에 이미 적혀 있습니다. 사고 당일의 기록은 규제 대응 문서이면서 동시에 소송 자료이고, 그때 남기지 않으면 나중에 만들 수 없습니다.

2026년 9월 11일부터 통지·신고에서 달라진 것

2026년 3월 10일 공포된 개정 개인정보 보호법(법률 제21445호)이 2026년 9월 11일 시행됐습니다. 이 단계와 직결되는 변화는 넷입니다.

첫째, "유출등"의 범위가 넓어집니다. 현행 제34조 제1항은 분실·도난·유출 세 가지를 "이 조에서" 통용되는 약칭으로 정의하고 있는데, 개정법은 이 정의를 삭제하고 제23조 제2항에 분실·도난·유출·위조·변조 또는 훼손을 "유출등"으로 정의하는 문언을 두었습니다. 제23조는 민감정보의 처리 제한을 정한 조문이지만 이 약칭에는 "이 조에서"라는 한정이 없고, 제34조가 자체 정의를 버린 이상 그 조문의 유출등은 제23조 제2항을 원용할 수밖에 없습니다. 밖으로 나간 것이 확인되지 않은 랜섬웨어 암호화 사고가 통지·신고 대상이 되는지는 이 지점에서 갈리며, 조문 단위 정리는 1단계의 글에 있습니다.

둘째, 유출 "가능성" 단계의 통지 의무가 신설됩니다. 대통령령으로 정하는 유출등의 가능성이 있음을 알게 되었을 때, 가능성이 있는 모든 정보주체에게 피해 최소화 정보 등을 알려야 합니다(개정 법 제34조 제2항). 확정된 유출만 알리면 되던 구조가 바뀌는 것입니다.

셋째, 통지 사항이 늘어납니다. 손해배상·법정손해배상 청구와 분쟁조정 등 정보주체의 법적 권리와 행사 방법 안내(신설 제6호), 대통령령으로 정하는 사항(신설 제7호)이 추가되고, 피해 최소화 방법 안내는 "구체적인" 정보여야 한다는 문구로 강화됩니다. 이에 따라 항 번호도 밀려서, 현행 제34조 제3항의 신고 의무는 개정법에서 제4항이 됩니다.

넷째, 이 개정을 구체화할 시행령이 공포됐습니다. 개인정보보호위원회가 2026년 6월 2일 입법예고한 시행령 일부개정령안(개인정보보호위원회 공고 제2026-59호, 예고기간 2026년 6월 2일~7월 13일)은 2026년 8월 31일 법제처 심사를 거쳐 **2026년 9월 10일 대통령령 제36671호로 공포**됐습니다. 부칙 제1조의 시행일은 법률과 같은 9월 11일입니다. 제39조의2는 유출 가능성 통지의 요건을 ① 개인정보처리시스템이나 개인정보취급자의 정보기기에 불법적인 접근이 있어 유출등이 의심되지만 어느 정보주체의 개인정보인지 특정하기 곤란한 경우(불법 접근을 알게 된 때) ② 일부 개인정보가 제3자에 의해 거래되는 등 유출등이 확인됐고 다른 정보주체의 개인정보도 유출됐을 수 있다고 인정되는 경우(그 사실을 알게 된 때)로 정하고, 통지 사항으로 가능성 있는 개인정보 항목, 의심되는 시점과 경위, 피해 최소화 방법·대응조치·담당부서, 유출 여부가 확정되면 추가 통지한다는 사실을 들었습니다. 제39조의3은 기한을 위 시점부터 72시간 이내로 정하고, 기한 안에 실제 유출이 확인되면 제34조 제1항의 통지로 갈음하며, 실제로 유출되지 않았음이 확인되면 그 사실도 즉시 통지하도록 합니다. 연락처를 알 수 없는 등 정당한 사유가 있으면 홈페이지에 30일 이상 게시하는 것으로 갈음할 수 있습니다. 신설 제7호의 추가 통지 사항은 공포본에도 따로 정해지지 않았습니다. 이제 확정된 문언이므로 통지문 서식을 이 조문으로 만들 수 있습니다.

숫자로 본 현실

개인정보보호위원회와 한국인터넷진흥원이 2026년 5월 15일 발간한 「2025년 개인정보 유출 신고 동향 및 조사·처분 사례」에 따르면, 2025년 접수된 유출 신고는 447건으로 2024년 307건 대비 약 45.6% 증가했습니다. 원인별로는 해킹이 62%(276건), 업무 과실이 25%(110건), 시스템 오류가 5%(24건)였습니다. 같은 해 개인정보위의 조사·처분은 총 227건, 과징금은 40건 1,677억 원, 과태료는 125건 5억 8,720만 원이었고, 이 중 115건이 유출 관련 조사·처분이었습니다.

두 가지를 눈여겨볼 만합니다. 민간 부문 처분 150건의 절반인 75건이 중소기업이었으므로, 규모가 작다고 조사와 처분을 비켜가지 않습니다. 그리고 유출 원인의 25%가 업무 과실이어서, 메일 오발송·첨부 실수·접근권한 설정 오류도 해킹과 똑같이 법 제34조의 통지·신고 절차를 작동시킵니다.

72시간 체크리스트

인지 직후

- [ ] 인지 시각, 인지 경위, 인지자를 문서로 기록하라
- [ ] 접속기록과 서버 로그의 사본을 별도 보전하라 (고시 제8조)
- [ ] 접속경로 차단 등 확산 방지 조치를 하되, 로그를 지우는 방식은 피하라 (법 제34조 제3항)

24시간 내

- [ ] 신고 대상 여부를 판단하라: 1천 명 이상인지, 민감정보·고유식별정보인지, 외부 불법접근인지 (시행령 제40조 제1항)
- [ ] 확인된 사실과 확인 중인 사항을 구분한 사실관계 문서를 만들어라
- [ ] 법 제34조 제1항 각 호를 기준으로 통지 문안을 준비하라

72시간 내

- [ ] 확인된 내용만으로라도 정보주체에게 우선 통지하라 (시행령 제39조 제2항)
- [ ] 신고 대상이면 보호위원회 또는 한국인터넷진흥원에 우선 신고하라 (시행령 제40조 제1항·제2항)
- [ ] 연락처를 알 수 없는 정보주체가 있으면 홈페이지 30일 이상 게시를 검토하라 (시행령 제39조 제3항)

그 이후

- [ ] 추가로 확인되는 내용은 확인되는 즉시 통지·신고하라

- [ ] 피해 최소화 대책의 이행 내역을 기록으로 남겨라 (법 제64조의2 제5항 제6호)
- [ ] 조사에 대비해 안전조치 이행 자료를 정리하라 (법 제64조의2 제1항 제9호 단서)

72시간은 대응의 전부가 아니라 입구입니다. 뒤로 개인정보보호위원회의 자료제출 요구와 검사(법 제63조), 사전 실태점검(제63조의2), 시정조치·과징금·과태료·고발과 공표(제64조·제64조의2·제75조·제65조·제66조), 그리고 손해배상과 집단분쟁조정(제39조·제39조의2·제49조)이 차례로 오고, 이 페이지의 4단계부터가 그 순서입니다. 마지막 단계에서 회사가 받아 드는 조정안에는 회신 기한이 15일이고, 회신하지 않으면 수락으로 봅니다. 그 기한과 효력은 조정안을 받고 15일 안에 회신하지 않으면 수락입니다에, 여섯 단계 각각의 조문과 9월 개정이 배상 조문까지는 오지 않는 이유는 유출 통지·신고를 마친 다음 — 조사·처분·분쟁으로 이어지는 여섯 단계에 정리해 두었습니다. 유출 통지·신고 의무(법 제34조) 위반으로 실제 부과된 처분은 개인정보 유출 통지·신고 위반 제재 사례에서 의결일·피심인·위반 조문·금액으로 걸러 볼 수 있습니다.

본사 인시던트 대응 절차서를 쓰는 회사는 여기서 한 번 걸립니다. GDPR 기준 절차서는 위험도 평가를 첫 분기점에 두는데, 한국법 제34조 제1항은 위험 정도를 요건으로 삼지 않습니다. 암호화에 따른 통지 면제도 없습니다.

→ 본사 인시던트 대응 플레이북을 한국에 그대로 적용할 수 있나

3단계 — 원인이 무엇이든 신고 의무자는 우리인가

원인별로 "우리가 피해자인데 왜 우리가 의무자인가"라는 질문이 반복됩니다. 아래는 그 질문이 실제로 나오는 네 가지 상황입니다.

직원의 업무 과실 — 제64조의2 제1항 제9호는 '유출된 경우' 자체를 사유로 정하고 원인을 묻지 않습니다. 2025년 유출 관련 조사·처분 115건에서 원인 1위가 업무 과실(53건, 46%)이었습니다.

→ 해킹이 아니라 직원 실수였습니다 — 업무 과실 유출도 개인정보 과징금 대상인가

퇴사자의 데이터 반출 — 회사는 영업비밀 침해 사건의 원고이면서 동시에 개인정보 유출의 통지 의무자입니다. 두 자리가 같은 사실관계 위에서 서로 반대 방향을 요구하는데, 어느 쪽을 먼저 확정해야 하는지는 아래 글에 있습니다.

→ 퇴사자가 고객 데이터를 가지고 나갔습니다 — 우리는 피해자인데 왜 신고 의무자인가

수탁사에서 난 사고 — 콜센터·배송·전산 유지보수 어느 쪽이든 책임의 무게중심은 위탁사에 있습니다.

→ 수탁사 직원의 실수로 개인정보가 유출됐다 — 위탁사는 어디까지 책임지나

고객 사업장에 놓인 우리 장비 — 기준은 장비가 어디에 있는지가 아니라 인증과 접속통제를 누가 하는지입니다. 키오스크·단말·온프레미스 설치형 제품을 고객사에 두는 회사에 그대로 적용됩니다.

→ 우리 장비가 고객 사업장에 설치돼 있습니다 — 거기서 난 사고는 누가 책임지는가

받는 쪽이 되는 경우도 있습니다. 요청하지 않은 개인정보가 제휴 API 응답에 섞여 들어와 보관되고 있었다면, 받은 쪽이 어느 조문의 수범자가 되는지부터 갈라야 합니다.

→ 제휴 API 응답에 요청하지 않은 개인정보가 섞여 왔습니다 — 받은 쪽도 책임이 있는가

원인을 하나씩 짚은 뒤에는 전체를 유형으로 놓고 볼 수 있습니다. 유출 경위가 기재된 결정문 180건은 여섯 유형으로 갈리고 과징금 부과율은 0%에서 54%까지 벌어지는데, 담당자의 단순 실수 38건에 과징금이 한 건도 없었던 이유는 유출 규모가 아니라 위원회가 거는 조문에 있습니다.

→ 우리 회사 유출은 어느 유형인가 — 개인정보위 결정문 180건의 경위 분류와, 유형마다 갈린 처분

4단계 — 조사와 처분

실제 처분이 어디에 어떤 유형으로 내려지는지는 통계로 보는 편이 빠릅니다. 2026년 상반기 개인정보위는 38개 사업자·기관에 과징금 6,806억 7,100만 원을 부과했고, 위반유형 1위는 안전조치의무였습니다.

→ 2026년 상반기 개인정보위 제재 정리: 과징금 6,807억 원은 어디에 부과됐나

조문 단위로도 갈라 볼 수 있습니다. 안전조치의무(제29조) 건에서 과징금은 건이고, 유출 통지·신고(제34조) 건에서는 **통지·신고 해태만으로 과징금이 부과된 사건이 확인되지 않습니다.** 신고를 늦게 한 것과 안전조치가 미흡했던 것은 처분의 무게가 다릅니다.

금액의 셈법은 2026년 9월 11일부터 달라졌습니다. 중대·반복 위반의 상한이 매출액 10%가 되고, 신속 신고를 감경 요소로, 은폐를 가중 요소로 다루는 방향이 함께 움직이고 있습니다.

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

셈법이 바뀌어도 감경을 주장하고 입증하는 부담은 조사받는 회사에 있습니다. 2026년 결정문 세 건에서 실제로 금액을 깎은 사유가 무엇이었는지는 아래 글에 정리했습니다.

→ 과징금이 '전체 매출액'으로 바뀐 뒤 실제로 인정된 감경 사유

피해 회복 조치는 고시상 감경 사유이지만, 보상 사실이 결정문에 적혔다고 해서 모두 산정에 반영되지는 않았습니다. 사고 직후 보상안을 결재할 때 무엇을 봐야 하는지는 아래 글이 다룹니다.

→ 유출 피해자에게 먼저 보상하면 과징금이 줄어드나요? 결정문 8건의 피해 회복 감경

조사가 유출 사고에서만 시작되는 것은 아닙니다. 위반 혐의도 신고도 없을 때 나오는 사전 실태점검이라는 입구가 따로 있고, 거기서 받은 시정권고를 수락하면 시정조치 명령을 받은 것으로 보기 때문에 수락은 협조가 아니라 지위가 바뀌는 결정입니다.

→ 개인정보위가 혐의 없이 점검을 나왔습니다 — 시정권고를 수락하면 그때부터 무엇이 달라지나

5단계 — 공표는 금액과 따로 결정됩니다

같은 날 의결된 사건에서 과태료가 더 많은 회사는 공표되지 않고 더 적은 회사가 1년간 공표된 사례가 있습니다. **금액과 공표는 같은 저울에 있지 않다**는 뜻이고, 그래서 의견제출도 두 갈래로 나누어 준비해야 합니다. 어느 요건에서 갈렸는지는 아래 글이 의결서 단위로 대조해 두었습니다.

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

6단계 — 처분이 끝난 뒤의 책임 배분

사고 대응은 처분으로 끝나지 않습니다. 위탁 관계였다면 그다음이 기업 간 책임 배분입니다.

계약이 끝난 뒤에 남아 있던 데이터에서 사고가 난 경우에는 처분이 발주사가 아니라 수탁사에게 온 사례가 있습니다. 제26조 제8항이 파기·안전조치·통지 의무를 수탁자에게 준용하기 때문입니다.

→ 위탁계약이 끝났는데 수탁사 서버에 데이터가 남아 있었습니다 — 위탁사와 수탁사 중 누가 처분을 받는가

먼저 배상한 쪽이 상대에게 돌려받는 경로는 열려 있지만, 돌아오는 금액은 배상액 전액이 아닙니다. 비율이 어떻게 정해지고 무엇이 그것을 가르는지는 아래 글에 있습니다.

→ 수탁사 잘못으로 우리가 먼저 손해배상을 했습니다 — 수탁사로부터 돌려받는 금액은 어떻게 결정되는가

책임을 나눈 뒤에는 그 손실을 어느 보험이 덮는지가 남습니다. 배상책임보험은 정보주체에 대한 손해배상금을 덮고 공개된 약관은 과징금을 제외하므로, 이사에게 오는 청구까지 포함해 보험별 범위를 아래 글에서 확인하실 수 있습니다.

→ 유출 과징금도 보험으로 처리되나요? 과징금 특약과 D&O 면책 조항

처분과 별개로 정보주체가 직접 청구해 오면 얼마가 인정되나

개인정보보호위원회의 처분과 정보주체의 민사 손해배상은 별개로 판단됩니다. 안전조치의무 위반으로 과징금이 부과된 사건에서도 민사에서는 청구가 기각되고 대법원에서 확정된 예가 있습니다(대법원 2023다311184). 그 판결은 법정손해배상(제39조의2) 청구에서도 개인정보처리자가 정신적 손해의 부존재를 증명하면 면책된다고 정리했습니다.

대량 유출 사건에서 결과를 가르는 것은 유출 사실 자체가 아니라, 유출된 정보가 실제로 제3자에게 유통·열람됐는가입니다. 법원은 유출된 정보의 종류와 성격, 정보주체 식별 가능성, 제3자의 열람 여부 또는 열람 가능성, 유출 범위와 확산 정도, 개인정보를 처리하는 자의 관리 실태와 유출 경위, 피해 확산을 막기 위해 취한 조치를 함께 봅니다(대법원 2012. 12. 26. 선고 2011다59834). 직원이나 기관이 특정인의 정보를 조회·누설한 내부자 누설은 피해자 한 사람의 사정을 따져 액수를 정하므로 인정액의 폭이 대량 유출보다 훨씬 넓고, 두 유형의 금액을 섞어 평균을 내면 안 됩니다.

→ 유출 손해배상 판결 정리

소송까지 가지 않고 끝나는 구제 절차가 분쟁조정이고, 실제로 가장 많이 쓰입니다. 개인정보분쟁조정위원회가 조정안을 제시하고 양쪽이 수락하면 재판상 화해와 같은 효력이 생기며, 조정안을 받은 날부터 15일 안에 수락 여부를 알리지 않으면 수락한 것으로 봅니다(제47조 제3항). 공개된 조정 사례는 비실명이어서 피신청인 회사 이름이 나오지 않고, 사건은 업종과 침해유형으로 특정됩니다.

→ 개인정보 분쟁조정 사례 조회

자주 묻는 질문

Q. 유출 규모를 아직 파악하지 못했는데 72시간을 넘겨도 되나요?

원칙적으로 안 됩니다. 확인된 내용만으로 72시간 안에 우선 통지·우선 신고하고, 추가로 확인되는 내용을 즉시 보태는 것이 시행령이 정한 절차입니다(제39조 제2항, 제40조 제2항). 기한을 미룰 수 있는 예외는 좁고 통지와 신고가 서로 다른데, 그 구분은 위 2단계에 조문 단위로 정리돼 있습니다. 유출 경로가 확인되어 회수·삭제로 침해 가능성이 현저히 낮아지면 신고는 면할 수 있으나(제40조 제1항 단서 후단), 정보주체 통지에는 그런 면제 규정이 없습니다.

Q. 초기 대응 중에 서버를 재설치했는데 문제가 되나요?

문제가 됩니다. 침해 대응을 서두르다 서버를 초기화·재설치하거나 접속기록을 덮어쓰면 두 가지가 동시에 일어납니다. 첫째, 접속기록 보관 의무 위반입니다. 개인정보처리시스템 접속기록은 1년 이상, 5만 명 이상의 정보주체를 처리하거나 고유식별정보·민감정보를 처리하는 시스템 등은 2년 이상 보관해야 하고, 위·변조·도난·분실되지 않도록 안전하게 보관할 의무도 있습니다(「개인정보의 안전성 확보조치 기준」 제8조 제1항·제3항). 둘째, 방어의 재료가 사라집니다. 유출 과징금에는 안전성 확보에 필요한 조치를 다한 경우 부과하지 않는다는 단서가 있고(법 제64조의2 제1항 제9호 단서), 산정 시에도 안전조치 이행 노력이 고려 요소입니다(같은 조 제4항 제4호). 그 조치를 다했다는 사실을 보여줄 수단이 로그입니다.

Q. 해킹이 아니라 직원 실수인데도 과징금 대상인가요?

대상이 됩니다. 과징금 조항은 유출이라는 결과를 사유로 삼고 원인의 종류를 요건으로 두지 않으며, 2025년 유출 관련 조사·처분에서도 원인 1위는 해킹이 아니라 업무 과실이었습니다. 원인은 처분 여부가 아니라 금액 쪽에서 안전조치 이행 수준과 사후 대응을 통해 반영됩니다. 조문과 건수는 3단계가 가리키는 글에 있습니다.

Q. 수탁사에서 사고가 났는데 우리도 처분을 받나요?

사고 국면과 계약 종료 국면이 다릅니다. 수탁사 직원의 과실로 사고가 난 경우 책임의 무게중심은 위탁사에 있고, 제26조 제4항·제7항과 제64조의2 제1항 제5호가 그 구조를 만듭니다. 반면 계약이 끝난 뒤 수탁사가 파기하지 않아 생긴 사고에서는 제26조 제8항의 준용에 따라 수탁사 자신이 처분 대상이 된 사례가 있습니다.

관련 가이드

- 2026년 개정 개인정보 보호법 — 9월 11일부터 무엇이 달라졌나
- 위탁·수탁 개인정보 책임 지도

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

- 개인정보 보호법 · 개인정보 보호법 시행령 — 국가법령정보센터
- 개인정보의 안전성 확보조치 기준 — 국가법령정보센터(행정규칙)
- 개정 개인정보 보호법(법률 제21445호, 2026. 9. 11. 시행) 원문 — 국가법령정보센터 시행예정 법령
- 개인정보위, 2025년 개인정보 유출 신고 및 조사·처분 사례 분석결과 보도자료 — 개인정보보호위원회
- 개인정보보호위원회 처분 결과 공표 — 개인정보보호위원회

자주 묻는 질문

Q. 유출 규모를 아직 파악하지 못했는데 72시간을 넘겨도 되나요?

원칙적으로 안 됩니다. 유출 항목이나 경위를 확인하지 못한 경우에는 유출 사실과 그때까지 확인된 내용, 피해 최소화 방법 등을 72시간 안에 우선 통지·우선 신고하고, 추가로 확인되는 내용을 확인되는 즉시 알리는 것이 법이 정한 절차입니다(시행령 제39조 제2항, 제40조 제2항). 72시간을 미룰 수 있는 예외는 통지와 신고가 다릅니다. 통지는 접속경로 차단·취약점 보완·회수삭제 등 긴급한 조치가 필요한 경우와 천재지변 등 부득이한 사유가 있는 경우에 미룰 수 있고(시행령 제39조 제1항), 신고는 천재지변 등 부득이한 사유가 있는 경우에만 미룰 수 있습니다(시행령 제40조 제1항 단서). 어느 쪽이든 사유가 해소되면 지체 없이 알려야 합니다. 같은 단서 후단은 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치로 정보주체의 권익 침해 가능성이 현저히 낮아진 경우 신고하지 않을 수 있도록 정하고 있으나, 정보주체 통지에는 그런 면제 규정이 없습니다.

Q. 초기 대응 중에 서버를 재설치했는데 문제가 되나요?

문제가 됩니다. 침해 대응을 서두르다 서버를 초기화·재설치하거나 접속기록을 덮어쓰면 두 가지가 동시에 일어납니다. 첫째, 접속기록 보관 의무 위반입니다. 개인정보처리시스템 접속기록은 1년 이상, 5만 명 이상의 정보주체를 처리하거나 고유식별정보·민감정보를 처리하는 시스템 등은 2년 이상 보관해야 하고, 위·변조·도난·분실되지 않도록 안전하게 보관할 의무도 있습니다(「개인정보의 안전성 확보조치 기준」 제8조 제1항·제3항). 둘째, 방어의 재료가 사라집니다. 유출 과징금에는 안전성 확보에 필요한 조치를 다한 경우 부과하지 않는다는 단서가 있고(법 제64조의2 제1항 제9호 단서), 산정 시에도 안전조치 이행 노력이 고려 요소입니다(같은 조 제4항 제4호). 그 조치를 다했다는 사실을 보여줄 수단이 로그입니다.

Q. 해킹이 아니라 직원 실수인데도 과징금 대상인가요?

대상이 됩니다. 과징금 조항은 유출이라는 결과를 사유로 삼고 원인의 종류를 요건으로 두지 않으며, 2025년 유출 관련 조사·처분에서도 원인 1위는 해킹이 아니라 업무 과실이었습니다. 원인은 처분 여부가 아니라 금액 쪽에서 안전조치 이행 수준과 사후 대응을 통해 반영됩니다. 조문과 건수는 3단계가 가리키는 글에 있습니다.

Q. 수탁사에서 사고가 났는데 우리도 처분을 받나요?

사고 국면과 계약 종료 국면이 다릅니다. 수탁사 직원의 과실로 사고가 난 경우 책임의 무게중심은 위탁사에 있고, 제26조 제4항·제7항과 제64조의2 제1항 제5호가 그 구조를 만듭니다. 반면 계약이 끝난 뒤 수탁사가 파기하지 않아 생긴 사고에서는 제26조 제8항의 준용에 따라 수탁사 자신이 처분 대상이 된 사례가 있습니다.