분석 · 2026년 5월 26일

← 이전 · 다음 →

실제 프라이버시 대 겉보기 프라이버시: 스스로에게 던져야 할 질문들

두 번째 사이클의 실무적 종합: 아키텍처적 프라이버시를 갖춘 서비스와 선언적 프라이버시에 그치는 서비스를 구별해 주는 질문들. 민감한 데이터에 어떤 디지털 도구든 도입하기 전에 유럽의 전문가를 위한 질문지.

요컨대: 같은 법적 고지를 내건 두 서비스가 매우 다르게 행동할 수 있다. 하나는 기술적 설계로 보호한다. 다른 하나는 계약상의 약속으로 보호한다. 그 차이는 고지를 읽어서는 알 수 없다——구체적인 질문을 던짐으로써 드러난다. 답의 질은 그 내용 자체만큼이나 제품에 대해 말해 준다.

아키텍처적 프라이버시와 선언적 프라이버시의 차이

이 사이클의 앞선 일곱 편의 글을 통해 우리는 같은 사안의 서로 다른 층들을 거쳐 왔다. Schrems II와 함께한 국제 이전의 법. 각 Cuaderno를 봉인하는 암호학적 해시라는 수학적 발상. kill switch라는 아키텍처상의 선택과 거의 언제나 그것에 동반되는 제도적 포획. 종단 간 암호화의 메커니즘과 키가 어디에 있는가라는 실무적 질문. 비즈니스 모델에 따른 유인의 정렬. 자기주권적 암호학적 정체성. 비례적 전략으로서의 셀프 호스팅. 각 글은 하나의 각도를 다루었다. 사이클의 마지막인 이 글은 그것들을 하나의 질문지로 모은다.

기억해 둘 만한 구별은 단순하다. 프라이버시가 *아키텍처적*인 서비스가 있고, 프라이버시가 *선언적*인 서비스가 있다. 전자는 기술적 설계에 박혀 있다. 프라이버시 약속에 대한 일정한 위반은 아키텍처가 그것을 허용하지 않기 때문에 기술적으로 어렵거나 불가능하다. 후자는 법적 고지의 문구에 맡겨져 있다. 일정한 위반은 일어난다면 계약상 제재의 대상이 될 수 있으나, 기술적으로는 아무것도 그것을 막지 못한다. 두 모델은 모두 GDPR을 충족할 수 있다. 그러나 하나는 구축에 의해 보호하고 다른 하나는 약속에 의해 보호하며, 그 차이는 실무적으로 막대하다.

이어지는 질문들은 한 경우를 다른 경우로부터 구별하기 위해 설계되었다. 이것들은 고도의 기술적 질문이 아니다. 정직한 제공자라면 누구나 자신의 공개 문서에서 답할 수 있는 질문이다. 답의 질과 정밀함은 답 자체만큼이나 그 제품에 대해 말해 준다. 질문들은 여섯 개의 층으로 묶여 있다. 민감한 데이터를 위해 서비스를 도입하기 전에, 첫 직감이 짚어내는 것만이 아니라 모두를 던져 보는 것이 좋다.

1층: 아키텍처

계속하기 전에 한 가지 용어를 정해 두자. 여기서 *operador*란 서비스를 제공하는 회사를 말한다——서버와 소프트웨어를 통제하는 주체이지 특정 개인이 아니다. 이 점을 분명히 하면, 근본적인 아키텍처상의 질문은 이렇다. operador는 발신자와 수신자 사이의 콘텐츠로 무엇을 하는가? 가능한 답은 세 가지이며 이를 구별할 줄 아는 것이 중요하다. 세 가지 모두 때때로 비슷한 어휘로 광고되기 때문이다.

- 첫째: 콘텐츠가 operador의 서버를 평문으로 거치며, 거기서 operador는 그러지 않겠다고 약속하더라도 그것을 읽을 수 있다.
- 둘째: 콘텐츠가 operador의 서버를 암호화되어 거치며, 키가 사용자의 기기에만 존재한다면 operador는 그것을 읽을 수 없다.
- 셋째: 콘텐츠가 operador의 어떤 서버도 거치지 않는다. 그 구체적인 흐름에는 operador의 서버가 존재하지 않기 때문이다.

이 세 가지 사이의 차이는 정도의 차이가 아니라 종류의 차이다.

보완 질문은——암호화에 관한 Cuaderno에서 이미 던진 것이지만——이러하다. 콘텐츠를 읽을 수 있게 하는 암호 키를 가진 것은 누구인가? 사용자가, 그리고 사용자만이 그것을 가졌다면 암호화는 진짜다. operador가 그에 더하여——「계정 복구」나 「기기 간 동기화」라는 이름 아래에서라도——어떤 형태로든 그것을 가졌다면 암호화는 명목뿐이다. 이 질문은 중간의 정직한 답을 허용하지 않는다.

2층: 비즈니스 모델

비즈니스 모델에 관한 질문은 아키텍처 질문만큼이나 중요하며, 같은 실질적 이유에서다. 유인은 선언된 목적이 똑같더라도 시간이 흐르면서 체계적으로 다른 제품을 만들어 낸다. operador는 오늘 어떻게 돈을 버는가? 단일 출처인가, 둘인가, 혼합인가? 자금 조달에 광고나 데이터 수익화가 포함된다면, 어떤 데이터가 수익화되며 GDPR의 어떤 법적 근거 위에서 그것이 이루어지는가? 법적 고지에 선언된 목적이 전문가가 서비스에 맡기려는 제3자의 데이터까지 포괄하는가?

그리고 항상 던져지지는 않는 2차적 질문. operador의 3~5년 후 재무 상황은 어떠한가? 벤처 캐피털 단계에 있는 회사는 안정적 수익에 있는 회사와는 다른 압력 아래에서 움직인다. 자금 조달 모델의 변경은, 거듭, 사용자와의 암묵적 계약이 협상 없이 다시 쓰이는 순간이다.

3층: 관할권

유럽의 전문가에게 관할권의 질문은 수사가 아니다. operador는 어느 관할권에 설립되어 있는가? 데이터를 처리하는 서버는 물리적으로 어느 나라에 있는가? 앞선 두 질문에 대한 답은 같은가 다른가, 다르다면 어느 법률이 적용되는가? 미국 기업이 운영하는 유럽 리전은 Schrems II의 관점에서 유럽의 답이 아니다. 서버가 어디에 있든 그 기업은 FISA 702에 종속된다.

실무적인 보완 질문은 이러하다. 내일 operador의 관할권에서 유효한 정보기관 명령이 내 데이터나 내 고객의 데이터의 인도를 요구하며 도착한다면 무슨 일이 일어나는가? 정직한 답이 「회사는 그것을 인도할 의무가 있을 것이다」로 시작한다면, 광고가 아무리 반대를 시사하더라도 그 서비스는 그 명령으로부터 보호하지 못한

다. 정직한 답이 「회사는 그것을 평문으로 갖고 있지 않으므로 인도할 수 없을 것이다」로 시작한다면, 그 서비스는 보호한다. 그리고 그 차이는 프라이버시 정책의 질이 아니라 거의 전적으로 처음 두 층에 달려 있다.

4층: operador와 kill switch

operador는 서비스를 원격으로 정지, 차단, 삭제, 또는 저하시키기 위한 어떤 기술적 능력을 보유하고 있는가? 이 질문은 편집증적인 것이 아니라 실무적인 것이다. 디지털 플랫폼은 최근 몇 년간 그 능력을 거듭 행사해 왔다. 때로는 자체 발의로, 때로는 정부의 명령 아래, 때로는 소유권이나 정책의 변경 이후에. 능력이 존재한다면, 그것이 계약상 선언된 어떤 전제 아래에서 행사되는지를 알고, 선언되지 않은 전제를 위한 여지를 남겨 두는 것이 좋다. 최근 몇 년의 관행은 그러한 전제들이 못지않게 중요함을 보여 왔다. 즉 예기치 못한 사법 명령, 국제적 제재, 기업 지배구조의 변경, 다른 정책을 가진 사업체에 의한 인수다.

짝을 이루는 질문은 연속성 계획에 관한 것이다. operador가——정당하든 아니든, 어떤 이유에서든——전문가에게 그 능력을 행사한다면, 얼마만큼의 가동 시간이 계속 이용 가능할 것인가, 어떤 데이터 내보내기 절차가 존재하는가, 그리고 어느 대체 제공자로 이전할 수 있는가? 답이 「그런 일은 일어나지 않을 것이다」로 시작한다면, 그것은 실무적인 답이 아니라 약속이다.

5층: 정체성과 접근

서비스 접근 자격 증명을 통제하는 것은 누구인가? operador가 사용자의 참여 없이 사용자의 접근을 재설정할 수 있다면——흔히 「계정 복구」라고 불리는 절차——, operador는 기술적으로 계정의 보관자이며, 적절한 절차를 통해 요청해 온 자에게 그것을 양도할 수도 있다. 정체성이 암호학적으로 사용자의 기기에 존재하기 때문에 operador가 접근을 재설정할 수 없다면, operador는 그것을 양도할 수도 없으며, 명령 아래에서조차 그렇다. 두 방식은 맥락에 따라 모두 정당하다. 그러나 여기서도 다시, 그것들은 서로 다르며, 어느 것을 채택하고 있는지를 아는 것이 좋다.

전문가가 접근을 잃으면 전문가의 데이터는 어떻게 되는가? operador에 의존하는 복구 메커니즘——계정의, 파일의, 세션의——이 존재하는가? operador가 그것들을 사용하도록 강요받는다면, 그 메커니즘들이 해당 분야의 직업 윤리와 양립할 수 있는가?

6층: 미래

이 마지막 층은 전망을 요구하기 때문에 흔히 소홀히 다뤄진다. 서비스가 다른 회사에 인수된다면 무슨 일이 일어나는가? 거의 모든 인수는 그 후 몇 달 안에 서비스 약관의 재검토를 동반한다. 규제 요구가 바뀐다면 무슨 일이 일어나는가? 유럽법은 2022년 이래 삭제와 차단의 의무를 늘려 왔지, 줄이지 않았다. operador가 사라진다면 무슨 일이 일어나는가? 클라우드 서비스의 적지 않은 부분은 operador의 폐쇄 시나리오에 대비한 문서화된 탈출 계획을 갖고 있지 않으며, 전문가는 더 이상 준비할 시간이 없을 때에야 그 문제를 발견한다.

이 층에 대해 기억해 둘 만한 한 가지 정식이 있다. operador에 덜 의존하는 아키텍처일수록 operador의 변화에 더 회복력이 있다. 어떤 방식의 셀프 호스팅이든, 자기주권적 암호학적 정체성, 중간에 서버가 없는 통신, 이

모두는 현재의 의존의 표면을 줄이는 절차를 통해 미래의 위험 표면을 줄인다. 그것은 위험을 없애는 것이 아니다. 줄이는 것이다.

구조와 약속의 차이

이 사이클을 단 한 문장으로 증류해야 한다면, 그것은 이러할 것이다. 구조적인 답은 operador도, 행정도, 법률도 바뀌더라도 유지된다. 약속에 의한 답은 약속하는 자가 그것을 유지할 수 있고 또 유지하려는 한 유지된다. 둘 다 채택하는 시점에서는 옳을 수 있다. 그러나 시간의 흐름과 상황의 변화에 좌우되지 않고 버티는 것은 둘 중 하나뿐이다.

이것은 각 전문가가 자신이 도입하는 모든 서비스에 구조적인 답을 요구해야 한다는 뜻이 아니다. 비례성은 여전히 정당하다. 내부 회계를 위한 스프레드시트가 필요로 하는 답은 환자의 진료 기록이 필요로 하는 답과 같지 않다. 그것이 뜻하는 바는 이러하다. 전문가다움이란 각 경우에 어떤 종류의 답을 받아들였는지를 알고, 그 종류의 답이 그 구체적인 데이터에 비례한다고 의식적으로 결정해 두었음에 있다.

정리된 질문지

이 사이클을 종합하는 열두 가지 구체적인 질문. 각 질문의 답이 다음 질문에 정보를 주도록 순서를 매겼다:

1. 콘텐츠가 operador의 서버를 거치는가? 거친다면: 평문인가, operador의 키로 암호화되는가, 아니면 사용자 전용 키로 암호화되는가?
2. 종단 간 암호화가 표방된다면, 암호 키는 어디에 있는가? operador가 「복구」를 포함한 어떤 형태로든 그 일부를 알거나 보관하고 있는가?
3. 서비스는 어떤 메타데이터를 생성하고 보관하는가? 얼마나 오래? 누구에게 보이는가?
4. operador는 어떻게 자금을 조달하는가? 자금 조달에 광고나 데이터 수익화가 포함된다면, 선언된 목적이 전문가가 맡긴 제3자의 데이터까지 포괄하는가?
5. operador의 3~5년 후 재무 상황은 어떠한가? 모델의 임박한 변경을 시사하는 요인이 있는가(보류 중인 기업공개, 소진되어 가는 펀딩 라운드, 가능성 있는 인수)?
6. operador는 어느 관할권에 설립되어 있는가? 서버는 물리적으로 어느 나라에 있는가? 둘이 다르다면, 처리에는 어느 나라의 법률이 적용되는가?
7. operador의 관할권에서 유효한 정보기관 명령이 내 데이터의 인도를 요구한다면 무슨 일이 일어나는가? 회사가 기술적으로 그것을 이행할 수 있는가?
8. operador는 서비스를 정지, 차단, 또는 삭제하기 위한 어떤 기술적 능력을 보유하고 있는가? 어떤 계약상의 전제 아래에서인가? 역사적으로 문서화된, 어떤 계약 외의 전제 아래에서인가?
9. operador가 그 능력을 정당하게든 부당하게든 나에게 행사한다면 어떤 탈출 계획이 있는가? 대체 제공자로 데이터를 내보내는 문서화된 절차가 있는가?
10. 접근 자격 증명을 통제하는 것은 누구인가? operador가 내 참여 없이 그것을 재설정할 수 있는가? 그것은 나를 보호하는가, 아니면 나를 노출시키는가?
11. 이 구체적인 기능에 대해 유럽산의, 셀프 호스트형의, 또는 중간에 서버가 없는 대안이 존재하는가? 평가한 위험과 비교했을 때 그것의 실제 비용은 얼마인가?

12. 오늘의 결정이 5년 후 감독관, 감사인, 또는 유출로 피해를 입은 고객에 의해 검토된다면, 현재의 선택은 오늘 가진 논거로 옹호할 수 있을 것인가, 아니면 합당한 질문을 던지지 않은 데 대해 사과해야 할 것인가?

이 질문들은 완벽한 답을 기대하지 않는다. 정직한 답을 기대한다. 정직한 operador는 그것을 답할 줄 알고, 덜 정직한 operador는 정확하게 진술하기를 피한다. 두 종류의 operador 사이의 실무적 차이는, 과장 없이 말하건대, 더 많은 것을 요청해야 할 필요가 생기기도 전에, 그들이 자발적으로 제시하는 답을 천천히 읽음으로써 감지되는 경우가 많다.

이 글로 우리는 Cuadernos Lacre의 두 번째 사이클을 마무리한다. Schrems II에서 물려받은 편집상의 부채로 시작해 실무적인 질문지로 끝맺었다. 그 길에서 우리는 여러 개념을——해시, 암호화, 정체성을——, 그리고 적용된 분석을——kill switch, 비즈니스 모델, 셀프 호스팅을——거쳐 왔다. 이 간행물이 표방한 편집 의도는 문제의 망라적인 목록으로 독자를 압도하는 것이 아니라, 어떤 새로운 서비스를 마주하든 자신이 어떤 종류의 답을 받아들이고 있는지를 구별할 도구를 그의 손에 쥐여 주는 것이었다. 그 구별——아키텍처와 약속 사이의——이 바로 그 도구다. 나머지는 각 전문가가 자신의 실무에서 그 질문에 값한다고 여기는 데이터를 위해 그것을 활용하면 된다.

참고 문헌 및 관련 자료

- 이 간행물, 두 번째 사이클(2026년 5월)——*슈렘스 II 판결, 5년 후*, *SHA-256이 정말 무엇인가*, *킬 스위치와 제도적 포획*, *종단 간 암호화를 제대로 설명하다*, *신뢰의 신호로서의 비즈니스 모델*, *24개의 단어: 암호학적 정체성이란 무엇인가*, *전문적 실천으로서의 셀프 호스팅*. 이 질문지가 기대고 있는 일곱 편의 글.
- 규정(EU) 2016/679——일반 데이터 보호 규정. 질문지가 제기하는 모든 질문의 참조 법적 틀이며, 특히 제5조, 제6조, 제25조, 제28조, 제32조, 제33조, 그리고 제5장.
- 유럽 데이터 보호 이사회——Schrems II, 국제 이전, 영향 평가, 능동적 책임에 관한 실무적 지침과 의견(2020-2024년 발행물).
- 스페인 데이터 보호청——부적절한 이전 수단을 사용했거나 실질적 내용이 없는 형식적 영향 평가를 한 처리자에 대해 2022-2024년에 공표된 제재.
- noyb.eu——Maximilian Schrems가 이끄는 유럽 디지털 권리 센터. 유럽 데이터 보호 규범의 겉보기가 아닌 실제 준수에 관한 신고, 항고, 분석의 공개 저장소.

← 이전전문적 실무로서의 셀프 호스팅다음 →서명으로 해결할 수 없는 것

최근 읽은 글

- 성찰 · 2026년 6월 29일 당신은 익명이 아닙니다
- 성찰 · 2026년 5월 27일 서명으로 해결할 수 없는 것
- 분석 · 2026년 5월 25일 전문적 실무로서의 셀프 호스팅

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 f75848f4804c58f174335e9207012c6a8e6416f838a4f1f0a09c029a7781208e

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