분석 · 2026년 5월 16일

← 이전·다음 →

GDPR과 비즈니스 메시징: 왜 대부분의 조직이 모르는 사이에 규정을 위반하는가

거의 모든 법률 사무소, 병원 또는 컨설팅 회사가 유럽 경제 지역(EEA) 외부의 서버를 사용하는 앱을 통해 고객의 서류를 전송하고 있습니다. 악의는 없으나 대부분의 경우 누구에게도 경고받지 못한 채 규정을 위반하고 있습니다.

생각보다 훨씬 멀리 여행하는 서류

일상적인 풍경: 세무사가 메시징 앱으로 고객 데이터가 포함된 서류를 받습니다. 영업 담당자가 채팅으로 동료에게 견적서를 전달합니다. 의사가 같은 방법으로 임상 보고서를 동료와 공유합니다. 아무도 두 번 생각하지 않습니다. 그것이 평범하고 편리하기 때문입니다. 유럽의 모든 도시, 모든 사무실에서 매일같이 행해지는 일입니다.

하지만 이 서류는 대부분의 경우 방금 미국 서버로 여행을 떠났습니다. 일시적이든 '저장 시 암호화'든 전문가도 고객도 관리하지 않는 클라우드에 저장되었습니다. 내용과 관련된 메타데이터를 기술적으로 인덱싱할 수 있는 시스템을 통과한 것입니다. 그리고 유럽 일반 데이터 보호 규칙은 이 점에 대해 매우 명확한 견해를 가지고 있습니다.

규범이 요구하는 것

GDPR 및 그에 수반되는 유럽 연합 사법 재판소의 판례(특히 2020년 Schrems II 판결, C-311/18)는 유럽 시민의 개인 데이터가 적절히 보호되어야 한다고 규정합니다. 만약 데이터가 EEA를 떠날 경우, 데이터 컨트롤러는 수신 측이 유럽과 '본질적으로 동등한' 보호 수준을 제공함을 보장해야 합니다. 실무상 영향 평가를 수행하지 않고 보완적인 보장(표준 계약 조항, 검증 가능한 암호화와 같은 추가 기술적 조치 등)을 구현하지 않은 채 서버가 미국 사법 관할 하에 있는 서비스를 통해 고객 데이터를 전송하는 것은 규정 위반이 될 수 있습니다. 설령 지금까지 아무도 아무 말도 하지 않았더라도 말입니다.

그리고 문제는 메시지 내용만이 아닙니다. 메타데이터(누가 누구에게 무엇을 언제 얼마나 자주 어디서 보냈는지) 또한 규정에 따라, 그리고 유럽 데이터 보호 이사회(EDPB)의 거듭된 해석에 따라 개인 데이터에 해당합니다. 사용자의 업무 통신에서 메타데이터를 수집하는 서비스는 그 사용자의 고객의 개인 데이터를 그들이 모르는 사이에, 또한 그러한 처리에 동의하지 않은 채 처리하고 있는 것입니다.

“앱은 글을 쓰기 위해서만 사용한다. 앱은 내 고객 데이터의 제공자가 아니다”라는 일반적인 사고 패턴은 법적으로 오류입니다. 고객의 데이터가 제3자의 인프라를 통과하는 경우, 그 제3자는 데이터를 처리하고 있는 셈입니다. 그리고 처리를 수행하는 이상 법적 근거, 데이터 처리 계약 및 적절한 보장이 존재해야 합니다.

누구에게 책임이 있는가

법적 책임을 누가 지는가라는 질문은 학술적인 것이 아닙니다. GDPR은 *데이터 컨트롤러*(어떤 데이터를 어떤 목적으로 처리할지 결정하는 자)와 *데이터 프로세서*(컨트롤러를 대신해 실질적으로 처리를 수행하는 자)를 구분합니다. 고객의 서류를 전송하는 전문가는 데이터 컨트롤러입니다. 메시징 앱 제공업체는 대부분의 경우 실질적인 데이터 프로세서입니다. 처리 계약을 체결하지 않고, 또한 그러한 계약에 포함되어야 할 조항의 상당 부분을 결여한 상태에서는 컨트롤러가 의무를 다한 것이 아닙니다.

선의의 해석으로는 “대부분의 전문가는 이를 모른다”가 됩니다. 엄격한 해석으로는 “법의 부지는 면책되지 않는다”가 됩니다. 그리고 이 건에 대해 자문을 받은 데이터 보호 전문 변호사의 해석은 대개 후자의 엄격한 것입니다.

구체적으로 누구에게 중요한가

간혹이더라도 제3자의 개인 정보를 취급하는 모든 전문가나 기업에 중요합니다.

- 고객의 서류(계약서, 소장, 신고서, 자산 보고서)를 받는 변호사.
- 건강 데이터를 공유하는 의사나 의료 종사자. 이들은 GDPR 제9조에 따라 강화된 보호 체계가 필요한 *특별 범주*로 간주됩니다.
- 식별 정보, 세무, 은행 데이터를 다루는 세무사나 행정사.
- 직원의 취업·개인 서류를 관리하는 인사 부서.
- 잠재 고객이나 기존 고객으로부터 연락처나 기밀성 높은 비즈니스 정보를 받는 영업 담당자.

어떤 경우든 정보는 GDPR에 의해 보호됩니다. 어떤 경우든 일반적인 관행에서 이러한 정보는 추가적인 보장 없이는 유럽의 틀과 '본질적으로 동등함'을 선언할 수 없는 관할권의 채널을 통해 흐르고 있습니다. 악의에서가 아니라 관습 때문입니다. 그리고 15년 동안 컴플라이언스보다 편의성을 우선시해 온 기술 인프라의 결과입니다.

“모두가 하고 있다”는 논리

가장 일반적인 반론을 예상해 두어야 할 것입니다. “만약 모두가 하고 있다면 진짜 문제일 리가 없다”는 것입니다. 이는 완전히 이해할 수 있는 주장이지만 법적으로는 아무런 효력이 없습니다. 어떤 관행이 널리 퍼져 있다는 사실이 그것을 규정에 준수하도록 만드는 것은 아닙니다. 데이터 보호 당국은 최근 몇 년간 검사 순간까지 무해해 보였던 메시징 사용 형태에 대해 정확히 몇몇 기업을 처벌하고 있습니다.

현재의 운영 현실은 발생 확률이라는 점에서는 리스크가 낮지만(당국의 검사가 중소 규모 사무소의 특정 메시징 도구를 감사하는 일은 매우 드뭅니다), 현실화되었을 때의 영향이라는 점에서는 높다는 것입니다. 그것은 대부분

의 사람이 리스크를 무릅쓰고 있다는 사실을 모른 채 무릅쓰고 있는 리스크입니다. 즉, 사용 중인 도구가 데이터 컨트롤러의 법적 책임과 정합하는지 여부를 평가하지 않는 것입니다.

디지털 발자국은 소급적이다

앞서 언급한 것과 거의 대칭적인 두 번째 논리가 있으며, 이 또한 예상해 둘 가치가 있습니다. “만약 이것이 심각한 문제라면 행정 당국은 이미 감시를 시작했을 것이다”라는 것입니다. 현재 관찰되는 현실은 표면적으로는 이를 긍정합니다. 중소기업, 특히 개인 사업자의 부적절한 메시징 이용에 대한 검사는 오늘날 거의 존재하지 않습니다. 그것은 그 행위가 허용되기 때문이 아니라, 한국이나 EU 대부분의 행정 당국에서 수백만의 대상자를 감사하는 데 필요한 인적 자원이 부족하기 때문입니다.

이것이 오늘날 관찰되는 관행이 시사하는 바입니다. 하지만 다음 10년이 시사하는 바는 다릅니다. 두 가지 요인이 수렴하여 비교적 단기간에 균형을 변화시키려 하고 있습니다.

첫째, 디지털 발자국은 소급적(과거로 거슬러 올라감)입니다. 중앙 서버를 가진 앱을 통해 전송된 모든 메시지는 최소한 메타데이터 상에서는 존속하는 인프라에 기록된 채로 남습니다. 6개월 전에 전송된 것은 기술적으로 오늘날에도 감사 가능합니다. 오늘 전송되는 것은 5년 후에도 감사 가능할 것입니다. 현재의 검사 부재가 미래의 검사 부재를 보장하는 것은 아닙니다. 그것은 평가의 연기일 뿐이며 면제가 아닌 것입니다.

둘째, 행정 당국의 감사 능력은 가속적으로 향상됩니다. 감시 프로세스에 인공지능(AI) 도구의 도입은 지금까지 중소기업이나 개인 사업자를 (법적이 아니라 사실상) 보호해 온 인적 병목 현상을 해소합니다. 방대한 메타데이터, 납세 신고서, 상업 등기 및 보안 침해 통지 의무를 크로스 체크할 수 있는 시스템에 검사관은 필요하지 않습니다. 필요한 것은 접근 권한입니다. 그리고 현재의 규범적 틀 안에서 EU 내에 법적 거점을 가진 프로바이더에 대한 요청을 통한 접근은 완전히 실행 가능합니다.

여기에 기술적인 것은 아니지만 똑같이 결정적인 요인이 추가됩니다. 유럽 국가들은 끊임없는 채무 증대 과정에 있으며, 거의 예외 없이 과세 베이스를 확대할 필요가 있습니다. GDPR 불이행에서 비롯되는 행정 처분은 순수하게 재정적인 관점에서 보면 성장하고 있으며 동시에 정치적으로 편리한 수익원입니다. 이는 추측이 아닙니다. 유럽 데이터 보호 당국의 연례 보고서에서 제재금 총액이 수 회계연도 연속으로 증가하고 있다는 관찰 가능한 경향입니다.

데이터 컨트롤러에게 운영상의 결론은 선동적인 것이 아니라 냉철한 것입니다. **오늘날 고객과의 통신을 어떻게 관리할 것인가라는 결정은 현재의 검사 능력이 아니라 실제로 검사가 이루어지는 해의 능력에 비추어 평가됩니다.** 그리고 그 능력은 타당한 기간 내에 오늘과는 근본적으로 다른 것이 될 것입니다. 오늘부터 사안을 올바르게 처리하기 시작하는 사람은 오늘 이후가 건전할 뿐만 아니라, 이 순간부터 생성되는 발자국이 규범에 준거한 것이 되며 그것이 소급적으로 다가올 기간을 보호하게 됩니다. 지금까지처럼 계속하는 사람은 미래의 기준과 리소스로 적합성이 평가될, 감사가 가능한 부정적인 유산을 계속 축적하게 되는 것입니다.

다른 아키텍처로 무엇이 바뀌는가

데이터가 제3자의 인프라에 저장되지 않고 송신자의 기기에서 수신자의 기기로 직접 이동하는 기술적인 대안이 존재합니다. 이 아키텍처에서는 국제 이전과 관련된 GDPR 준수는 표준 계약 조항에도, 프로바이더의 선의에도,

미래의 감사에도 의존하지 않습니다. 그것은 *'이전이 존재하지 않는다'*는 사실에 의존합니다. 존재하지 않는 것을 위반할 수는 없기 때문입니다.

이것은 유일한 해결책도, 유일하게 가능한 방법도 아닙니다. 하지만 구조적으로 다르며 규범 준수는 절차상의 부수물이 아니라 설계의 직접적인 결과가 됩니다. 데이터 컨트롤러로서의 책임을 진지하게 받아들이는 전문가에게 그 차이는 큰 의미를 갖습니다.

다음 회 Cuadernos에서는 Schrems II 판결과 미국 클라우드 서비스에 의존하는 중소기업에 미치는 실무적인 영향에 대해 공개 후 5년이 경과한 시점에서의 상세한 분석을 수행합니다.

참고 문헌 및 법적 틀

- GDPR(EU 규정 2016/679), 특히 국제 이전에 관한 제5장.
- 유럽 사법 재판소 C-311/18("Schrems II"), 2020년 7월 16일.
- EDPB – 이전 도구를 보완하는 조치에 관한 권고 01/2020.
- 각국 데이터 보호 당국 – 전문적인 환경에서 인스턴트 메시지의 부적절한 사용으로 인한 제재 사례를 포함한 연례 보고서.

← 이전디지털 시대의 비밀 유지 의무다음 →중간에 아무도 없을 때

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 1b03f0493ea0bf9270a4416b3f34b67a4231a769b11b62675e7ae8d652371576

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