Аналіз · 26 травня 2026 р.

← Попередній·Наступний →

Справжня проти видимої приватності: питання, які варто собі поставити

Операційний синтез циклу 2: питання, які відрізняють сервіс з архітектурною приватністю від сервісу з декларативною приватністю. Опитувальник для європейського фахівця, перш ніж прийняти будь-який цифровий інструмент для чутливих даних.

Щоб порозумітися: Два сервіси з однаковим правовим повідомленням можуть поводитися дуже по-різному. Один захищає за технічним дизайном. Інший захищає за договірною обіцянкою. Різниця не читається в повідомленні — вона виявляється через формулювання конкретних питань. Якість відповідей каже про продукт стільки ж, скільки його власний зміст.

Різниця між архітектурною приватністю та декларативною приватністю

Протягом семи попередніх статей цього циклу ми пройшли крізь різні шари того самого питання. Право міжнародних передач із Schrems II. Математичну ідею криптографічного хешу, що скріплює кожен Cuaderno. Архітектурний вибір kill switch та інституційне захоплення, яке майже завжди його супроводжує. Механізм наскрізного шифрування та операційне питання про те, де знаходяться ключі. Узгодження стимулів відповідно до бізнес-моделі. Самосуверенну криптографічну ідентичність. Самостійне розміщення як пропорційну стратегію. Кожна стаття займалася одним кутом зору. Ця, остання в циклі, зводить їх в одному опитувальнику.

Розрізнення, яке варто запам'ятати, просте: є сервіси, чия приватність є *архітектурною*, і є сервіси, чия приватність є *декларативною*. Перша вбудована в технічний дизайн: певні порушення зобов'язання щодо приватності технічно складні чи неможливі, тому що архітектура їх не дозволяє. Друга закладена в текст правового повідомлення: певні порушення були б договірно караними, якби сталися, але технічно ніщо їх не перешкоджає. Обидві моделі можуть відповідати РЗД; але одна захищає за конструкцією, а інша захищає за обіцянкою, і різниця операційно величезна.

Питання, що йдуть далі, розроблені, щоб відрізнити один випадок від іншого. Це не складні технічні питання. Це питання, на які будь-який чесний постачальник може відповісти у своїй публічній документації. Якість і точність відповіді кажуть про продукт стільки ж, скільки сама відповідь. Питання згруповані в шість шарів; варто поставити їх усі, перш ніж приймати сервіс для чутливих даних, а не лише ті, які ідентифікує перший інстинкт.

Шар 1: архітектура

Перш ніж продовжити, уточнімо один термін. Під *оператором* ми розуміємо компанію, яка надає послугу: суб'єкт, який контролює сервери та програмне забезпечення, а не конкретну особу. Після цього уточнення основне архітектурне питання таке: що оператор робить із вмістом між відправником і

одержувачем? Можливих відповідей три, і варто вміти їх розрізняти, бо всі три інколи рекламують схожою лексикою.

- Перша: контент проходить через сервер оператора у відкритому вигляді, де оператор може його читати, навіть якщо обіцяє цього не робити.
- Друга: контент проходить через сервер оператора зашифрованим, де оператор не може його читати, якщо ключі знаходяться виключно на пристроях користувачів.
- Третя: контент не проходить через жоден сервер оператора, тому що в цьому конкретному потоці сервера оператора не існує.

Різниця між цими трьома не за ступенем: вона за типом.

Доповнювальне питання — вже сформульоване в Cuaderno про шифрування — таке: хто має криптографічні ключі, що дозволяють читати контент? Якщо їх має користувач і лише користувач, шифрування реальне. Якщо їх має ще й оператор у будь-якій формі — навіть під назвою «відновлення облікового запису» чи «синхронізація між пристроями» —, шифрування номінальне. Питання не допускає чесної проміжної відповіді.

Шар 2: бізнес-модель

Питання про бізнес-модель важить стільки ж, скільки архітектурне питання, і з тієї самої сутнісної причини: стимули виробляють із плином часу систематично різні продукти навіть за ідентичних заявлених цілей. Як заробляє гроші сьогодні оператор? Одне джерело, два, суміш? Якщо фінансування включає рекламу чи монетизацію даних, які дані монетизуються і на якій правовій підставі РЗД це робиться? Чи покриває мета, заявлена в правовому повідомленні, дані третіх осіб, які фахівець має намір довірити сервісу?

І питання другого порядку, не завжди сформульоване: яке фінансове становище оператора в перспективі трьох-п'яти років? Компанія у фазі венчурного капіталу працює під іншим тиском, ніж компанія зі стабільною прибутковістю. Зміна моделі фінансування — це, неодноразово, момент, коли неявний договір із користувачами переписується без перемовин.

Шар 3: юрисдикція

Для європейського фахівця питання юрисдикції не є риторичним. У якій юрисдикції зареєстрований оператор? У якій країні фізично розташовані сервери, що обробляють дані? Чи відповідь на два попередні питання та сама чи різна, і якщо різниться, яке законодавство застосовується? Європейський регіон, керований американською компанією, не є, для цілей Schrems II, європейською відповіддю: компанія підпорядкована FISA 702 незалежно від того, де знаходяться сервери.

Доповнювальне операційне питання таке: якби завтра надійшло чинне в юрисдикції оператора розвідувальне розпорядження з вимогою видати мої дані чи дані моїх клієнтів, що сталося б? Якщо чесна відповідь починається з «компанія була б зобов'язана їх видати», сервіс не захищає від цього розпорядження, хоч би скільки реклама натякала на протилежне. Якщо чесна відповідь починається з «компанія не могла б їх видати, бо не має їх у відкритому вигляді», сервіс таки захищає; і різниця залежить майже цілком від перших двох шарів, а не від якості політики приватності.

Шар 4: оператор та kill switch

Яку технічну спроможність зберігає оператор, щоб призупинити, заблокувати, видалити чи погіршити сервіс на відстані? Питання не є параноїдальним: воно операційне. Цифрові платформи неодноразово застосовували цю спроможність в останні роки, іноді з власної ініціативи, іноді за розпорядженням

урядів, іноді після зміни власності чи політики. Якщо спроможність існує, варто знати, за яких договірно заявлених передумов вона застосовується, і зберегти запас для незаявлених передумов, які практика останніх років показала не менш значущими: несподіване судове розпорядження, міжнародна санкція, зміна корпоративного керівництва, поглинання суб'єктом з іншою політикою.

Споріднене питання — це питання плану безперервності: якби оператор застосував спроможність проти фахівця — з будь-якої причини, справедливої чи ні —, який час активності залишився б доступним, яка процедура експорту даних існує і до якого альтернативного постачальника можна було б мігрувати? Якщо відповідь починається з «цього не повинно статися», це не операційна відповідь; це обіцянка.

Шар 5: ідентичність та доступ

Хто контролює облікові дані доступу до сервісу? Якщо оператор може відновити доступ користувача без участі користувача — процедура, яку зазвичай називають «відновленням облікового запису» —, оператор є технічно зберігачем облікового запису і може також передати його тому, хто це запросить через відповідну процедуру. Якщо оператор не може відновити доступ, тому що ідентичність криптографічно знаходиться на пристрої користувача, оператор не може і передати її, навіть за розпорядженням. Обидва різновиди легітимні залежно від контексту; але, знову ж таки, вони різні, і варто знати, який саме приймається.

Що відбувається з даними фахівця, якщо фахівець втрачає доступ? Чи існують механізми відновлення — облікового запису, файлу, сесії —, що залежать від оператора? Чи сумісні ці механізми з професійною деонтологією галузі, якщо оператора примусять їх використати?

Шар 6: майбутнє

Цей останній шар часто залишають поза увагою, бо він вимагає проєкції. Що сталося б, якби сервіс був придбаний іншою компанією? Майже всі поглинання тягнуть за собою перегляд умов сервісу в наступні місяці. Що сталося б, якби регуляторні вимоги змінилися? Європейське право збільшило зобов'язання щодо вилучення та блокування з 2022 року, а не зменшило їх. Що сталося б, якби оператор зник? Значна частина хмарних сервісів не має задокументованого плану виходу для сценарію закриття оператора; фахівець виявляє проблему, коли вже немає часу її підготувати.

Є формулювання, яке варто запам'ятати для цього шару: архітектури, що менше залежать від оператора, є стійкішими до змін оператора. Самостійне розміщення в будь-якому з його різновидів, самосуверенна криптографічна ідентичність, комунікації без сервера посередині — усі вони зменшують майбутню поверхню ризику через процедуру зменшення нинішньої поверхні залежності. Вони її не усувають; вони її зменшують.

Різниця між структурою та обіцянкою

Якби нам довелося дистилювати цикл в одне речення, воно було б таким: структурні відповіді зберігаються, навіть якщо оператор, адміністрація чи законодавство зміняться; відповіді через обіцянку зберігаються, доки той, хто обіцяє, може і хоче їх зберігати. Обидві можуть бути правильними в момент прийняття. Лише одна з двох тримається незалежно від плину часу та зміни обставин.

Це не означає, що кожен фахівець має вимагати структурних відповідей від усіх сервісів, які він приймає. Пропорційність залишається легітимною: електронна таблиця для внутрішньої бухгалтерії не потребує такої самої відповіді, як медична картка пацієнта. Це означає, однак, що професійність полягає в тому, щоб знати, який тип відповіді було прийнято в кожному випадку, і свідомо вирішити, що цей тип відповіді пропорційний конкретним даним.

Опитувальник, упорядкований

Дванадцять конкретних питань, які синтезують цикл, упорядкованих так, щоб відповідь на кожне інформувала наступне:

1. Чи проходить контент через сервер оператора? Якщо проходить: у відкритому вигляді, зашифрований ключами оператора чи зашифрований ключами, що належать виключно користувачеві?
2. Якщо посилаються на наскрізне шифрування, де знаходяться криптографічні ключі? Чи знає або зберігає оператор будь-яку їх частину в будь-якій формі, включно з «відновленням»?
3. Які метадані генерує та зберігає сервіс? Як довго? Кому вони видимі?
4. Як фінансується оператор? Якщо фінансування включає рекламу чи монетизацію даних, чи покриває заявлена мета дані третіх осіб, довірені фахівцем?
5. Яке фінансове становище оператора в перспективі трьох-п'яти років? Чи є фактори, що вказують на неминучу зміну моделі (очікуваний вихід на біржу, раунд фінансування, що вичерпується, ймовірне поглинання)?
6. У якій юрисдикції зареєстрований оператор? У якій країні фізично розташовані сервери? Якщо вони різняться, яке національне законодавство застосовується до обробки?
7. Що сталося б, якби чинне в юрисдикції оператора розвідувальне розпорядження вимагало видати мої дані? Чи могла б компанія виконати його технічно?
8. Яку технічну спроможність зберігає оператор, щоб призупинити, заблокувати чи видалити сервіс? За яких договірних передумов? За яких історично задокументованих недоговірних передумов?
9. Який план виходу існує, якщо оператор застосував би цю спроможність проти мене, справедливо чи несправедливо? Чи є задокументована процедура експорту даних до альтернативного постачальника?
10. Хто контролює облікові дані доступу? Чи може оператор відновити їх без моєї участі? Це мене захищає чи наражає?
11. Чи існує європейська, самостійно розміщена або без сервера посередині альтернатива для цієї конкретної функції? Яка її реальна вартість порівняно з оціненим ризиком?
12. Якби сьогоднішнє рішення було розглянуте через п'ять років інспектором, аудитором чи клієнтом, постраждалим від витоку, чи був би нинішній вибір захищуваним наявними сьогодні аргументами, чи вимагав би вибачення за те, що не було поставлено розумних питань?

Питання не очікують досконалих відповідей. Вони очікують чесних відповідей, які чесний оператор уміє давати, а менш чесний оператор уникає формулювати з точністю. Операційну різницю між двома видами операторів, кажемо це без драматизму, зазвичай відчувають, повільно читаючи відповіді, які вони пропонують добровільно, ще до того, як доведеться просити більше.

Цією статтею ми завершуємо другий цикл Cuadernos Lacre. Ми почали з редакційного боргу, успадкованого від Schrems II, і закінчуємо операційним опитувальником. Дорогою ми пройшли крізь поняття — хеш, шифрування, ідентичність — та прикладні аналізи — kill switch, бізнес-модель, self-hosting. Заявлений редакційний намір видання полягав не в тому, щоб приголомшити читача вичерпним переліком проблем, а в тому, щоб дати йому інструменти, аби він розрізняв, перед будь-яким новим сервісом, який тип відповіді він приймає. Це розрізнення — між архітектурою та обіцянкою — і є інструментом. Решту кожен фахівець поставить на службу тим даним, які у своїй практиці вважатиме гідними цього питання.

Джерела та додаткова література

- Це видання, цикл 2 (травень 2026 р.) — *Schrems II через п'ять років, Що таке насправді SHA-256, Kill switch та інституційне захоплення, Наскрізне шифрування, пояснене по-справжньому, Бізнес-*

модель як ознака довіри, 24 слова: що таке криптографічна ідентичність, Self-hosting як професійна практика. Сім статей, на яких ґрунтується цей опитувальник.

- Регламент (ЄС) 2016/679 — Загальний регламент про захист даних. Референтна правова рамка для всіх питань, які ставить опитувальник, зокрема статті 5, 6, 25, 28, 32, 33 та розділ V.
- Європейська рада із захисту даних — настанови та операційні висновки щодо Schrems II, міжнародних передач, оцінок впливу та проактивної відповідальності (публікації 2020-2024).
- Іспанське агентство із захисту даних — санкції, опубліковані 2022-2024, проти контролерів даних за неналежні інструменти передачі чи за формальні оцінки впливу без суттєвого змісту.
- noyb.eu — Європейський центр цифрових прав, очолюваний Maximilian Schrems. Публічне сховище скарг, ресурсів та аналізів щодо реального, а не видимого дотримання європейських норм захисту даних.

← ПопереднійSelf-hosting як професійна практикаНаступний →Те, що підпис не може виправити

Останні матеріали

- Роздуми · 29 червня 2026 р. Ви не анонімні
- Рефлексія · 27 травня 2026 р. Те, що підпис не може виправити
- Аналіз · 25 травня 2026 р. Self-hosting як професійна практика

Візьміть цю статтю з собою куди завгодно.

↓ Markdown ↓ Звичайний текст ↓ PDF

Файл буде завантажено на ваш пристрій. Звідти ви можете зберегти його, імпортувати в Solo2 або поділитися ним де завгодно. Cuadernos не вирішує місце призначення за вас.

Сургучна печатка · SHA-256 83870d97775fe2faaa318617db315d86175f668e3fc68c208cad616a41b90e63

Cuadernos Lacre · Видання Menzuri Gestión S.L. ·
автор R.Eugenio · під редакцією команди Solo2.

Цей сайт не використовує куки. Усе, що завантажує ваш браузер, написане або контрольоване нами та розміщене на наших європейських серверах: анонімний лічильник відвідувань (Umami, самостійно розміщений) і мінімум JavaScript, необхідний для вибору мови та вашого налаштування світлої/темної теми, яке зберігається на вашому власному пристрої. Без сторонніх ресурсів, без трекерів, без профілювання, без поширення даних. Якщо ви хочете стежити за нами: RSS.