개인정보 국외 이전 지도 — 해외 클라우드·SaaS·AI를 쓰는 회사는 무엇을 갖춰야 하나

이현섭 변호사(법무법인 세움 파트너) · 기준일 2026-11-19 · 최신판: https://datalaw.kr/guides/overseas-transfer/

핵심 요약 — 해외 클라우드에 데이터를 저장하거나, 해외 SaaS와 생성형 AI API를 서비스에 붙이거나, 해외 본사와 고객 정보를 나누는 회사는 대부분 개인정보를 국외로 이전하고 있습니다. 개인정보 보호법 제28조의8 제1항은 국외 제공(조회 포함)·처리위탁·보관을 묶어 「이전」으로 부르고, 원칙적으로 막은 뒤 다섯 가지 경우에만 허용합니다. 회사가 실제로 고를 수 있는 근거는 대개 둘입니다. 하나는 정보주체의 별도 동의(제1호)이고, 다른 하나는 정보주체와의 계약 이행에 필요한 처리위탁·보관을 처리방침에 공개하거나 알리는 방법(제3호)입니다. 제3호는 「제공」을 대상으로 하지 않으므로 받는 쪽이 데이터를 자기 목적으로 쓰는 흐름에는 쓸 수 없습니다. 어느 근거를 쓰든 보호조치를 이전받는 자와 협의해 계약에 반영해야 하고(제4항), 처리방침에는 근거와 법정 사항을 적어야 합니다. 실제 처분은 이전 자체보다 처리방침에 적지 않은 것, 동의라고 볼 수 없는 동의, 서류와 실제 흐름의 불일치에서 나왔습니다.

이 사이트에는 국외 이전을 다룬 글이 열 편 넘게 있습니다. 그런데 상당수가 「본사가 보내온 계약서」에서 출발하는 외국계 한국 법인의 시점으로 쓰였습니다. 이 면의 주 독자는 다릅니다. 해외 클라우드·SaaS·생성형 AI API를 쓰는 한국 회사의 실무자와 대표, 그리고 한국 이용자에게 서비스하는 해외 사업자입니다. 순서는 판단 순서를 따릅니다. 먼저 우리 회사의 데이터 흐름이 국외 이전인지 가리고, 그다음 장면별로 근거와 기재 사항을 보고, 마지막으로 처분 사례와 세부 글로 내려갑니다. 외국계 한국 법인의 담당자라면 본사와 데이터를 나누는 경우 절에서 기존 글로 바로 가실 수 있습니다.

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

우리 회사의 데이터 흐름은 국외 이전인가?

판단은 세 가지 질문으로 나뉩니다. 데이터가 어디에 있는지, 누가 어디에서 그 데이터에 닿을 수 있는지, 받는 쪽이 그 데이터로 무엇을 하는지입니다.

첫째 질문에서 회사가 흔히 놓치는 것은 「보관」입니다. 제28조의8 제1항은 국외로 보관하는 것도 이전에 넣습니다. 따라서 해외 리전의 클라우드나 해외 호스팅 서버에 고객 데이터를 저장하는 회사는 데이터를 다른 회사에 넘기지 않았더라도 이전 근거를 갖추어야 합니다.

둘째 질문은 서버 위치만으로 끝나지 않는다는 점을 짚습니다. 같은 항은 국외 제공에 「조회되는 경우」를 포함시킵니다. 이 사이트의 생성형 AI 처리방침 글은 국내 리전을 쓰더라도 본사나 해외 사업자가 계정 관리·로그·남용 탐지 목적으로 데이터에 접근할 경로가 남아 있다면 이 정의에 걸릴 수 있다고 보았습니다. 데이터가 국경을 넘지 않았는데도 이전으로 다뤄진 경우도 있습니다. 개인정보위는 2026년 7월 틱톡·애플 사건 보도자료에서 국외 이전을 「보호법의 법적 관할이 미치지 않아 보호수준이 담보되지 않는 범위로의 이전」으로 설명했습니다. 그래서 계열사 사이의 이전이나 같은 나라 안의 이전이라도 국외 이전 규정이 적용될 수 있습니다.

셋째 질문이 근거를 가릅니다. 받는 쪽이 우리 회사를 위해 데이터를 처리하고 돌려주는 데 그친다면 처리위탁·보관에 가깝고, 받는 쪽이 그 데이터를 자기 광고나 모델 개선에 쓴다면 제3자 제공에 가깝습니다. 대법원 판결이 제시한 잣대도 같은 방향입니다. 넘긴 목적이 처음 수집한 목적 안에 머무는지, 받는 쪽이 대가를 받는 것 말고 그 정보에서 따로 얻는 이익이 있는지를 함께 봅니다(대법원 2017. 4. 7. 선고 2016도13263 판결). 이 구별이 국외 이전에서 결정적인 이유는 다음 절에서 보듯 제3호가 처리위탁·보관만을 대상으로 하기 때문입니다. 위탁과 제공을 도구별로 가르는 방법은 SDK 위탁·제공 판정 글에 정리되어 있습니다.

확인할 것	국외 이전 쪽으로 기우는 신호	먼저 볼 자료
데이터 위치	해외 리전·해외 호스팅에 저장	클라우드 콘솔, 호스팅 계약
접근 주체	해외 본사·해외 사업자가 조회 가능	계약서, 서브프로세서 목록

확인할 것	국외 이전 쪽으로 기우는 신호	먼저 볼 자료
받는 쪽의 이용	상대가 자기 목적으로 활용	상대 이용약관의 데이터 활용 조항

제28조의8 제1항은 어떤 근거를 열어 두었나?

제28조의8 제1항 단서는 다섯 개 호를 둡니다. 다만 다섯 개가 모두 회사의 선택지는 아닙니다. 기존 글들이 확인한 범위에서 대부분의 회사에게 실무상 남는 경로는 제1호와 제3호이고, 이전처가 EU·EEA인 흐름에 한해 제5호가 더해집니다.

호	근거	회사가 쓸 수 있는가
제1호	국외 이전에 관한 별도 동의	쓸 수 있음. 제2항 다섯 사항을 미리 알려야 함
제2호	법률·조약 등의 특별한 규정	해당 규정이 있을 때만
제3호	계약 체결·이행을 위한 처리위탁·보관 + 공개 또는 통지	가장 많이 쓰임. 제공에는 쓸 수 없음
제4호	이전받는 자의 고시 인증 + 조치	고시 목록이 좁음
제5호	이전대상국의 동등성 인정	개인정보위가 인정한 나라로 갈 때만

별도 동의(제1호)

별도 동의를 받으려면 회사는 제28조의8 제2항이 정한 다섯 사항을 동의 전에 정보주체에게 알려야 합니다. 어떤 정보가 어느 나라로 언제 어떤 방식으로 가는지, 누가 받는지(법인이면 명칭과 연락처), 받는 쪽이 그 정보를 무엇에 얼마 동안 쓰는지, 정보주체가 어떻게 거부할 수 있고 거부하면 어떻게 되는지가 그 내용입니다. 이 사항 가운데 하나라도 달라지면 회사는 새로 알리고 동의를 다시 받아야 합니다(같은 조 제3항). 처리방침에 「국외 이전을 원하지 않으면 탈퇴하라」는 문구만 두고 동의란을 두지 않은 상태는 제1호의 동의를 받은 것으로 보기 어렵다는 것이 SDK 위탁·제공 판정 글의 판단입니다. 가입 화면의 체크박스 하나로도 충분하지 않을 수 있습니다. 개인정보위는 알리익스프레스 사건(2024년 7월 의결)에서 가입 때 「개인정보 해외 이전 동의(필수)」에 체크하게 했을 뿐 정보가 실제로 넘어가는 구매 단계에서 이전 국가 등 법정 사항을 알리고 동의를 받은 사실이 없다고 보고, 법정 사항의 고지 없이 형식적으로 받은 체크는 동의가 아니라고 판단했습니다(영문 해설).

계약 이행을 위한 처리위탁·보관(제3호)

제3호는 두 겹으로 되어 있습니다. 첫째 겹은 그 이전이 「정보주체와의 계약의 체결 및 이행을 위하여」 필요한 처리위탁·보관이어야 한다는 본문 요건입니다. 둘째 겹은 제2항의 다섯 사항을 처리방침에 공개하거나(가목) 정보주체에게 알리는(나목) 절차 요건입니다. 시행령 제29조의7은 나목의 방법을 「서면등의 방법」으로 정합니다. 서면등의 방법은 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법을 가리킵니다(시행령 제17조 제5항).

실무에서 자주 어긋나는 곳은 첫째 겹입니다. 조문이 말하는 계약은 회사가 이용자와 맺은 계약이지, 회사가 클라우드나 SaaS 벤더와 맺은 계약이 아닙니다. 한 회사가 쓰는 여러 해외 도구가 서로 다른 근거로 갈리는 이유가 여기에 있습니다. 주문 대금을 처리하려고 해외 결제대행사에 보내는 흐름은 이용자와의 계약 이행에 가깝습니다. 반면 서비스 개선을 위한 행동 분석은 그 요건을 채우기 어려운 경우가 많아 제1호로 가야 할 수 있습니다. 처리방침 공개는 첫째 겹을 통과한 흐름에서만 의미가 있습니다. 이용자 계약과의 연결이 없는 흐름이라면 처리방침의 국외 이전 표를 빈칸 없이 채워 두어도 제3호의 근거가 되지 못합니다.

인증(제4호)과 동등성 인정(제5호)

제4호는 인증을 받아야 하는 쪽을 이전받는 자로 정하고, 인증의 종류를 보호위원회가 고시한 것으로 한정합니다. 국외 이전 인증 목록 글이 확인한 바로는 「개인정보 국외 이전 운영 등에 관한 규정」(개인정보보호위원회고시 제2023-11호) 별표 2에 올라 있는 인증은 2026년 11월 18일 기준 ISMS-P 하나입니다. 외국 본사가 흔히 내세우는 ISO/IEC 27701, BCR, APEC CBPR은 등재되지 않았습니다.

제5호에서 인정의 주체는 개인정보위이고 인정의 단위는 나라입니다. 회사가 할 일은 데이터를 보내려는 나라가 인정 목록에 들어 있는지 찾아보는 것입니다. 개인정보위는 2025년 9월 16일 EU 27개국과 EEA 3개국의 GDPR 적용 컨트롤러·프로세서에 대해 이 인정을 공고했습니다(개인정보보호위원회공고 제2025-68호). 다만 주민등록번호와 개인신용정보의 이전에는 그 효과가 미치지 않습니다. 영국은 2026년 10월 1일 검토에 착수했다고 발표됐을 뿐 인정된 나라가 아닙니다(영국 이전 글). 미국 서버로 가는 흐름에는 제5호를 쓸 수 없습니다.

장면별로 무엇을 갖춰야 하나?

아래 표는 장면별로 대개 어느 근거를 검토하게 되는지와 자주 빠지는 것을 한 줄로 줄인 것입니다. 성격은 계약과 실제 데이터 흐름으로 판단하므로 표의 「대개」는 출발점일 뿐입니다. 장면별 설명은 표 아래에 이어집니다.

장면	대개 검토하는 근거	자주 빠지는 것
해외 클라우드·호스팅에 보관	제3호	접근 주체, 리전 국가 전부
해외 SaaS(분석·CRM·상담)	제3호 또는 제1호	이용자 계약과의 연결
광고 픽셀·전환 추적 SDK	제1호(+제17조)	위탁 표에 올려 둔 것
서비스에 붙인 생성형 AI API	제3호	입력값 처리 항목, 모델 교체
사내 업무로 해외 AI에 문서 입력	문서별로 다름	계약 당사자가 아닌 사람
국내 수탁사가 해외에 재위탁	위탁자 쪽에서 정리	위탁 표의 국내 회사 이름 뒤
해외 본사·계열사와 공유	흐름별로 다름	계열사 이전도 이전

해외 클라우드·호스팅에 데이터를 보관할 때

회사가 해외 리전의 클라우드나 해외 호스팅 서버에 고객 데이터를 두는 것은 국외 보관이고, 대개 처리위탁·보관으로 정리되어 제3호를 검토하게 됩니다. 처리방침의 국외 이전 항목에는 근거와 제2항의 다섯 사항을 적습니다. 이 사이트의 SDK 위탁·제공 판정 글에 따르면 개인정보위 처리방침 작성지침은 클라우드 이용 등으로 여러 나라에 이전되면 그 나라를 모두 적도록 안내합니다. 계약에는 시행령 제29조의10 제1항의 보호조치(안전성 확보 조치, 고충처리·분쟁해결 조치 등)를 이전받는 자와 미리 협의해 반영합니다(같은 조 제2항). 회사가 자주 놓치는 것은 접근 주체입니다. 데이터를 국내 리전에 두었더라도 해외에서 조회할 수 있는 경로가 있는지 계약서와 서브프로세서 목록으로 확인해 두는 편이 안전합니다.

해외 SaaS를 쓸 때

분석 도구, CRM, 고객상담 도구처럼 우리 계정 안에서 우리를 위해 쓰이는 SaaS는 위탁 쪽에 놓이는 경우가 많습니다. 그러나 위탁으로 정리되더라도 제3호의 첫째 겹이 남습니다. 이용자와의 계약을 이행하는 데 그 도구의 국외 처리가 필요한지를 물어야 하고, 서비스 개선 목적의 행동 분석이라면 제1호의 동의가 필요할 수 있습니다. 회사는 SaaS 사업자의 약관에서 수집 데이터를 자기 제품 개선이나 통계에 쓸 수 있게 한 조항이 있는지도 확인해야 합니다. 그런 조항이 있다면 그 도구는 제공 쪽으로 기울 수 있습니다.

광고 플랫폼의 픽셀과 전환 추적 SDK는 도구 이름만으로 단정할 수는 없지만 제공 쪽에 놓이는 경우가 많습니다. 사업자가 받은 행태정보를 자기 맞춤형 광고에 쓰는 구조라면 제공에 가깝고, 그러면 제3호는 쓸 수 없습니다. 이 경우 회사는 제3자 제공의 근거(제17조, 통상은 동의)와 국외 이전에 관한 별도 동의(제28조의8 제1항 제1호)를 각각 갖추어야 합니다. 제28조의8 제4항이 국외로 이전할 때에도 제17조를 지키도록 정하기 때문입니다. 행태정보가 개인정보인지와 틱톡 사건의 사실관계는 틱톡 픽셀 글에 있습니다.

서비스에 생성형 AI API를 붙일 때

이용자의 질문을 해외 모델 서버로 보내 답을 받아 오는 구조에서는, 질문에 들어 있는 개인정보가 매 호출마다 국경 밖의 사업자에게 넘어갑니다. 처리방침에서는 두 곳이 바뀝니다. 하나는 처리하는 개인정보의 항목(시행령 제31조 제1항 제1호)으로, 이용자

가 입력한 내용과 생성 결과물에 개인정보가 들어 있고 회사가 그것을 수집·저장하거나 국외로 전송한다면 여기에 적습니다. 다른 하나는 국외 이전 항목(같은 항 제2호)으로, 근거와 다섯 사항을 적습니다. 모델을 바꾸면 이전받는 자, 국가, 보유 기간이 함께 바뀌므로 외부 모델 목록을 국외 이전 현황표로 관리하는 방법을 생성형 AI 처리방침 글이 제안합니다. 사업자가 입력값을 학습에 쓰는지도 확인해야 합니다. 학습 미사용이 확인되지 않으면 그 흐름은 위탁이 아니라 제공으로 기울 수 있습니다. 개인정보위는 딥시크 사건(2025년 4월 시정권고)에서 이용자가 프롬프트에 입력한 내용이 중국 소재 클라우드 사업자로 전송된 것을 국외 이전 문제로 다루었습니다.

사내 업무로 해외 AI에 문서를 넣을 때

직원이 업무 문서를 해외 AI에 넣는 장면은 서비스에 API를 붙이는 장면과 따로 보아야 합니다. 문서 속 사람이 회사와 계약한 사람이 아니면 제3호의 「정보주체와의 계약」을 찾기 어렵기 때문입니다. 소송 상대방 회사의 담당자나 거래처 담당자가 그런 예입니다. 사내 AI 입력 글은 계약 당사자가 아닌 사람의 정보에 제3호가 서는지를 직접 다룬 개인정보위 문서를 확인 범위에서 찾지 못했다고 적고, 문서 유형별로 근거를 기록하고 근거가 서지 않는 문서는 입력 대상에서 빼 두는 방법을 권합니다. AI 사업자와 맺은 기업용 계약(DPA)에 그런 조항이 실제로 있더라도 거기서 확인되는 것은 사업자가 입력값을 학습에 쓰지 않는다는 점과 처리자로 행동한다는 점까지이고, 문서 속 사람과 회사 사이의 계약 관계는 그 계약으로 생기지 않습니다.

국내 수탁사가 해외 클라우드에 다시 맡길 때

처리방침의 위탁 표에는 국내 회사만 적혀 있는데 실제 데이터는 해외 서버에 있는 경우가 있습니다. 회사가 상담이나 예약 관리를 맡긴 국내 SaaS 회사가 자기 인프라로 해외 리전 클라우드를 쓰는 경우가 그렇습니다. 국내 수탁사가 해외 클라우드를 쓰는 것은 재위탁입니다. 따라서 수탁사는 먼저 위탁자에게 동의를 받아야 하고(제26조 제6항), 해외 클라우드 사업자는 재수탁자로서 위탁자가 공개해야 하는 수탁자 범위에 들어옵니다(제26조 제2항). 국외 이전의 근거는 정보주체와 계약을 맺은 위탁자 쪽에서 갖추어 두는 편이 안전하다는 것이 SDK 위탁·제공 판정 글의 판단입니다. 다만 그 글도 이 구간을 개인정보위 안내서가 직접 다룬 문장은 찾지 못했다고 밝혔습니다. 수탁사 쪽도 제26조 제8항의 준용으로 국외 이전 조문의 적용을 받으므로(준용 목록에 제28조의7부터 제28조의11까지가 들어 있습니다), 위탁자가 근거를 갖추었다고 해서 수탁사의 의무가 없어지지는 않습니다. 이 구간에서 위탁자가 손댈 수 있는 문서는 위탁계약입니다. 리전 변경이나 해외 재위탁을 사전 통지 사항으로 정해 두면, 위탁자는 실제 이전이 일어나기 전에 처리방침을 고치거나 동의 절차를 준비할 시간을 얻습니다. 약관으로 맺는 수탁 SaaS의 문서 요건은 수탁 SaaS 약관 글에서 다룹니다.

해외 본사·계열사와 데이터를 나눌 때

외국계 한국 법인이 본사 시스템에 고객·임직원 정보를 올리는 흐름은 이 사이트에서 가장 많이 다룬 장면입니다. 요점만 적으면 이렇습니다. 개인정보위의 설명에 따르면 계열사 사이의 이전도 국외 이전입니다. 본사가 그 데이터를 자기 목적으로 쓰면 제공 쪽으로 기울어 제1호를 검토해야 합니다. 본사가 가진 인증은 대개 제4호의 근거가 되지 못하고, 이전받는 본사가 EU·EEA에 있고 GDPR의 적용을 받는다면 제5호를 쓸 수 있습니다(주민등록번호와 개인신용정보는 제외). 근거와 별개로 보호조치를 협의해 계약에 반영해야 하는데 본사 표준 DPA에 서명한 것만으로는 그 요건이 채워졌다고 보기 어렵습니다. 이전한 뒤에도 열람·삭제 같은 정보주체 요구에 답할 의무는 한국 법인에 남습니다.

서비스 자체를 본사로 넘기는 경우는 국외 이전 요건과 영업양도 통지(제27조)를 함께 보아야 한다는 것이 개인정보위 안내서의 입장입니다. 계약 주체만 본사로 바꾸는 경우에도 제27조가 적용된다는 판단과, 양도 시점에 국외 양수자에게 직접 넘기는 이전은 제1호 동의가 필요하다는 판단은 영업양도 통지 글이 필자의 견해로 밝혀 둔 것입니다. 세부는 아래 관련 글의 「해외 본사와 나눌 때」 묶음에 있습니다.

처리방침에는 무엇을 적어야 하나?

처리방침의 국외 이전 항목은 시행령 제31조 제1항 제2호가 정합니다. 회사는 국외 이전의 근거가 제28조의8 제1항 각 호 가운데 무엇인지와 같은 조 제2항 각 호의 사항을 적어야 합니다. 제3호를 근거로 삼으면서 처리방침 공개(가목)를 택한 회사에게는 이 기재가 이전 근거의 요건 그 자체이기도 합니다.

적을 것	근거
이전의 근거(제1호~제5호 중 무엇인지)	시행령 제31조 제1항 제2호
이전되는 개인정보 항목	법 제28조의8 제2항 제1호
이전되는 국가, 시기, 방법	같은 항 제2호
이전받는 자의 성명(법인은 명칭·연락처)	같은 항 제3호
이전받는 자의 이용목적, 보유·이용 기간	같은 항 제4호
이전을 거부하는 방법·절차, 거부의 효과	같은 항 제5호
국외에서 직접 수집·처리하는 경우 처리 국가명	시행령 제31조 제1항 제4호

회사가 근거를 바꾸었으면 처리방침도 함께 고쳐야 합니다. EU 적정성 재검토 글은 처리방침에는 근거를 별도 동의로 적어 두고 실제로는 동의를 받지 않는 상태가 자주 보인다고 적었습니다. 처리방침 전체의 필수 항목과 신설 시점은 처리방침 필수 기재사항 글에, 영문판을 따로 둘 때의 관리 방법은 영문 처리방침 글에 있습니다.

이전한 뒤 계약과 재이전은 어떻게 관리하나?

근거를 갖춘 것으로 국외 이전 작업이 끝나지는 않습니다. 제28조의8 제4항은 다섯 근거 가운데 무엇을 택했든, 국외 이전에 관한 다른 규정과 제17조부터 제19조까지, 그리고 정보주체의 권리를 정한 제5장을 지키고 대통령령의 보호조치를 하라고 정합니다. 시행령 제29조의10은 그 보호조치를 안전성 확보 조치, 고충처리·분쟁해결 조치, 그 밖의 필요한 조치로 정하고, 이전받는 자와 미리 협의해 계약 등에 반영하도록 합니다. 나아가 법 제28조의8 제5항에 따라 회사는 이 법에 어긋나는 내용을 담은 국외 이전 계약에 서명해서는 안 됩니다. 글로벌 DPA 글이 확인한 바로는 고시 제2023-11호에 이 계약의 서식을 정한 조문은 없어서, 계약 문언은 회사가 설계해야 합니다.

이전받은 자가 다시 제3국으로 넘기는 구간에는 제28조의11이 제28조의8과 제28조의9를 준용합니다. 따라서 회사는 해외 벤더의 서브프로세서 조항도 한국 조문에 비추어 보아야 합니다. 수탁자에게도 제26조 제8항이 제28조의7부터 제28조의11까지를 준용하므로, 수탁자로서 데이터를 해외로 보내는 회사도 같은 틀 안에 있습니다.

정보주체의 권리 쪽은 이전한 회사에 남습니다. 본사 서버 데이터 삭제 요구 글은 제28조의8 제4항이 이전한 회사에 제5장 준수를 요구하고 제28조의11의 준용 목록에는 제5장이 없다는 점을 근거로 열람·삭제 요구에 답할 의무가 이전한 한국 법인에 있다고 보고, 열람·정정·삭제·처리정지 요구에 대한 통지 기한이 시행령상 요구를 받은 날부터 10일이라는 점을 정리했습니다.

해외 사업자는 무엇을 따로 보아야 하나?

한국 이용자에게 서비스하는 해외 사업자는 한국 회사와 다른 지점에서 걸립니다. 개인정보위는 외국 본사를 직접 피심인으로 처분해 왔고, 실명이 공개된 처분 가운데 본사 직접 처분이 건, 외국 본사의 한국 법인이 피심인인 건이 건입니다(해외 사업자 제재 표).

해외 사업자가 먼저 확인할 것은 넷입니다.

1. 국내대리인. 국내에 주소나 영업소가 없는 개인정보처리자 가운데 시행령이 정한 매출·이용자 규모 기준이나 조사 계기에 해당하면 국내대리인을 문서로 지정해야 합니다(법 제31조의2 제1항). 한국에 세운 법인이나 지배적 영향력을 행사하는 국내 법인이 있으면 그 법인 중에서 지정해야 하고, 처리방침에 국내대리인의 정보를 적어야 합니다. 기준과 기한은 국내대리인 재지정 글과 영문 해설에 있습니다.
2. 처리 국가명. 해외에서 한국 정보주체의 개인정보를 직접 수집해 처리한다면 처리방침에 처리하는 국가명을 적어야 합니다(시행령 제31조 제1항 제4호).
3. 계열사·수탁사로 넘기는 흐름. 한국 이용자에게서 받은 정보를 같은 나라의 계열사에 맡기더라도 국외 이전 요건을 지켜야 한다는 것이 틱톡 사건에서 개인정보위가 밝힌 판단입니다(틱톡 픽셀 글).

4. 동의 화면과 처리방침의 한국어판. 가입 때의 필수 체크박스가 국외 이전 동의로 인정되지 않은 알리익스프레스 사건과, 한국어 처리방침 공개가 시정권고에 들어간 딥시크 사건이 있습니다.

실제 처분은 어디에서 나왔나?

결정문이 공개된 의결 가운데 제28조의8 위반이 인정된 것은 적어도 건이고, 그중 과징금이 부과된 의결이 건입니다. 아래 표는 그 가운데 유형이 갈리는 사건을 추리고, 보도자료로 확인되는 빗썸 사건을 더한 것입니다(빗썸은 위 건수에 들어 있지 않습니다). 표의 사건들에서 문제 된 것은 해외로 보냈다는 사실 자체가 아니라 동의·공개·통지 같은 근거 요건을 갖추지 못했다는 점이었습니다.

사건	무엇이 문제였나	더 읽을 곳
카카오페이(2025년 1월 의결)	이용자 동의나 국외 이전 고지 없이 알리페이에 정보를 보냄. 위원회는 이 전송을 제3자 제공으로 보고 국외 이전 부분에 제28조의8을 적용	금감원·개인정보위 이중 제재 글
애플(2025년 1월 의결)	국외 수탁자에게 처리를 맡긴 사실을 정보주체에게 알리지 않음	해외 사업자 제재 표
테무(2025년 5월 의결)	처리위탁·보관하면서 처리방침에 법정 사항을 공개하지 않아 제3호 요건을 갖추지 못함	영문 해설
알리익스프레스(2024년 7월 의결)	가입 시 필수 체크박스만 두고 구매 단계에서 법정 사항을 알리지 않아 동의로 인정되지 않음. 판매자와의 약관에 보호조치가 없어 제4항 위반으로 과태료	영문 해설
빗썸(2026년 6월 의결)	동의를 받은 이전처와 실제 이전처가 다름	글로벌 DPA 글
틱톡(2026년 7월 의결)	같은 나라의 계열사에 위탁하면서 법정 사항을 공개하거나 알리지 않음	틱톡 픽셀 글

몇 가지는 따로 읽어야 합니다. 카카오페이는 한국 회사이고, 결정문에 적힌 위반 조문이 제28조의8뿐이었습니다. 다른 위반과 섞이지 않고 국외 이전 조문만으로 금전 제재가 매겨진 셈입니다. 카카오페이가 처분에 불복한 행정소송의 1심은 2026년 6월 위원회의 판단을 유지했고, 항소심(서울고등법원 2026누4926)은 2026년 11월 19일 나의 사건검색 조회 기준으로 기일이 지정되지 않은 채 계속 중입니다. 틱톡 사건에서는 국외 이전 위반이 인정됐지만 위원회가 과징금 부과기준 고시의 면제 사유를 적용해 그 위반에는 과징금을 매기지 않았습니다. 이 면제를 일반 기준으로 읽으면 안 됩니다. 틱톡 픽셀 글에 따르면 위원회는 틱톡이 조사 도중 처리방침을 고친 점, 위탁 상대가 같은 그룹의 같은 나라 법인이었던 점 등을 모아 판단했고, 이 판단을 다른 사건에 쓸 기준으로 내세우지는 않았습니다. 해외 사업자 제재 가운데 국외 이전 조문이 과징금 근거가 된 건은 건입니다.

위반하면 무엇이 걸리고, 중지 명령은 언제 나오나?

제재는 항에 따라 갈립니다. 근거 없이 이전한 것(제28조의8 제1항 위반)은 제64조의2 제1항 제7호의 과징금 사유이고, 그 상한은 전체 매출액의 100분의 3입니다(제64조의2 제1항 본문). 2026년 9월 11일부터는 같은 조 제2항이 정한 경우에 100분의 10까지 올라갑니다(아래 개정 절). 보호조치를 하지 않은 것(제4항 위반)은 제75조 제2항 제14호의 과태료 사유입니다. 위반 계약을 체결한 것(제5항 위반)은 과징금·과태료 조항에 열거되어 있지 않다는 것이 글로벌 DPA 글의 정리입니다. 제28조의8은 제26조 제8항과 제28조의11에 따라 수탁자와 재이전하는 자에게도 준용되고, 과징금 조항과 과태료 조항도 그 준용을 문언에 적어 두었습니다.

금액보다 무거울 수 있는 것이 국외 이전 중지 명령(제28조의9)입니다. 개인정보위는 국외 이전이 계속되고 있거나 추가 이전이 예상되는 경우로서, 회사가 제28조의8 제1항·제4항·제5항을 위반했거나 이전받는 자나 이전대상국이 개인정보를 적정하게 보호하지 않아 정보주체의 피해가 발생하거나 그 우려가 현저하면 이전 중지를 명할 수 있습니다. 시행령 제29조의11은 명령 전에

이전된 정보의 유형과 규모, 위반의 중대성, 피해의 회복 가능성, 중지가 정보주체에게 명백히 더 이익인지 등을 종합해 고려하고 국외이전전문위원회의 평가를 거치도록 합니다. 명령에 이의를 제기할 수 있는 기간은 짧습니다. 이의 제기 기한은 명령을 받은 때부터 7일이고, 위원회의 회신 기한은 이의신청서 접수 뒤 30일입니다(법 제28조의9 제2항, 시행령 제29조의12). 명령을 따르지 않으면 제64조의2 제1항 제8호의 과징금 사유가 됩니다. 이 명령은 데이터 흐름 자체를 멈추게 하므로, 해외 클라우드나 AI API에 서비스가 묶여 있는 회사일수록 영향이 큽니다.

제28조의10은 국외 이전을 제한하는 나라의 개인정보처리자에게 그 나라 수준에 상응하는 제한을 할 수 있게 하는 상호주의 조항입니다. 실무에서 이 조항을 근거로 한 처분은 기존 글에서 확인되지 않았습니다.

2026년 9월 11일 개정으로 바뀐 것이 있나?

국외 이전 조문 자체는 이번 개정의 대상이 아니었습니다. 법률 제21445호가 2026년 9월 11일 시행된 뒤에도 제28조의8·제28조의9·제28조의11은 종전 문언 그대로이고, 개정은 그 주변 조문에서 일어났습니다. 제64조의2 제2항이 신설되어 고의·중과실 반복 위반 등 일정한 경우에 전체 매출액 10%까지의 과징금 구간이 생겼고, 국내대리인의 대리 업무에 유출등의 가능성 단계 통지가 들어왔습니다. 그 밖의 개정 내용은 2026년 개정법 가이드에 있습니다.

2027년 3월 9일 시행되는 AI 학습 특례(법률 제21910호)도 국외 이전과 맞닿아 있습니다. 특례 의결을 받으면 일부 조문의 적용을 배제할 수 있는데, 제28조의8은 「국외로 처리위탁하는 경우」에 한해서만 배제 목록에 들어 있습니다. 국외 제공이나 보관 구조라면 특례와 별도로 이전 근거를 갖추어야 하는 것으로 읽힙니다(AI 학습 특례 가이드).

자주 묻는 질문

Q. 서버가 국내 리전에 있으면 국외 이전이 아닌가요?

그것만으로 판단할 수는 없습니다. 제28조의8 제1항은 국외 제공에 조회되는 경우를 포함시키므로, 해외 본사나 해외 사업자가 데이터에 접근할 수 있다면 국외 이전 여부를 검토해야 합니다(위 국외 이전인가 절).

Q. 처리방침에 국외 이전 항목을 적어 두었으면 동의를 따로 받지 않아도 되나요?

그 흐름이 정보주체와의 계약 이행에 필요한 처리위탁·보관일 때만 그렇습니다. 제공이거나 이용자와의 계약 이행과 연결되지 않는 처리라면 제1호의 별도 동의를 검토해야 합니다(위 근거 절).

Q. 생성형 AI API를 호출하는 것도 국외 이전인가요?

이용자의 입력에 개인정보가 들어갈 수 있고 모델 제공자의 서버가 해외에 있다면 국외 이전으로 보고 처리방침의 처리 항목과 국외 이전 항목을 함께 고쳐야 합니다. 사내 업무용 입력은 문서 속 사람과 회사의 관계에 따라 근거가 달라집니다(위 장면별 절).

Q. 본사가 ISO 27701이나 CBPR 인증을 받았으면 인증 근거로 이전할 수 있나요?

기존 글이 확인한 기준으로는 어렵습니다. 고시 별표 2에 올라 있는 인증은 2026년 11월 18일 기준 ISMS-P 하나이고, 인증은 이전받는 자가 받아야 합니다.

Q. 국외 이전 위반은 과태료로 끝나나요?

근거 없는 이전은 과징금 조항에, 보호조치 미이행은 과태료 조항에 들어 있습니다. 여기에 국외 이전 중지 명령이 따로 있습니다(위 제재 절).

Q. 해외 사업자가 한국 이용자 정보를 같은 나라의 계열사에 맡기면 국외 이전이 아닌가요?

개인정보위는 틱톡 사건에서 그 주장을 받아들이지 않았습니다. 같은 나라 안의 계열사라도 국외 이전 요건을 지켜야 한다고 판단했습니다.

관련 글

우리 회사의 흐름이 국외 이전인지, 어느 근거인지 가를 때

- 처리방침에 SDK를 모두 '위탁'으로 적어 두었습니다 — 광고 픽셀도 같은 칸인가
- 본사는 인증을 받았으니 국외이전 근거가 있다고 합니다 — 한국 고시 목록에 올라 있는 인증은 하나뿐입니다
- EU 고객 데이터를 한국 서버로 그냥 가져와도 되나요? — 적정성 결정 첫 재검토(2026.7.23)가 바꾼 것과 바꾸지 않은 것
- 영국 본사와 데이터를 주고받고 있습니다 — EU와 같은 근거를 쓸 수 있나

생성형 AI를 쓸 때

- 생성형 AI 서비스의 개인정보 처리방침 — 프롬프트 입력값은 어디에 적히나
- ChatGPT에 거래처·상대방 정보가 담긴 문서를 넣어도 되나 — 처리방침에 적어 둔 국외이전 근거가 통하지 않을 수 있는 이유
- 본사가 한국 이용자 데이터로 AI를 학습시키겠다고 합니다 — 새 특례로 적용이 제외되는 조문과 그대로 적용되는 국외이전 규정

처리방침과 수탁 계약을 고칠 때

- 개인정보처리방침 필수 기재사항 — 2026년 기준 15개 항목과 2023년 이후 늘어난 것
- 개인정보처리방침 영어로 만들기 — 번역본이면 되는 경우와 별개의 Privacy Policy가 필요한 경우
- 「수백 개 고객사와 위수탁 계약을 다 맺을 수 없습니다」 — 수탁 SaaS의 약관과 정책 링크로 제26조 문서 요건이 서는가

해외 본사와 나눌 때(외국계 한국 법인)

- 본사가 보내온 글로벌 DPA에 서명했습니다 — 한국법이 계약에 넣으라고 정한 것은 따로 있습니다
- 본사 서버에 있는 데이터를 지워 달라는 요구가 들어왔습니다 — 기한은 10일이고, 의무자는 한국법인입니다
- 본사 프라이버시 정책을 한국 법인에 그대로 옮겼습니다 — 9월 11일 전에 다시 봐야 할 아홉 지점
- M&A에서 고객 개인정보는 두 번 넘어갑니다 — 실사 때는 제17조, 클로징 때는 제27조
- 개인정보보호법 영문본은 어디서 받나 — 현행(법률 제21445호)과 영문본이 반영한 판 구별법

해외 사업자일 때

- 한국에 자회사가 있는데 국내대리인은 로펌입니다 — 재지정 기한은 2026년 4월에 이미 지났습니다
- 해외 사업자는 개인정보위에 어떻게 처분받나 — 실명 공개분 전수

처분과 실사에서 드러날 때

- 웹사이트에 심은 광고 픽셀이 수집하는 행태정보도 개인정보인가 — 틱톡 과징금 103억 원이 확인한 것
- 금감원·금융위 제재를 받았는데 개인정보위도 처분하나요? 같은 사건 두 건이 보여 준 경계
- 실사에서 개인정보를 볼 때 무엇을 요청해야 하나 — 파기 미이행과 국외이전 근거 미비를 찾는 자료
- 투자 실사에서 개인정보로 밸류에이션이 깎이는 세 가지 — 파기·국외이전·과징금 기준연도

English

- Our headquarters is certified. Is that a transfer ground under Korean law? · What does Korean law separately require the transfer contract to contain? · Who has to answer data subject requests for headquarters' servers?

관련 가이드

- 위탁·수탁 개인정보 책임 지도 — 우리는 어느 자리에 있나
- AI 서비스 규제 지도 — AI기본법과 개인정보 보호법이 각각 어디에서 걸리나
- 2026년 개정 개인정보 보호법 — 9월 11일부터 무엇이 달라졌나
- AI 학습 특례 가이드 — 개인정보 보호법 제28조의12~제28조의15, 2027년 3월 9일 시행

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

참고 자료

- 개인정보 보호법(법률 제21445호, 2026. 9. 11. 시행) · 개인정보 보호법 시행령(대통령령 제36671호): 국가법령정보센터. 제26조, 제28조의8부터 제28조의11까지, 제31조의2, 제64조의2, 제75조와 시행령 제29조의7부터 제29조의12까지, 제31조를 인용했습니다
- 개인정보 국외 이전 운영 등에 관한 규정(개인정보보호위원회고시 제2023-11호): 국가법령정보센터(행정규칙)
- 개인정보 보호법 영문본(Personal Information Protection Act): 국가법령정보센터 영문법령. 해외 본사·해외 사업자에게 전달할 때 참고용이며 판 확인이 필요합니다
- 대법원 2017. 4. 7. 선고 2016도13263 판결: 처리위탁과 제3자 제공의 구별

자주 묻는 질문

Q. 서버가 국내 리전에 있으면 국외 이전이 아닌가요?

그것만으로 판단할 수는 없습니다. 개인정보 보호법 제28조의8 제1항은 국외 제공에 「조회되는 경우」를 포함시키므로, 데이터가 국내 리전에 저장되어 있어도 해외 본사나 해외 사업자가 계정 관리·로그 분석 등의 목적으로 그 데이터를 들여다볼 수 있다면 국외 이전 여부를 검토해야 합니다. 계약서와 서브프로세서 목록에서 누가 어디에서 접근하는지를 확인하는 것이 출발점입니다.

Q. 처리방침에 국외 이전 항목을 적어 두었으면 동의를 따로 받지 않아도 되나요?

그 흐름이 정보주체와의 계약 이행에 필요한 처리위탁·보관일 때만 그렇습니다. 제28조의8 제1항 제3호는 처리방침 공개나 통지로 동의를 갈음하게 하지만, 대상을 처리위탁·보관으로 한정하고 정보주체와의 계약 이행에 필요할 것을 요구합니다. 받는 쪽이 데이터를 자기 목적으로 쓰는 제공이거나, 이용자와의 계약 이행과 연결되지 않는 처리라면 제1호의 별도 동의를 검토해야 합니다.

Q. 생성형 AI API를 호출하는 것도 국외 이전인가요?

프롬프트에 개인정보가 들어갈 수 있고 모델 제공자의 서버가 해외에 있다면 국외 이전으로 보는 것이 이 사이트의 기존 글과 개인정보위 안내의 전제입니다. 프롬프트에 담긴 개인정보가 해외 사업자의 시스템에서 처리되기 때문입니다. 서비스에 AI 기능을 붙인 회사라면 처리방침에 입력값을 처리 항목으로 적고, 국외 이전 항목에 근거와 법정 사항을 적어야 합니다. 사내 업무용으로 문서를 넣는 경우에는 문서 속 사람이 회사와 계약한 사람인지에 따라 근거를 세울 수 있는지가 달라집니다.

Q. 본사가 ISO 27701이나 CBPR 인증을 받았으면 인증 근거로 이전할 수 있나요?

기존 글이 확인한 기준으로는 어렵습니다. 제28조의8 제1항 제4호의 인증은 보호위원회가 고시한 목록에 있어야 하고 이전받는 자가 받아야 합니다. 고시 별표 2에 올라 있는 인증은 2026년 11월 18일 확인 기준 ISMS-P 하나입니다. 본사 인증은 안전조치를 입증하는 자료로는 쓸 수 있지만 그 자체가 이전 근거가 되지는 않습니다.

Q. 국외 이전 위반은 과태료로 끝나나요?

근거 없이 이전한 것(제28조의8 제1항 위반)은 과징금 조항(제64조의2 제1항 제7호)에 들어 있습니다. 이전 근거와 별개로 요구되는 보호조치를 하지 않은 것(같은 조 제4항 위반)은 과태료 조항(제75조 제2항 제14호)에 들어 있습니다. 여기에 개인정보위는 국외 이전 중지를 명할 수 있고(제28조의9), 명령을 따르지 않으면 다시 과징금 대상이 됩니다.

Q. 해외 사업자가 한국 이용자 정보를 같은 나라의 계열사에 맡기면 국외 이전이 아닌가요?

개인정보위는 틱톡 사건에서 그 주장을 받아들이지 않았습니다. 위원회는 국외 이전을 물리적 국경 이동이 아니라 한국 보호법의 관할이 미치지 않는 곳으로 정보가 옮겨 가는 것으로 보았고, 해외 사업자가 한국 정보주체에게서 받은 정보를 다른 사업자에게 맡기면 두 회사가 같은 나라에 있어도 국외 이전 요건을 지켜야 한다고 판단했습니다.