Анализ · 26 май 2026 г.

← Предишна·Следваща →

Истинска срещу привидна поверителност: въпросите, които си заслужава да си зададем

Оперативен синтез на цикъл 2: въпросите, които отличават услуга с архитектурна поверителност от услуга с декларативна поверителност. Въпросник за европейския професионалист, преди да приеме какъвто и да е цифров инструмент за чувствителни данни.

За да се разберем: Две услуги с едно и също правно известие могат да се държат много различно. Едната защитава по технически дизайн. Другата защитава по договорно обещание. Разликата не се чете в известието — открива се чрез формулиране на конкретните въпроси. Качеството на отговорите казва за продукта толкова, колкото и самото му съдържание.

Разликата между архитектурна поверителност и декларативна поверителност

В хода на седемте предишни статии от този цикъл преминахме през различни слоеве на един и същ въпрос. Правото на международните трансфери с Schrems II. Математическата идея за криптографския хеш, който подпечатва всеки Cuaderno. Архитектурният избор на kill switch и институционалното овладяване, което почти винаги го съпровожда. Механизмът на криптирането от край до край и оперативният въпрос къде се намират ключовете. Подравняването на стимулите според бизнес модела. Самосуверенната криптографска идентичност. Самохоствания като пропорционална стратегия. Всяка статия се занимаваше с един ъгъл. Тази, последната от цикъла, ги събира в един въпросник.

Различаването, което си заслужава да се запомни, е просто: има услуги, чиято поверителност е *архитектурна*, и има услуги, чиято поверителност е *декларативна*. Първата е вградена в техническия дизайн: определени нарушения на ангажимента за поверителност са технически трудни или невъзможни, защото архитектурата не ги позволява. Втората е положена в текста на правното известие: определени нарушения биха били договорно санкционируеми, ако настъпят, но технически нищо не ги възпрепятства. Двата модела могат да спазват РЗД; но единият защитава по конструкция, а другият защитава по обещание, и разликата е оперативно огромна.

Въпросите, които следват, са замислени, за да отличат единия случай от другия. Те не са напреднали технически въпроси. Те са въпросите, на които всеки честен доставчик може да отговори в публичната си документация. Качеството и прецизността на отговора казват за продукта толкова, колкото и самият отговор. Въпросите се групират в шест слоя; добре е да се зададат всички, преди да се приеме услугата за чувствителни данни, не само онези, които първият инстинкт идентифицира.

Слой 1: архитектура

Преди да продължим, нека уточним един термин. Под *оператор* разбираме компанията, която предоставя услугата: субектът, който контролира сървърите и софтуера, а не конкретно лице. След това уточнение основният архитектурен въпрос е: какво прави операторът със съдържанието между подателя и

получателя? Възможните отговори са три и си струва да се научим да ги различаваме, защото и трите понякога се рекламират със сходна терминология.

- Първият: съдържанието минава през сървър на оператора в явен вид, където операторът може да го чете, дори ако обещае да не го прави.
- Вторият: съдържанието минава през сървър на оператора криптирано, където операторът не може да го чете, ако ключовете се намират изключително в устройствата на потребителите.
- Третият: съдържанието не минава през никакъв сървър на оператора, защото не съществува сървър на оператора в този конкретен поток.

Разликата между тези три не е по степен: тя е по вид.

Допълващият въпрос — вече формулиран в Cuaderno за криптирането — е: кой притежава криптографските ключове, които позволяват четенето на съдържанието? Ако ги притежава потребителят и само потребителят, криптирането е реално. Ако ги притежава освен това и операторът под каквато и да е форма — дори под името «възстановяване на акаунт» или «синхронизация между устройства» —, криптирането е номинално. Въпросът не допуска честен междинен отговор.

Слой 2: бизнес модел

Въпросът за бизнес модела има толкова значение, колкото и архитектурният въпрос, и поради същата същностна причина: стимулите произвеждат с течение на времето системно различни продукти дори при идентични заявени цели. Как печели пари днес операторът? Един-единствен източник, два, смесица? Ако финансирането включва реклама или монетизация на данни, какви данни се монетизират и на какво правно основание на РЗД се прави това? Покрива ли целта, заявена в правното известие, данните на трети лица, които професионалистът възнамерява да повери на услугата?

И въпросът от втори ред, не винаги формулиран: какво е финансовото състояние на оператора в перспектива от три до пет години? Компания във фаза на рисков капитал работи под различен натиск от компания в стабилна рентабилност. Промяната на модела на финансиране е, многократно, моментът, в който подразбиращият се договор с потребителите се пренаписва без преговори.

Слой 3: юрисдикция

За европейския професионалист въпросът за юрисдикцията не е реторичен. В коя юрисдикция е регистриран операторът? В коя държава са физически разположени сървърите, които обработват данните? Отговорът на двата предходни въпроса един и същ ли е или различен, и ако се различава, кое законодателство се прилага? Европейски регион, опериран от американска компания, не е, за целите на Schrems II, европейски отговор: компанията е подчинена на FISA 702 независимо от това къде са сървърите.

Допълващият оперативен въпрос е: ако утре пристигне валидна разузнавателна заповед в юрисдикцията на оператора с искане за предаване на моите данни или тези на моите клиенти, какво би станало? Ако честният отговор започва с «компанията би била длъжна да ги предаде», услугата не защитава срещу тази заповед, колкото и рекламата да подсказва обратното. Ако честният отговор започва с «компанията не би могла да ги предаде, защото не ги притежава в явен вид», услугата наистина защитава; и разликата зависи почти изцяло от първите два слоя, не от качеството на политиката за поверителност.

Слой 4: оператор и kill switch

Какъв технически капацитет запазва операторът, за да спре, блокира, премахне или влоши услугата от разстояние? Въпросът не е параноичен: той е оперативен. Цифровите платформи са упражнявали този

капацитет многократно през последните години, понякога по собствена инициатива, друг път по заповед на правителства, друг път след промяна на собствеността или политиката. Ако капацитетът съществува, добре е да се знае при какви договорно заявени предпоставки се упражнява и да се запази резерв за незаявените предпоставки, които практиката от последните години показа за също толкова важни: неочаквана съдебна заповед, международна санкция, промяна на корпоративното ръководство, придобиване от субект с друга политика.

Сродният въпрос е този за плана за непрекъснатост: ако операторът упражни капацитета срещу професионалиста — по каквато и да е причина, справедлива или не —, какво време на активност би останало на разположение, каква процедура за експортиране на данни съществува и към кой алтернативен доставчик би могло да се мигрира? Ако отговорът започва с «не би трябвало да се случи», това не е оперативен отговор; това е обещание.

Слой 5: идентичност и достъп

Кой контролира идентификационните данни за достъп до услугата? Ако операторът може да възстанови достъпа на потребителя без участието на потребителя — процедура, наричана обикновено «възстановяване на акаунт» —, операторът е технически попечител на акаунта и може също да го предостави на този, който го поиска чрез подходящата процедура. Ако операторът не може да възстанови достъпа, защото идентичността се намира криптографски в устройството на потребителя, операторът не може и да я предостави, дори по заповед. Двете разновидности са легитимни според контекста; но, отново, те са различни и е добре да се знае коя се приема.

Какво става с данните на професионалиста, ако професионалистът загуби достъп? Съществуват ли механизми за възстановяване — на акаунт, на файл, на сесия —, които зависят от оператора? Съвместими ли са тези механизми с професионалната деонтология на сектора, ако операторът бъде принуден да ги използва?

Слой 6: бъдеще

Този последен слой често се пренебрегва, защото изисква проекция. Какво би станало, ако услугата бъде придобита от друга компания? Почти всички придобивания водят след себе си преразглеждане на условията на услугата през следващите месеци. Какво би станало, ако регулаторните изисквания се променят? Европейското право увеличи задълженията за оттегляне и блокиране от 2022 г. насам, не ги е намалило. Какво би станало, ако операторът изчезне? Значителна част от облачните услуги нямат документиран план за излизане за сценария на закриване на оператора; професионалистът открива проблема, когато вече няма време да го подготви.

Има една формулировка, която си заслужава да се запомни за този слой: архитектурите, които зависят по-малко от оператора, са по-устойчиви на промени в оператора. Самохоствания в която и да е от своите разновидности, самосуверенната криптографска идентичност, комуникациите без сървър по средата — всички те намаляват бъдещата повърхност на риск чрез процедурата на намаляване на настоящата повърхност на зависимост. Не я елиминират; намаляват я.

Разликата между структура и обещание

Ако трябваше да дестилираме цикъла в едно изречение, то би било това: структурните отговори се запазват, дори ако операторът, администрацията или законодателството се променят; отговорите чрез обещание се запазват, докато този, който обещава, може и иска да ги запази. И двата могат да бъдат правилни в момента на приемането им. Само единият от двата се удържа независимо от хода на времето и промяната на обстоятелствата.

Това не означава, че всеки професионалист трябва да изисква структурни отговори от всички услуги, които приема. Пропорционалността остава легитимна: електронна таблица за вътрешно счетоводство не се нуждае от същия отговор като клиничното досие на пациент. Означава обаче, че професионализмът се състои в това да се знае какъв вид отговор е приет във всеки случай и съзнателно да е било решено, че този вид отговор е пропорционален на конкретното данно.

Въпросникът, подреден

Дванайсет конкретни въпроса, които синтезират цикъла, подредени така, че отговорът на всеки да информира следващия:

1. Минава ли съдържанието през сървър на оператора? Ако минава: в явен вид, криптирано с ключове на оператора, или криптирано с ключове, изключителна собственост на потребителя?
2. Ако се позовава на криптиране от край до край, къде се намират криптографските ключове? Знае ли или пази ли операторът някаква тяхна част под каквато и да е форма, включително «възстановяване»?
3. Какви метаданни генерира и пази услугата? За колко време? За кого са видими?
4. Как се финансира операторът? Ако финансирането включва реклама или монетизация на данни, покрива ли заявената цел данните на трети лица, поверени от професионалиста?
5. Какво е финансовото състояние на оператора в перспектива от три до пет години? Има ли фактори, които подсказват предстояща промяна на модела (предстоящо излизане на борсата, изчерпващ се кръг на финансиране, вероятно придобиване)?
6. В коя юрисдикция е регистриран операторът? В коя държава са физически разположени сървърите? Ако се различават, кое национално законодателство се прилага към обработването?
7. Какво би станало, ако валидна разузнавателна заповед в юрисдикцията на оператора поиска предаване на моите данни? Би ли могла компанията да я изпълни технически?
8. Какъв технически капацитет запазва операторът, за да спре, блокира или премахне услугата? При какви договорни предпоставки? При какви исторически документирани недоговорни предпоставки?
9. Какъв план за излизане съществува, ако операторът упражни този капацитет срещу мен, справедливо или несправедливо? Има ли документирана процедура за експортиране на данните към алтернативен доставчик?
10. Кой контролира идентификационните данни за достъп? Може ли операторът да ги възстанови без моето участие? Това ме защитава ли, или ме излага?
11. Съществува ли европейска, самохоствана или без сървър по средата алтернатива за тази конкретна функция? Каква е реалната ѝ цена, в сравнение с оценения риск?
12. Ако днешното решение бъде разгледано след пет години от инспектор, одитор или клиент, засегнат от пробив, би ли било настоящият избор защитим с наличните днес аргументи, или би изисквал извинение за това, че не са били зададени разумни въпроси?

Въпросите не очакват съвършени отговори. Очакват честни отговори, които честният оператор умее да дава, а по-малко честният оператор избягва да формулира с точност. Оперативната разлика между двата вида оператор, казваме го без драматизъм, обикновено се долавя при бавно четене на отговорите, които предлагат доброволно, още преди да се наложи да се иска повече.

С тази статия закриваме втория цикъл на Cuadernos Lacre. Започнахме с редакционния дълг, наследен от Schrems II, и завършваме с оперативен въпросник. По пътя преминахме през понятия — хеш, криптиране, идентичност — и приложни анализи — kill switch, бизнес модел, self-hosting. Заявеното редакционно намерение на изданието не беше да затрупа читателя с изчерпателен списък от проблеми, а да му даде инструменти, за да различава, изправен пред всяка нова услуга, какъв вид отговор приема. Това различаване — между архитектура и обещание — е инструментът. Останалото всеки професионалист ще постави в служба на данните, които в своята практика смята за достойни за въпроса.

Източници и допълнително четиво

- Това издание, цикъл 2 (май 2026 г.) — *Schrems II, пет години по-късно*, *Какво всъщност е SHA-256*, *Kill switch и институционалното овладяване*, *Криптиране от край до край, обяснено наистина*, *Бизнес моделът като сигнал за доверие*, *24-те думи: какво е криптографска идентичност*, *Self-hosting като професионална практика*. Седемте статии, върху които почива този въпросник.
- Регламент (ЕС) 2016/679 — Общ регламент относно защитата на данните. Референтна правна рамка за всички въпроси, които въпросникът поставя, по-специално членове 5, 6, 25, 28, 32, 33 и глава V.
- Европейски комитет по защита на данните — насоки и оперативни становища относно Schrems II, международните трансфери, оценките на въздействието и проактивната отговорност (публикации 2020-2024).
- Испанска агенция за защита на данните — санкции, публикувани 2022-2024, срещу администратори на лични данни за неадекватни инструменти за трансфер или за формални оценки на въздействието без съществено съдържание.
- noyb.eu — Европейски център за цифрови права, ръководен от Maximilian Schrems. Публично хранилище на жалби, ресурси и анализи относно реалното, а не привидното спазване на европейските норми за защита на данните.

← ПредишнаSelf-hosting като професионална практикаСледваща →Какво един подпис не може да поправи

Скорошни четива

- Размисъл · 29 юни 2026 г. Не сте анонимни
- Размисъл · 27 май 2026 г. Какво един подпис не може да поправи
- Анализ · 25 май 2026 г. Self-hosting като професионална практика

Вземете тази статия със себе си навсякъде, където ви е необходима.

↓ Markdown ↓ Обикновен текст ↓ PDF

Файлът ще бъде изтеглен на вашето устройство. Оттам можете да го запазите, импортирате в Solo2 или споделите където пожелаете. Cuadernos не решава дестинацията вместо вас.

Восъчен печат · SHA-256 136584432e50af1192feb70cf041c5e315de83f93e1fc72f76265b5b1bff6e1c

Cuadernos Lacre · Публикация на Menzuri Gestión S.L. ·
написана от R.Eugenio · редактирана от екипа на Solo2.