분석 · 2026년 5월 18일

← 이전·다음 →

슈렘스 II 판결, 5년 후

개인정보의 국제 전송 법규를 바꾼 판결. 5년이 지난 지금도, 유럽의 일상 업무 중 상당 부분은 아무 일도 없었던 것처럼 운영되고 있다.

규칙을 바꾸는 데 단 3시간이 걸린 판결

2020년 7월 16일, 룩셈부르크 시간으로 오전 10시 15분경, 유럽연합 사법재판소(CJEU)는 사건 C-311/18의 판결문을 공개했습니다. 그 후 3시간 만에 유럽에서 미국으로의 일상적인 개인정보 전송을 뒷받침하던 법적 체계, 즉 프라이버시 쉴드(Privacy Shield, 공식 명칭)는 소멸했습니다. 유럽의 데이터 보호 책임자들이 그날 점심 식사를 마쳤을 때, 기업과 행정 기관이 의존하던 프레임워크는 더 이상 유효하지 않았습니다.

이 판결은 오늘날 페이스북 아일랜드를 상대로 제소한 오스트리아 활동가 맥시밀리언 슈렘스의 이름을 따서 '슈렘스 II'로 알려져 있습니다. 구체적으로는 페이스북 아일랜드와 페이스북 미국 간의 정보 전송에 관한 제소였습니다. 그러나 판결의 영향은 그보다 훨씬 광범위하여, 유럽 영토에서 수집된 모든 개인정보가 어떤 조건 하에 미국으로 전송될 수 있는지를 규정합니다.

거의 6년이 지난 지금, 대체 프레임워크인 'EU-US 데이터 프라이버시 프레임워크'가 2023년 7월에 채택되었지만, 이 또한 법적 압박을 받고 있습니다. 새로운 '슈렘스 라운드'가 준비 중입니다. 한편, 유럽의 중소기업들은 일상 업무에 미국의 클라우드 서비스를 계속 사용하고 있으며, 대부분은 이러한 서비스가 의존하는 법적 근거가 여전히 미결 상태라는 사실을 모르고 있습니다.

슈렘스 II의 정확한 내용

판결은 세 가지 요소에 기반합니다. 첫째는 유럽연합 기본권 헌장, 특히 제7조(사생활 및 가족생활), 제8조(개인정보 보호), 제47조(실효적인 사법적 구제)입니다. 둘째는 일반 데이터 보호 규칙(GDPR)으로, 특히 국제 전송에 관한 제5장(제44조~제50조)입니다. 셋째는 미국의 정보 활동 관련법인 외국정보감시법 제702조(법률 용어로 FISA 702)와 대통령령 12333입니다.

재판소는 대비 방식을 통해 심리를 진행했습니다. 기본권 헌장은 유럽 시민의 개인정보가 연합 외부로 전송될 때 GDPR이 보장하는 것과 '본질적으로 동등한' 수준의 보호를 누릴 것을 요구합니다. 따라서 문제는 미국이 그러한 본질적으로 동등한 수준을 제공하느냐 하는 것이었습니다.

답변은 부정적이었습니다. 이는 단순히 미세한 차이 때문이 아니었습니다. FISA 702는 미국 정부가 개별적인 사법 허가나 대상자 통지 없이, 그리고 유럽과 동등한 실효적인 구제 수단 없이 국외 거주 비미국인의 통신 정보를 수집할 수 있도록 허용합니다. 대통령령 12333은 이러한 권한을 국외에서도 유사하게 확대합니다. 재판소는 유럽 시민이 미국의 법 체계 하에서 헌장이 요구하는 본질적으로 동등한 보호를 받지 못한다고 결론지었습니다. 따라서 동등성은 존재하지 않는 것입니다.

그 직접적인 결과로, 프라이버시 쉴드를 적절한 전송 프레임워크로 승인했던 유럽위원회의 결정 2016/1250은 무효로 선언되었습니다. 해당 프레임워크에만 기반한 모든 정보 전송은 그 즉시 법적 근거를 잃게 되었습니다.

살아남은 것(그리고 그 조건)

슈렘스 II가 모든 수단을 제거한 것은 아닙니다. 표준 계약 조항(SCC, Standard Contractual Clauses)은 살아남았습니다. 이는 유럽위원회가 승인한 모델 계약으로, 유럽의 수출자와 수입국의 수입자가 유럽 표준에 따라 정보를 처리할 것을 약속하며 서명하는 것입니다. 2020년 7월 17일에 서비스 제공업체와 SCC를 체결하고 문제가 해결되었다고 생각하며 만족한 기업들도 있었습니다.

판결문을 자세히 읽으면서 불안감이 시작되었습니다. 재판소는 SCC가 여전히 유효함을 명시했지만, 그 유효성이 '정보 수입자가 실제로 이를 준수할 수 있어야 한다'는 조건에 달려 있음을 강조했습니다. 만약 수입국의 국내법(예: FISA 702에 따른 명령이 유럽 측에 통지 없이 정보를 제출하도록 강제하는 경우)이 조항 준수를 방해한다면, 해당 조항은 실제로 보호 기능을 수행하지 못합니다. 이 경우 재판소는 유럽 수출자가 정보 전송을 중단해야 한다고 명시했습니다.

이로 인해 유럽의 데이터 보호 실무에 새로운 개념인 전송 영향 평가, 즉 TIA(Transfer Impact Assessment)가 도입되었습니다. 유럽 기업이 SCC에 기반하여 미국으로 정보를 전송할 때마다, 적용 법률에 비추어 수취인이 조항을 준수할 수 있는지 공식적으로 평가해야 합니다. 유럽 데이터 보호 이사회(EDPB)는 TIA 실시 방법에 관한 상세 가이드라인을 발표했습니다. 성실하게 실무를 수행하면 대개 같은 결과에 도달합니다. 수입자가 대형 클라우드 기업의 미국 자회사라면, TIA에 대한 솔직한 답변은 '조항이 명시된 대로 준수될 수 없다'는 것입니다.

프라이버시 프레임워크와 계류 중인 슈렘스 III

2023년 7월 10일, 유럽위원회는 새로운 적정성 결정인 2023/1795를 채택했습니다. 이는 폐지된 프라이버시 쉴드를 대체하며 'EU-US 데이터 프라이버시 프레임워크'라는 이름으로 운영됩니다. 미국은 이에 앞서 대통령령 14086을 통해 국내 제도를 수정했습니다. 이를 통해 신호 정보 수집의 범위를 유럽 독자들에게는 익숙하지만 미국의 행정 실무에는 생소한 '필요하고 비례적인' 범위로 제한하고, 데이터 보호 심사 법원(DPRC)이라는 재심사 기관을 창설했습니다. 유럽위원회는 이러한 수정이 본질적으로 동등한 수준을 회복하는 데 충분하다고 판단했습니다.

슈렘스가 설립한 단체 noyb는 2023년 9월 7일 새로운 결정에 대해 제소했습니다. 논점은 예상대로입니다. DPRC는 헌장 제47조가 의미하는 독립적인 법원이 아니라는 점, '필요하고 비례적인'이라는 개념이 유럽의 기준을 기계적으로 번역한 것이 아니라는 점, 그리고 궁극적으로 대통령령에 기반한 보호는 다음 대통령령에 의해 취소될 수 있다는 점입니다. 새로운 결정에 대한 CJEU의 판결(이미 많은 이들이 체념 섞인 어조로 '슈렘스 III'라고

부르는 것)은 향후 수년 내에 나올 것으로 예상됩니다. 결과는 예측할 수 없으나, 논리 구조는 2020년과 매우 유사합니다.

유럽 중소기업이 듣지 못하는 것

CJEU의 대심판정에서 심의가 계속되는 동안에도, 중소 규모의 법률 사무소들은 FISA 702의 대상인 미국 기업이 소유한 유럽 리전의 Microsoft 365를 통해 고객과 계속 연락을 주고받습니다. 개인 병원은 Google Workspace로 일정을 동기화하고, 세무사는 DocuSign으로 서명된 신고서를 보냅니다. 심리학자는 Notion 스프레드시트로 청구 업무를 처리하고, 노동법 전문 변호사는 Dropbox에 사건 기록을 보관합니다. 그리고 거의 모든 이들이 WhatsApp으로 고객을 응대합니다. 서비스 제공업체들에 따르면 이 모든 것은 적정성 결정 2023/1795 하에서 운영 가능합니다. 그러나 슈렘스 III에서 그 결정이 무효가 되는 날, 이 모든 관계는 순식간에 법적 보호가 없는 상태로 남게 됩니다.

이는 수사적인 문제가 아닙니다. 2022년에서 2024년 사이, 여러 유럽 당국은 프라이버시 프레임워크가 발효되기 전임에도 불구하고 CJEU의 논리를 그대로 적용하여, 적절한 전송 수단 없이 Google Analytics를 사용한 컨트롤러에 대해 처분을 내렸습니다. 프랑스 당국인 CNIL이 2022년에 처음으로 기준을 공식화했고, 오스트리아, 이탈리아 등 다른 당국들이 그 뒤를 이었습니다. 유럽 중소기업의 현재 운영 설계상 불비점은 이를 아는 이들에게는 실시간으로 기록되고 있습니다.

요식 행위가 아닌 도구로서의 TIA

유럽 사무소들에서 유통되는 TIA의 상당수는 자세히 살펴보면 형식적인 절차에 불과합니다. 계약 수단을 나열하고, 제공업체의 인증을 열거하며, 기술적 보증을 인용하고 체크박스를 채우는 식입니다. FISA 702 명령이 제공업체에게 정보 제출을 강제할지 여부를 진지하게 묻는 경우는 거의 없습니다. 프라이버시 프레임워크가 가상적으로 수정될 경우 그 전송이 어떻게 될지 묻는 경우는 더 적습니다. GDPR 제5조는 컨트롤러가 준수 여부를 입증할 수 있을 것을 요구합니다. 진지하게 수행되지 않은 TIA는 아무것도 입증하지 못합니다. 그것은 실제로는 반대로 행동하면서 서류상으로만 준수하려는 의지를 보여줄 뿐입니다.

TIA의 정직한 버전은 간단한 질문에서 시작됩니다. '내일 이 제공업체에 이 특정 정보에 대한 FISA 702 명령이 전달되면 어떻게 되는가?' 만약 솔직한 답변이 '우리에게 알리지 않고 정보를 제출해야 한다'라면, 계약 조항은 문제를 해결하지 못합니다. 이 질문이 정말로 중요한 경우에 문제를 해결하는 유일한 방법은 정보를 해당 제공업체의 손에 맡기지 않는 것뿐입니다.

구조적 리스크로서의 정치적 변화

추가적으로, 너무 자극적이지 않게 언급해야 할 정치적 계층이 있습니다. 적정성 결정 2023/1795는 궁극적으로 2022년 10월 바이든 대통령이 서명한 대통령령 14086에 기반하고 있습니다. 대통령령은 현직 대통령이 서명하고, 차기 대통령이 취소, 수정 또는 내용을 무효화할 수 있습니다. 따라서 미국 내 유럽 정보의 보호는 미국 의회가 보장하는 것도, 미국 법 체계가 다른 국내 사항과 동일한 견고함으로 보호하는 것도 아닌 행정적 결정에 의존하고 있습니다. 2025년 1월부터 새로운 정부가 미국을 통치하고 있으며, EO 14086의 실질적 지속성에 대한 질문

은 이제 가설이 아닌 현실적인 과제가 되었습니다. 정부가 이 명령을 철회하거나 완화하기로 결정하는 모든 시나리오는 유럽의 결정을 지탱하는 토대를 무너뜨리게 될 것입니다.

이는 음모론이 아닙니다. 법적 설계를 냉정하게 읽어낸 결과입니다. 대서양 간 데이터 보호 프레임워크는 이미 두 번 무너졌습니다. 2015년의 세이프 하버(슈렘스 I 판결)와 2020년의 프라이버시 쉴드(슈렘스 II)입니다. 세 번째 프레임워크는 이전 두 가지보다 더 취약한 토대 위에 서 있습니다. 오늘날 그 토대에 데이터 처리를 걸고 있는 유럽 기업은 단순한 법규 준수가 아닌 리스크 관리 차원의 결정을 내리고 있는 것입니다.

전문가 독자를 위하여

전문적인 정보를 위해 클라우드 서비스를 선택하기 전에 스스로에게 던져야 할 운영상의 질문(데이터 보호 조사관이 제기할 법한 엄격한 질문)은 다음과 같습니다.

1. 데이터가 물리적으로 어디에 저장됩니까? 운영자가 미국 기업이라면 유럽 리전에 저장된다는 사실만으로는 충분한 답변이 되지 않습니다.
2. 누가 서비스를 운영하며, 어느 관할권에 법인이 설립되어 있고, 어떤 법적 명령을 받을 수 있습니까?
3. 어떤 전송 수단이 사용됩니까: 2023/1795 적정성 결정, TIA를 포함한 SCC, GDPR 제49조의 예외 규정? 이러한 선택은 실사 과정에서 방어 가능합니까?
4. 적정성 결정이 내일 무효가 된다면, 비즈니스를 유지하기 위한 어떤 운영 계획이 있습니까?
5. 해당 기능을 대체할 유럽산 또는 셀프 호스팅 대안이 있습니까? 또한 이전 시 실제 비용은 어느 정도입니까?

일상 업무의 모든 기능이 동일한 답변을 요구하는 것은 아닙니다. 내부 회계용 스프레드시트라면 아마도 이 정도 수준의 질문은 필요하지 않을 것입니다. 하지만 고객의 형사 사건 기록, 진료 기록, 직원의 급여 명세서 등은 다릅니다. 비례성은 정당하지만, 유럽의 중소기업들이 가장 민감한 정보에 이르기까지 모든 것을 미국 제공업체에 의존해 온 집단적 관성은 정당하다고 보기 어렵습니다.

슈렘스 II 판결이 이번 7월로 6주년을 맞이합니다. 이 판결이 대부분의 유럽 기업의 일상적인 습관을 바꾸지는 못했습니다. 하지만 기업들이 노출된 리스크 지도는 분명히 바꾸어 놓았습니다. 미국의 행정적 결정이 유럽의 규정과 중소기업의 실제 운영 사이에 끼어들 때, 최소한 그 결정이 존재하며 취약하다는 사실을 알아야 합니다. Cuadernos Lacre(봉인 노트)를 관통하는 핵심인 '중개자 없는 아키텍처'를 선택한 우리는, 슈렘스가 이의를 제기할 때마다 이런 분석을 쓰지 않아도 되기를 바랍니다. 그러나 우리는 앞으로도 계속 써 내려갈 것입니다.

참고 문헌 및 관련 자료

- 유럽연합 사법재판소 — 2020년 7월 16일 판결, 사건 C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems.*
- 규정 (UE) 2016/679 제5장, 제44조~제50조 — 개인정보의 국제 전송.
- 위원회의 시행 결정 (UE) 2023/1795 (2023년 7월 10일), EU-US 데이터 프라이버시 프레임워크에 따른 개인정보의 적절한 보호 수준에 관하여.

- 유럽 데이터 보호 이사회 — *유럽연합의 개인정보 보호 수준 준수를 보장하기 위한 전송 수단 보완 조치에 관한 권고 01/2020* (2021년 6월 18일 채택).
- noyb.eu — 유럽 데이터 보호 당국에 결정 (UE) 2023/1795에 반하여 2023년 9월 7일 제출된 제소 건.
- *외국정보감시법 (Foreign Intelligence Surveillance Act)* 제702조 (50 U.S.C. § 1881a에 법전화됨) 및 국외에서의 미국 정보 활동에 관한 대통령령 12333.

← 이전중간에 아무도 없을 때다음 →CUADERNOS_LIST_SHA256_TITLE

최근 읽은 글

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

이 기사를 다운로드하여 필요한 곳에서 활용하십시오.

↓ 마크다운 ↓ 텍스트 형식 ↓ PDF

파일이 기기에 다운로드됩니다. 해당 위치에서 저장하거나 Solo2로 가져오거나 원하는 곳에 공유할 수 있습니다. Cuadernos는 전송 대상을 결정하지 않습니다.

봉인 · SHA-256 fc263cb8fb5d42a61c41ea845047d28842a578fe96ddf3dc1968cccaa52527b2

Cuadernos Lacre · Menzuri Gestión S.L.의 간행물 ·
저자: R.Eugenio · Solo2 팀 편집