개인정보 사고 뒤 위탁사·수탁사 책임 배분 — 따로 정리할 쟁점을 사내에서 먼저 가려 보는 표

이현섭 변호사(법무법인 세움 파트너) · 기준일 2026-11-17 · 최신판: https://datalaw.kr/guides/breach-liability-allocation-check/

핵심 요약 — 이 표는 개인정보 사고가 난 뒤 위탁사와 수탁사가 상대 회사와의 책임 배분을, 이미 진행 중인 신고·통지·조사 대응과 떼어 사내에서 따로 정리할지 먼저 가려 보는 확인표입니다. 개인정보 보호법 제26조가 만드는 위·수탁 구조를 전제로, 위탁 관계와 원인·규제 대응·비용 분담의 세 묶음 10개 쟁점마다 이미 확인된 사실을 적는 「별도 검토가 열리는 사실」 칸과 아직 확보하지 못한 자료를 적는 「판단에 부족한 사실」 칸을 두었습니다. 이 표는 누가 얼마를 부담하는지, 계약의 배상 상한·면책 조항이 효력을 갖는지, 처분이나 판결이 어떻게 나올지, 외부 자문이 필요한지를 정하지 않습니다. 표시한 결과는 어느 쟁점을 따로 정리할지 고르는 자료로만 씁니다.

누가 이 표를 쓰나

이 표는 사고 대응이 이미 돌아가고 있는 회사를 위해 만들었습니다. 유출 신고와 정보주체 통지를 마쳤거나 진행 중이고, 개인정보위 조사에도 대응하고 있는데, 상대 회사와의 책임 배분을 지금 따로 정리할지는 아직 정하지 못한 상태를 가정했습니다. 그 결정에는 보통 법무·재무 담당자, 개인정보 보호책임자(CPO), 경영진이 함께 관여합니다. 그래서 행 이름 옆 괄호에 그 행을 주로 확인할 부서를 적어, 부서마다 행을 나눠 채운 뒤 한 장으로 모아 볼 수 있게 했습니다.

위탁사와 수탁사 어느 쪽이든 쓸 수 있도록 주어는 「우리 회사」로 적었습니다. 한쪽에만 해당하는 행에는 행 이름에 (위탁사)·(수탁사)를 붙였습니다. 위탁 관계에서 누가 위탁자이고 누가 수탁자인지, 조문이 어떻게 짜여 있는지는 위탁·수탁 개인정보 책임 지도 — 우리는 어느 자리에 있나가 다룹니다. 사고가 인지부터 처분까지 어떤 순서로 진행되는지는 개인정보 유출 사고 대응 — 인지부터 처분·구상까지가 다룹니다. 이 표는 두 가이드 위에서 책임 배분을 따로 떼어 정리할지를 가르는 데에만 씁니다.

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

두 칸은 각각 무엇을 뜻하나

표의 두 칸은 성격이 다릅니다. 첫 칸에는 이미 확인된 사실만 적었고, 둘째 칸에는 아직 손에 들어오지 않은 자료의 이름만 적었습니다. 두 칸은 서로 다른 것을 적으므로 한 행에서 함께 볼 수 있습니다.

- 별도 검토가 열리는 사실: 「문서가 사고 뒤에 작성됐다」 「두 회사의 원인 설명이 다르다」처럼 이미 확인된 사실입니다. 이런 사실이 확인되면 그 쟁점은 진행 중인 신고·통지·조사 대응과 별도로 사내에서 따로 정리할 대상이 됩니다. 이 칸은 외부 자문이 필요하다는 판정이 아니고, 어느 쪽이 불리해지는지도 말하지 않습니다.
- 판단에 부족한 사실: 그 쟁점을 보려면 있어야 하는데 아직 확보하지 못한 자료입니다. 자료가 들어오면 첫 칸의 사실이 확인되는지 다시 봅니다.

첫 칸에 적은 사실들은 아래 「행마다 왜 갈리나」의 근거 문단과 연결 글이 다룬 장면에서 뽑은 예시입니다. 목록이 전부는 아니고, 그 사실이 어느 회사의 법적 책임으로 이어지는지는 이 표가 정하지 않습니다.

여기서 「진행 중인 대응」은 지금 하고 있는 신고·통지·조사 대응과 그 대응을 맡은 체계를 말합니다. 그 체계가 사내 담당자이든 외부 자문사이든 상관없고, 맡은 쪽의 역량을 평가하는 말도 아닙니다. 「별도 검토」는 상대 회사와의 책임 배분을 그 대응에서 떼어 쟁점으로 정리하는 일을 가리킵니다. 그 일은 사내 법무, 지금 사고 대응을 맡은 자문사, 다른 변호사 누구든 맡을 수 있습니다.

표는 어떤 순서로 채우나

1. 「판단에 부족한 사실」 칸부터 봅니다. 행마다 적힌 자료 가운데 아직 확보하지 못한 것을 표시하고, 담당 부서가 모읍니다.
2. 확보한 자료로 「별도 검토가 열리는 사실」 칸의 사실이 확인되는지 봅니다. 확인된 사실이 있는 행에만 표시하고, 표시하지 않은 행은 「확인해 보니 해당 없음」과 「아직 확인 못 함」으로 나눠 적어 둡니다. 같은 기록이라도 찾아본 범위에서 없었다면 그 범위를 함께 적어 첫 칸에, 아직 찾아보지 못한 곳(상대방 보관분 등)이 남았다면 둘째 칸에 둡니다.
3. 첫 칸에 표시된 행은 떼어 사내에서 따로 정리할 쟁점으로 올립니다. 「아직 확인 못 함」으로 남은 행은 자료가 들어오는 대로 다시 봅니다 — 표시가 없다고 검토를 끝낸 것이 아닙니다.
4. 첫 칸에 표시된 행이 없더라도 책임 배분 문제가 없다는 뜻은 아닙니다. 둘째 칸의 자료가 들어오거나 조사·청구 과정에서 새 사실이 드러나면 해당 행을 다시 봅니다.

어떤 사실이 책임 배분 검토를 여나

행 이름 옆 괄호는 그 행을 주로 확인하는 부서입니다. 각 행의 근거와 근거의 한계는 표 아래 「행마다 왜 갈리나」에 적었습니다.

묶음 A. 위탁 관계와 사고 원인

쟁점	별도 검토가 열리는 사실	판단에 부족한 사실
1. 위탁 관계가 문서로 서 있는가 (법무)	두 회사 자료를 찾아본 범위에서 사고 당시 체결본은 나오지 않고 사고 뒤에 작성된 문서만 나왔다. 문서에 적힌 명칭(제공·공동이용·processor 등)과 실제 처리 구조가 다르다. 재위탁이 위탁사 동의 기록 없이 이뤄졌다	사고 당시 위탁 문서의 최종본과 체결일·처리기간·자동갱신 조항, 실제 처리 범위를 보여 주는 자료, 재위탁 사슬과 동의 기록
2. 사고가 어디에서, 위탁 범위 안에서 났는가 (보안·법무)	원인 지점이 두 회사 시스템에 걸쳐 있다. 유출된 처리가 위탁 업무 범위 밖이었다. 유출 데이터가 계약 종료 뒤 남아 있던 것이다. 두 회사가 내놓은 원인 설명이 서로 다르다	원인 조사 보고서와 그 작성 주체(상대방 자체 조사뿐인지), 보존된 로그의 범위
3. 교육·감독 기록 (위탁사) / 접근통제·권한 기록 (수탁사) (개인정보)	사고 전 기간의 교육·점검 기록(위탁사)이나 권한 부여·변경·말소 기록(수탁사)에 빠진 기간이 있다. 점검에서 낸 개선 요구에 후속 확인 기록이 없다. 실제 감독 방식이 계약에 약정한 방식과 다르다	계약에 약정한 감독 방식(현장·원격·인증 결과 통지), 사고 전 기간의 교육·점검·권한 관리 기록 원본, 상대방이 보관한 기록
4. 데이터를 어떤 형태로 넘겼는가 (개인정보·보안)	개발·테스트 등에 실데이터 원본이 그대로 넘어갔다(4행 근거 판결에서 쟁점이 된 사실). 위탁 업무에 쓰이지 않는 항목까지 넘어갔다	넘긴 항목 목록과 전달 방식, 누가 무엇을 요청했는지의 기록, 수탁사 쪽 저장 위치

묶음 B. 규제 대응: 누가 무엇을 했고 누가 대상인가

쟁점	별도 검토가 열리는 사실	판단에 부족한 사실
5. 신고·통지를 누가 어떻게 했는가 (개인정보·법무)	상대방의 일괄 신고서에 우리 회사가 빠져 있다. 정보주체 통지가 상대방 명의로만 나갔다. 인지 시점에 관한 두 회사 기록이 다르다	상대방 신고서 사본과 신고 내용, 통지문과 발송 명의·대상·일시, 상대방 통보를 받은 일시의 기록
6. 개인정보위 조사·처분의 대상이 누구인가 (법무)	두 회사가 모두 자료 제출 요구를 받았다. 두 회사가 개인정보위에 낸 원인·경위 설명이 서로 다르다	상대방이 받은 요구서와 제출한 의견, 처분 사전통지를 받았는지 여부

묶음 C. 비용: 누가 먼저 내고 무엇으로 나누나

쟁점	별도 검토가 열리는 사실	판단에 부족한 사실
7. 계약의 손해배상·구상 조항 (법무·재무)	배상 상한이나 면책 조항이 있다. 과징금·대응 비용이 배상 범위에 드는지 문언이 정하지 않았다. 손해배상 조항이 없다. 조항의 적용을 두고 상대방과 견해가 갈렸다	계약서 최종본과 부속 합의·약관, 청구 통지 기한 조항
8. 정보주체의 청구가 들어왔는가 (법무·재무)	소장이나 분쟁조정 신청서를 받았다. 조정안을 제시받아 회신 기한이 진행 중이다. 상대방과 분담을 정하기 전에 정보주체에게 배상금·합의금을 먼저 지급하려는 안이 있다	유출된 정보가 제3자에게 열람·유통됐는지에 관한 자료, 접수된 청구의 규모, 조정안을 제시받은 날
9. 사고 대응 비용과 증빙 (재무)	통지·콜센터·재발급 등 비용을 상대방에게 청구하려 하거나 상대방에게서 청구받았다. 청구 항목을 두고 다툼이 있다	항목별 지출 증빙, 사고 전 같은 기간의 수치(9행 근거 판결에서 비교 기준으로 쓰인 자료)
10. 보험 (재무)	보험사가 이번 사고에 면책 조항(고의·중과실 등)을 들어 회신했거나 보상 여부 회신을 미뤘다(보험사 쪽 의견이고, 보상 여부가 정해졌다는 뜻은 아니다)	증권과 특약 사본, 보험사에 사고를 알린 일시와 보험사 회신, 상대방의 보험 가입 여부

행마다 왜 갈리나

1. 위탁 관계가 문서로 서 있는가

개인정보 보호법 제26조 제1항은 처리 업무의 위탁을 문서로 하도록 정하고, 시행령 제28조 제1항은 그 문서에 담을 사항으로 위탁업무의 목적과 범위, 재위탁 제한, 손해배상 등 책임을 듭니다. 이와 별도로 개인정보위는 자동갱신 조항이 없는 위탁이라면 처리 기간이 끝났을 때 계약을 다시 맺는 등의 조치가 필요하다고 안내했는데(「개인정보 질의응답 모음집」 92번), 이는 법령이 정한 갱신 요건과 구별되는 행정 안내입니다. 따라서 이 행은 사고 당시 어떤 문서가 있었고 무엇이 적혀 있었는지를 사실로 확인하는 데까지만 씁니다. → 「수백 개 고객사와 위수탁 계약을 다 맺을 수 없습니다」 — 수탁 SaaS의 약관과 정책 링크로 제26조 문서 요건이 서는가

2. 사고가 어디에서, 위탁 범위 안에서 났는가

제26조 제7항은 수탁자가 「위탁받은 업무와 관련하여」 개인정보를 처리하다 생긴 손해배상책임을 두고 수탁자를 「개인정보처리자의 소속 직원」으로 봅니다. 위탁 관계에서 그 개인정보처리자는 위탁사입니다. 개인정보위 「개인정보 유출등 대응 안내서」(2026. 9.)도 수탁사가 위탁받은 업무 범위를 벗어난 사유로 유출된 경우를 수탁사 일괄 신고로 갈음되지 않는 예로 들었는데, 이는 법령 문언이 아니라 행정 안내입니다. 한편 위탁계약이 끝난 뒤 수탁사가 파기하지 않은 데이터에서 사고가 난 사건에서는 처분이 수탁사에게 내려졌습니다(의결 제2026-213-269호). → 위탁계약이 끝났는데 수탁사 서버에 데이터가 남아 있었습니다 — 위탁사와 수탁사 중 누가 처분을 받는가

3. 교육·감독 기록과 접근통제·권한 기록

제26조 제4항은 위탁자에게 수탁자를 교육하고 처리 현황 점검 등으로 감독할 의무를 지우고, 위탁자가 이를 소홀히 하여 수탁자가 법을 위반하면 제64조의2 제1항 제5호의 과징금 사유가 됩니다. 보람상조 계열 사건에서 개인정보위는 시스템을 운영한 수탁사(의결 제2026-009-057호)와 별도로 일을 맡긴 계열사 6곳을 각자 피심인으로 의결했습니다(의결 제2026-009-058호~제2026-009-063호). 그 사건에서 그룹이 한 조직처럼 운영됐다는 사정은 과실의 정도를 평가하는 데에만 쓰였고, 제26조 제4항 위반 인정은 그대로였습니다. → 그룹 공용 상담 시스템이 뚫리면 일을 맡긴 계열사도 처분받나 — 보람상조 계열 7건 의결

4. 데이터를 어떤 형태로 넘겼는가

서울중앙지방법원 2025. 9. 4. 선고 2022가합550574 판결(1심·확정)은 구상금 사건에서 위탁사의 부담부분을 정하면서, 위탁사가 고객정보를 변환하지 않은 원본 그대로 넘겼다는 사실을 들었고 그 제공이 수탁사 측 요청에 따른 것이었다는 사실도 함께 적었습니다. 다만 이 판결은 9행의 판결들과 같은 한 사고(2014년 카드고객정보 유출)에서 나온 것입니다. 표의 「원본 전달」은 그 판결에서 쟁점이 된 사실이라는 뜻이고, 다른 사고에서도 같은 사실이 같은 무게로 다뤄진다는 뜻은 아닙니다. → 수탁사 잘못으로 우리가 먼저 손해배상을 했습니다 — 수탁사로부터 돌려받는 금액은 어떻게 결정되는가

5. 신고·통지를 누가 어떻게 했는가

같은 사고에서 위탁사와 수탁사 양쪽에 신고 의무가 생길 수 있는 것은, 제26조 제8항이 제34조의 통지·신고 의무를 수탁자에게도 준용하기 때문입니다. 수탁사가 위탁사들을 명시해 일괄 신고하면 위탁사의 신고를 갈음한다고 볼 수 있다는 것은 개인정보위 안내서의 설명이고, 안내서는 그 범위를 같은 경위로 유출된 경우로 좁혔습니다. 우리 회사가 일괄 신고에 기대려 할 때 무엇을 확인할지는 아래 글의 해당 절에 정리돼 있습니다. → 수탁사 직원의 실수로 개인정보가 유출됐다 — 위탁사는 어디까지 책임지나

6. 개인정보위 조사·처분의 대상이 누구인가

수탁사도 제26조 제8항의 준용에 따라 자기 매출액을 기준으로 과징금을 받을 수 있는 의무 주체이고, 위탁사가 제64조의2 제1항 제5호로 과징금을 받을 때의 매출액은 위탁사의 매출액입니다. 보람상조 계열 사건처럼 수탁사와 위탁사들이 같은 사건번호 아래 각각 따로 의결된 경우가 있습니다. 그런 경우에는 두 회사가 같은 조사 절차 안에 함께 놓이고, 각자 낸 설명을 서로 맞춰 볼 일이 생길 수 있습니다. → 수탁사 직원의 실수로 개인정보가 유출됐다 — 위탁사는 어디까지 책임지나

7. 계약의 손해배상·구상 조항

두 회사 사이의 정산을 볼 때는 위·수탁 계약서의 손해배상 조항이 먼저 확인 대상이 되고, 그 조항에서 살펴볼 곳은 배상 범위의 정의, 상한의 유무, 과징금 등 행정제재금의 포함 여부, 면책 사유입니다. 다만 먼저 배상한 쪽의 구상은 민법상 부진정연대채무의 부담부분 법리로 처리되고, 계약의 상한·면책 조항이 그 법리와 어떻게 맞물리는지나 실제로 효력을 갖는지는 이 표가 답하지 않습니다. 조항이 있는지와 그 문언은 규제 대응이 진행되는 동안에도 확인해 둘 수 있습니다. → 수탁사 직원의 실수로 개인정보가 유출됐다 — 위탁사는 어디까지 책임지나

8. 정보주체의 청구가 들어왔는가

정보주체가 손해배상을 청구할 때는 제26조 제7항이 수탁자를 개인정보처리자(위탁사)의 소속 직원으로 보므로, 정보주체는 수탁사의 잘못으로 생긴 손해도 위탁사를 상대로 청구할 수 있습니다. 분쟁조정의 회신 기한은 조정안을 제시받은 날부터 셉니다. 제47조 제3항은 「제시받은 날부터 15일 이내에 수락 여부를 알리지 아니하면 조정을 수락한 것으로 본다」고 정합니다. 한편 4행의 구상금 판결(2022가합550574)은 먼저 배상한 위탁사의 구상을 자기 부담부분을 넘는 금액에 대해서만 인정했고, 그래서 먼저 지급하려는 회사에는 지급 전에 상대방과 분담을 어떻게 다룰지가 쟁점으로 떠오릅니다. → 수탁사 잘못으로 우리가 먼저 손해배상을 했습니다 — 수탁사로부터 돌려받는 금액은 어떻게 결정되는가

9. 사고 대응 비용과 증빙

2014년 카드고객정보 유출 사고에서 카드회사들이 수탁사에 대응 비용을 청구한 사건들에서 법원은 통지·재발급·콜센터 같은 항목을 하나씩 넣고 뺐고, 재발급 비용은 전년 같은 기간보다 늘어난 몫만 손해로 셌습니다(서울고등법원 2019나2042526, 2022나2004326, 2022나2006841, 모두 확정). 표의 「사고 전 같은 기간의 수치」는 그 판결들에서 비교 기준으로 쓰인 자료를 가리킵니다. 한 사고에서 나온 판결들이므로, 다른 사고에서도 같은 자료가 요구된다는 뜻으로 읽지 않습니다. → 수탁사 잘못으로 우리가 먼저 손해배상을 했습니다 — 수탁사로부터 돌려받는 금액은 어떻게 결정되는가

10. 보험

제39조의7은 일정 기준에 해당하는 개인정보처리자에게 손해배상책임 이행을 위한 보험·공제 가입이나 준비금 적립을 요구합니다. 아래 글이 살펴본 공개 약관 두 종에서는 정보주체에 대한 법률상 손해배상금이 보상 대상이고 과징금·과태료는 손해배상금에서 빠지며, 과징금은 같은 글이 살펴본 특약에서 보상 대상이 되되 그 특약에도 고의(특약에 따라서는 고의·중과실)로 생긴

과징금을 빼는 조항이 있었습니다. 이는 그 약관과 특약에 관한 관찰이고, 우리 회사 증권이 무엇을 보상하는지는 그 증권의 문언으로 정해집니다. → 유출 과징금도 보험으로 처리되나요? 과징금 특약과 D&O 면책 조항

이 표가 답하지 않는 것은 무엇인가

1. 두 회사가 각각 얼마를 부담하는지, 그 비율과 금액은 이 표가 정하지 않습니다. 실제 판결에서 부담부분이 어떻게 정해졌는지는 4·8행의 링크 글에 있습니다.
2. 계약의 배상 상한·면책 조항이 실제로 효력을 갖는지는 다루지 않습니다. 이 표의 7행은 그 조항이 있는지, 문언이 정해져 있는지, 견해가 갈렸는지라는 사실까지만 묻습니다.
3. 개인정보위 처분이나 법원 판결이 어떻게 나올지는 이 표로 알 수 없습니다.
4. 이 표는 외부 자문이 필요한지, 책임 배분 문제가 있는지 없는지를 판정하지 않습니다. 어느 행도 첫 칸에 해당하지 않아도, 그것은 확인한 범위에서 첫 칸의 사실이 나오지 않았거나 아직 확인하지 못했다는 표시일 뿐입니다.
5. 근거에는 한계가 있습니다. 4·9행의 판결은 모두 2014년 카드고객정보 유출 한 사고에서 나온 것입니다. 1행이 인용한 질의응답 모음집과 2·5행이 인용한 유출등 대응 안내서는 개인정보위의 행정 안내이지 법령 문언이 아닙니다. 위탁 문서 없이 운영하다 처분된 최근 사례는 보도자료 기준이고 의결서가 공개되지 않아 이 표의 근거로 쓰지 않았습니다.
6. 이 표는 2026년 9월 11일 시행 개인정보 보호법을 기준으로 2026년 11월 17일에 작성했습니다. 이후 법령이나 안내서가 바뀌면 행의 내용도 달라질 수 있습니다.

이 표는 누가 만들었나

이 표는 법무법인 세움의 이현섭 변호사가 썼습니다. 개인정보 사고 이후 기업 사이의 책임 분쟁은 이현섭 변호사가 주로 다루는 일 가운데 하나이고, 주로 다루는 일의 목록은 문의 안내에 있습니다. 같은 쟁점이라도 회사마다 어떤 사실이 확인될지는 사실관계에 따라 달라질 수 있습니다.

자주 묻는 질문

관련 가이드

- 위탁·수탁 개인정보 책임 지도 — 우리는 어느 자리에 있나
- 개인정보 유출 사고 대응 — 인지부터 처분·구상까지

본 글은 일반적인 정보 제공을 위한 것으로 법률자문이 아닙니다. 구체적 사안은 개별 검토가 필요합니다.

참고 자료

- 개인정보 보호법 · 개인정보 보호법 시행령, 국가법령정보센터
- 법률 제21445호 개정문·부칙, 2026. 9. 11. 시행
- 개인정보 유출등 대응 안내서(2026. 9.), 개인정보보호위원회, 46쪽 FAQ Q2
- 개인정보보호위원회 「개인정보 질의응답 모음집」(2025. 12.) 92번(반복 위탁의 계약 갱신)
- 개인정보보호위원회 의결 제2026-213-269호(2026. 7. 8.), 제2026-009-057호~제2026-009-063호
- 서울중앙지방법원 2025. 9. 4. 선고 2022가합550574 판결(구상금), 2025. 9. 27. 확정
- 서울고등법원 2020. 11. 12. 선고 2019나2042526 판결, 2023. 9. 8. 선고 2022나2004326 판결, 2025. 5. 1. 선고 2022나2006841 판결

- 대법원 2006. 1. 27. 선고 2005다19378 판결), 국가법령정보센터 (부진정연대채무 부담부분과 구상)

자주 묻는 질문

Q. 「별도 검토가 열리는 사실」 칸에 한 행만 해당해도 상대 회사에 청구하거나 소송을 해야 하나요?

이 표는 그렇게 읽도록 만든 것이 아닙니다. 그 행이 책임 배분 쟁점으로 사내에서 따로 정리할 대상이 됐다는 뜻이고, 청구나 소송을 할지, 외부 자문을 받을지는 이 표가 정하지 않습니다. 따로 정리하는 일은 사내 법무, 지금 사고 대응을 맡은 자문사, 다른 변호사 누구든 맡을 수 있습니다.

Q. 어느 행도 「별도 검토가 열리는 사실」 칸에 해당하지 않으면 책임 배분 문제는 없는 것인가요?

그렇게 볼 수 없습니다. 이 표는 책임 배분 문제가 있는지 없는지를 판단하지 않습니다. 첫 칸의 사실을 확인해 보니 해당하지 않았거나 아직 확인하지 못했다는 것일 뿐이고(둘은 구분해 적어 두십시오), 「판단에 부족한 사실」 칸의 자료가 들어오거나 조사·청구 과정에서 새 사실이 드러나면 그 행을 다시 봅니다.

Q. 수탁사도 이 표를 쓸 수 있나요?

쓸 수 있습니다. 개인정보 보호법 제26조 제8항은 유출 통지·신고와 안전조치 의무를 수탁자에게 준용하므로, 수탁사도 같은 사고에서 자기 이름으로 의무를 지는 주체입니다. 그래서 표의 주어를 「우리 회사」로 적었고, 한쪽에만 해당하는 행에는 (위탁사)·(수탁사)를 붙였습니다.