고찰 · 2026년 5월 16일

← 이전·다음 →

디지털 시대의 비밀 유지 의무

전문가와 고객의 통신이 기술적으로 부적절한 채널에서 이루어질 경우, 비밀은 정보 유출의 날에 깨지는 것이 아닙니다. 도구를 선택한 그 순간에 이미 깨진 것입니다.

거의 아무도 보지 못하는 문제

변호사가 고객으로부터 기밀 서류를 스마트폰으로 받습니다. 의사가 동료와 민감한 진단에 대해 상담합니다. 심리상담사가 정신과 의사와 환자의 치료 방침을 조정합니다. 세무사가 감사를 기다리는 신고 데이터를 전송합니다. 이 모든 일들이 인스턴트 메시지로 이루어지고 있지만, 그 메시지들이 실제로 어디에 도달하는지 멈춰서 생각하는 사람은 거의 없습니다.

답은 대부분의 경우 동일합니다. 전문가가 관리하지 않는 서버, 반드시 숙지하지 못한 법률이 적용되는 국가, 그리고 직접적인 경제적 의미에서 '데이터를 축적하는 것'을 비즈니스 모델로 하는 기업의 관리 하에 있습니다. 메시지는 전송 중에 암호화되어 있을 수 있지만, 서버에 도달한 시점에서 그것은 제3자의 인프라에 저장된 복사본이 되며 그 제3자의 운영, 법률, 상업적 결정에 맡겨지게 됩니다. 전문가의 결정이 아닙니다.

법규가 요구하는 것

유럽 일반 데이터 보호 규칙(GDPR) 제32조는 명확합니다. 개인 데이터를 처리하는 자는 리스크에 걸맞은 보안 수준을 보장하기 위해 '적절한' 기술적 및 조직적 조치를 취해야 합니다. 조치의 적절성은 '앱이 무엇을 한다고 자처하는가'가 아니라 실제 리스크에 비추어 측정됩니다. 만약 고객 데이터가 유럽 경제 지역과 동등한 보호 수준을 보장하지 않는 관할권의 서버에 도달할 경우, 데이터 컨트롤러(즉, 전문가)는 아마도 본인조차 충분히 인식하지 못한 리스크를 지게 됩니다.

그리고 이것은 GDPR만의 문제가 아닙니다. 변호사, 의사, 심리상담사, 감사인, 저널리스트 등을 위해 특별히 규정되어 있는 비밀 유지 의무는 고객과의 통신이 기밀일 것을 요구합니다. '가능한 한 기밀일 것'이 아니라 무조건적인 기밀입니다. 사용되는 기술적 채널이 이를 보장할 수 없다면, 전문가는 직무 윤리가 허용하지 않는 리스크를 무릅쓰고 있는 셈입니다.

역설은 그 리스크가 불가시적이라는 점입니다. 사무실의 메시징을 감사하는 사람은 없습니다. 채팅 제공자에게 데이터 처리 계약을 요구하는 사람도 없습니다. 리스크가 표면화되는 것은 항상 너무 늦은 뒤입니다. 유출, 공개된 취약점, 혹은 사용자에게 통지되지 않은 채 타 대륙에서 집행된 법원의 명령. 이것들이 일어나고 나서야 리스크는 현실이 됩니다.

전문가가 기술적으로 필요로 하는 것

비밀 유지 의무를 지는 인물이 필요로 하는 것은 요구 사항의 관점에서 보면 사실 놀라울 정도로 간단합니다.

- 메시지가 복사본을 저장하는 중간 서버를 거치지 않고 송신자의 기기에서 수신자의 기기로 직접 전달되는 채널.
- 법적 관할권과 정책이 홍보 문구가 아니라 설계(by design)를 통해 GDPR과 정합하는 인프라스트럭처.
- 업무용 연락처(고객명, 전화번호, 연락처 목록)를 제3자에게 넘기지 않고 대화 상대와 본인 확인을 수행하는 방법.
- 제공자의 말에 의존하지 않고 메시지가 정확한 상대에게 전달되었음을 확인할 수 있는 검증 가능한 시스템.

이것들은 과도한 요구가 아닙니다. 실은 디지털화 이전의 전문적인 통신에서는 당연한 것으로 여겨졌던 것들입니다. 등기 우편은 이 모든 기준을 충족했습니다. 사무실 전화 교환기에서 고객의 교환기로의 통화도 마찬가지입니다. 기묘한 점은 오늘날 이러한 보장이 요구된다는 사실이 아니라, 디지털 채널로의 이행 과정에서 아무도 눈치채지 못한 채 이것들이 소실되어 버렸다는 점입니다.

‘암호화하는 것’과 ‘저장하지 않는 것’의 차이

유용한 비유가 있습니다. 메시지를 암호화하여 서버에 저장하는 것은 서류를 금고에 넣고 그 금고를 낯선 사람의 집에 두는 것과 같습니다. 금고는 튼튼합니다. 서류는 원칙적으로 읽을 수 없습니다. 하지만 서류는 *여전히 타인의 집 안에 있습니다*. 그리고 그 타인은 법원의 명령을 받거나 사이버 공격을 당하거나 서비스 약관을 변경하거나 다른 윤리관을 가진 다른 회사에 인수되거나 혹은 내일 사라질 수도 있는 것입니다.

절차적이지도 신뢰 기반도 아닌 구조적인 대안은 서류를 사무실 밖으로 한 걸음도 내보내지 않는 것입니다. 전문가의 책상에서 고객의 책상으로 어떠한 중개자도 거치지 않고 직접 이동시키는 것입니다. 기기 간의 포인트 투 포인트 통신이 기술적으로 수행하는 것이 바로 이것, 즉 중개자의 배제입니다. 중개자가 악하다는 뜻이 아닙니다. 다만 비밀 유지 의무라는 맥락에서 중개자는 *불필요*할 뿐입니다. 그리고 안전하기를 원하는 모든 시스템에서 불필요한 것은 원칙적으로 배제되어야 합니다.

책임의 문제

결국 비밀 유지 의무가 있는 모든 전문가가 단호하게 '예'라고 답할 수 있어야 하는 질문은 다음과 같습니다.

> 만약 내일 고객과의 대화가 유출되어 법원이나 직능 단체로부터 기밀 유지를 어떻게 관리하고 있는지 질문을 받았을 때, 내가 사용한 채널이 제3자의 인프라에 복사본을 저장하지 않는다는 것을 기술적으로 증명할 수 있는가? 대화에 참여한 두 사람의 기기에서 데이터가 한 걸음도 밖으로 나가지 않았음을 증명할 수 있는가? 타 대륙에 있는 기업의 말에 의존하지 않고 기밀성이 '약속'이 아니라 '아키텍처'에 의해 보장되었음을 증명할 수 있는가?

만약 대답이 아니오라면, 문제는 구체적인 도구 그 자체가 아닙니다. 문제는 도구가 지원하도록 설계되지 않았던 책임을 도구에 맡겨버린 데 있습니다. 그것은 기밀 파일을 투명한 봉투에 넣고 우체부가 안을 보지 않을 것이라

고 믿는 것과 같습니다.

전문가가 고객과의 통신에 선택하는 도구는 그 인물이 고객의 신뢰를 얼마나 소중히 여기는지를 말해줍니다. 그 신뢰가 약속이 아니라 아키텍처에 의존하도록 설계된 도구가 존재합니다. 그리고 그렇지 않은 도구도 존재합니다. 그 차이를 아는 것은 업무의 일부입니다.

인용된 법적 틀

- GDPR(EU 규정 2016/679), 특히 제5조, 제25조(설계에 의한 데이터 보호), 제32조(처리의 안전성).
- 비밀 유지 의무에 관한 국내법(변호사법, 의료법, 공인회계사법, 개인정보 보호법 등).
- 형법 등에서의 업무상 과실치사상죄 및 비밀 누설죄 관련 규정.
- 기밀 유지 및 직업상의 비밀에 관한 전문직 단체의 윤리 강령.

← 이전암호화가 곧 프라이버시는 아니다: 메타데이터가 말해주는 진실다음 →GDPR과 비즈니스 메시징: 왜 대부분의 조직이 모르는 사이에 규정을 위반하는가

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 2244b9641fb6e387487736d4a81f9c702beb89fe84a096f1455a2245afb90ba1

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