Analýza · 26. května 2026

← Předchozí·Další →

Skutečné versus zdánlivé soukromí: otázky, které je vhodné si položit

Operativní shrnutí cyklu 2: otázky, které odlišují službu s architektonickým soukromím od služby se soukromím deklarativním. Dotazník pro evropského profesionála před přijetím jakéhokoli digitálního nástroje pro citlivá data.

Abychom si rozuměli: Dvě služby se stejným právním upozorněním se mohou chovat velmi odlišně. Jedna chrání technickým návrhem. Druhá chrání smluvním slibem. Rozdíl se nečte v upozornění — objevuje se kladením konkrétních otázek. Kvalita odpovědí vypovídá o produktu stejně jako jejich vlastní obsah.

Rozdíl mezi architektonickým soukromím a deklarativním soukromím

V průběhu sedmi předchozích článků tohoto cyklu jsme prošli různými vrstvami téže věci. Právo mezinárodních přenosů se Schrems II. Matematickou myšlenkou kryptografického hashe, který pečetí každý Cuaderno. Architektonickou volbu kill switche a institucionální zajetí, které ho téměř vždy doprovází. Mechanismus koncového šifrování a operativní otázku, kde se nacházejí klíče. Sladění pobídek podle obchodního modelu. Sebesvrchovanou kryptografickou identitu. Self-hosting jako proporcionální strategii. Každý článek se zabýval jedním úhlem pohledu. Tento, poslední v cyklu, je spojuje do dotazníku.

Rozlišení, které je vhodné si zapamatovat, je jednoduché: existují služby, jejichž soukromí je *architektonické*, a existují služby, jejichž soukromí je *deklarativní*. První je zabudováno do technického návrhu: jistá porušení závazku k soukromí jsou technicky obtížná nebo nemožná, protože architektura je nedovoluje. Druhé je uloženo v textu právního upozornění: jistá porušení by byla smluvně postižitelná, pokud by k nim došlo, ale technicky jim nic nebrání. Oba modely mohou splňovat GDPR; ale jeden chrání svou konstrukcí a druhý chrání slibem, a ten rozdíl je operativně obrovský.

Otázky, které následují, jsou navrženy tak, aby odlišily jeden případ od druhého. Nejsou to pokročilé technické otázky. Jsou to otázky, na které každý poctivý poskytovatel dokáže odpovědět ve své veřejné dokumentaci. Kvalita a přesnost odpovědi vypovídá o produktu stejně jako odpověď sama. Otázky se sdružují do šesti vrstev; je vhodné položit je všechny před přijetím služby pro citlivá data, nejen ty, které identifikuje první instinkt.

Vrstva 1: architektura

Ujasněme si jeden pojem, než budeme pokračovat. *Operátorem* rozumíme společnost poskytující službu: subjekt ovládající servery a software, nikoli konkrétní osobu. Po tomto upřesnění zní základní architektonická otázka: co dělá operátor s obsahem mezi odesílatelem a příjemcem? Možné odpovědi jsou tři a vyplatí se je umět rozlišit, protože všechny tři se někdy propagují podobným slovníkem.

- První: obsah prochází serverem operátora v otevřené podobě, kde ho operátor může číst, i kdyby slíbil, že tak neučiní.
- Druhá: obsah prochází serverem operátora šifrovaný, kde ho operátor nemůže číst, pokud klíče sídlí výhradně v zařízeních uživatelů.

- Třetí: obsah neprochází žádným serverem operátora, protože v tomto konkrétním toku žádný server operátora neexistuje.

Rozdíl mezi těmito třemi není rozdílem stupně: je rozdílem druhu.

Doplňující otázkou — již položenou v Cuaderno o šifrování — je: kdo má kryptografické klíče umožňující číst obsah? Má-li je uživatel a pouze uživatel, je šifrování skutečné. Má-li je navíc operátor v jakékoli podobě — byť pod názvem „obnova účtu" nebo „synchronizace mezi zařízeními" —, je šifrování nominální. Otázka nepřipouští poctivou mezilehlou odpověď.

Vrstva 2: obchodní model

Otázka obchodního modelu je stejně důležitá jako otázka architektonická, a to ze stejného podstatného důvodu: pobídky v průběhu času produkují systematicky odlišné produkty i při totožných deklarovaných záměrech. Jak operátor dnes vydělává peníze? Jeden zdroj, dva, směs? Pokud financování zahrnuje reklamu nebo monetizaci dat, jaká data se monetizují a na jakém právním základě GDPR se tak děje? Pokrývá účel deklarovaný v právním upozornění data třetích osob, která profesionál hodlá službě svěřit?

A otázka druhého řádu, ne vždy položená: jaká je finanční situace operátora v horizontu tří až pěti let? Firma ve fázi rizikového kapitálu funguje pod jinými tlaky než firma se stabilní ziskovostí. Změna modelu financování je opakovaně okamžikem, kdy se implicitní smlouva s uživateli přepíše bez vyjednávání.

Vrstva 3: jurisdikce

Pro evropského profesionála není otázka jurisdikce řečnická. V jaké jurisdikci je operátor zapsán? Ve které zemi se fyzicky nacházejí servery zpracovávající data? Je odpověď na obě předchozí otázky stejná, nebo odlišná, a pokud se liší, jaké právo se uplatní? Evropský region provozovaný americkou firmou není pro účely Schrems II evropskou odpovědí: firma podléhá FISA 702 bez ohledu na to, kde se servery nacházejí.

Doplňující operativní otázkou je: kdyby zítra přišel zpravodajský příkaz platný v jurisdikci operátora požadující vydání mých dat nebo dat mých klientů, co by se stalo? Pokud poctivá odpověď začíná slovy „firma by byla povinna je vydat", služba před tímto příkazem nechrání, ať reklama naznačuje cokoli opačného. Pokud poctivá odpověď začíná slovy „firma by je nemohla vydat, protože je nemá v otevřené podobě", služba chrání; a ten rozdíl závisí téměř výhradně na prvních dvou vrstvách, nikoli na kvalitě zásad ochrany soukromí.

Vrstva 4: operátor a kill switch

Jakou technickou schopnost si operátor ponechává k dálkovému pozastavení, zablokování, zrušení nebo zhoršení služby? Otázka není paranoidní: je operativní. Digitální platformy tuto schopnost v posledních letech opakovaně uplatnily, někdy z vlastní iniciativy, jindy na příkaz vlád, jindy po změnách vlastnictví nebo politiky. Pokud schopnost existuje, je vhodné vědět, za jakých smluvně deklarovaných předpokladů se uplatňuje, a ponechat si rezervu pro nedeklarované předpoklady, které praxe posledních let ukázala jako stejně relevantní: nečekaný soudní příkaz, mezinárodní sankce, změna podnikového vedení, akvizice subjektem s jinou politikou.

Sesterskou otázkou je otázka plánu kontinuity: kdyby operátor tuto schopnost uplatnil proti profesionálovi — z jakéhokoli důvodu, oprávněného či nikoli —, jak dlouhá doba provozu by zůstala k dispozici, jaký postup exportu dat existuje a ke kterému alternativnímu poskytovateli by bylo možné migrovat? Pokud odpověď začíná slovy „to by se nemělo stát", není to operativní odpověď; je to slib.

Vrstva 5: identita a přístup

Kdo ovládá přístupové údaje ke službě? Může-li operátor obnovit přístup uživatele bez účasti uživatele — postup obvykle nazývaný „obnova účtu” —, je operátor technicky správcem účtu a může ho rovněž postoupit tomu, kdo o to požádá příslušným postupem. Nemůže-li operátor přístup obnovit, protože identita se kryptograficky nachází v zařízení uživatele, nemůže ji operátor ani postoupit, a to ani na příkaz. Oba způsoby jsou podle kontextu legitimní; ale, znovu, jsou odlišné a je vhodné vědět, který se přijímá.

Co se stane s daty profesionála, pokud profesionál ztratí přístup? Existují mechanismy obnovy — účtu, souboru, relace —, které závisejí na operátorovi? Jsou tyto mechanismy slučitelné s profesní deontologií oboru, pokud je operátor donucen je použít?

Vrstva 6: budoucnost

Tato poslední vrstva bývá opomíjena, protože vyžaduje projekci. Co by se stalo, kdyby službu koupila jiná firma? Téměř všechny akvizice s sebou v následujících měsících nesou revizi podmínek služby. Co by se stalo, kdyby se změnily regulační požadavky? Evropské právo od roku 2022 povinnosti odstranění a blokování zvýšilo, nikoli snížilo. Co by se stalo, kdyby operátor zmizel? Významná část cloudových služeb nemá zdokumentovaný plán odchodu pro scénář ukončení činnosti operátora; profesionál objeví problém, když už není čas se na něj připravit.

Existuje formulace, kterou je vhodné si pro tuto vrstvu zapamatovat: architektury, které méně závisejí na operátorovi, jsou odolnější vůči změnám operátora. Self-hosting v kterékoli ze svých podob, sebesvrchovaná kryptografická identita, komunikace bez serveru uprostřed — to vše snižuje budoucí plochu rizika tím, že snižuje současnou plochu závislosti. Neodstraňuje ji; snižuje ji.

Rozdíl mezi strukturou a slibem

Kdybychom měli celý cyklus vydestilovat do jediné věty, zněla by takto: strukturální odpovědi se udrží, i když se operátor, správa nebo právo změní; odpovědi založené na slibu se udrží, dokud ten, kdo slibuje, může a chce je dodržet. Obě mohou být v okamžiku přijetí správné. Jen jedna z nich se udrží nezávisle na plynutí času a změně okolností.

To neznamená, že každý profesionál musí vyžadovat strukturální odpovědi od všech služeb, které přijímá. Proporcionalita zůstává legitimní: tabulka pro vnitřní účetnictví nepotřebuje tutéž odpověď jako klinická dokumentace pacienta. Znamená to však, že profesionalita spočívá v tom vědět, jaký druh odpovědi byl v každém případě přijat, a vědomě rozhodnout, že tento druh odpovědi je proporcionální konkrétnímu údaji.

Dotazník, uspořádaný

Dvanáct konkrétních otázek, které shrnují cyklus, uspořádaných tak, aby odpověď na každou z nich utvářela tu následující:

1. Prochází obsah serverem operátora? Pokud prochází: v otevřené podobě, šifrovaný klíči operátora, nebo šifrovaný klíči výhradně uživatele?
2. Pokud se odkazuje na koncové šifrování (end-to-end), kde se nacházejí kryptografické klíče? Zná nebo uchovává operátor jakoukoli jejich část v jakékoli podobě, včetně „obnovy”?
3. Jaká metadata služba generuje a uchovává? Po jak dlouhou dobu? Komu jsou viditelná?
4. Jak se operátor financuje? Pokud financování zahrnuje reklamu nebo monetizaci dat, pokrývá deklarovaný účel data třetích osob svěřená profesionálem?
5. Jaká je finanční situace operátora v horizontu tří až pěti let? Existují faktory naznačující bezprostřední změnu modelu (čekající vstup na burzu, vyčerpávající se kolo financování, pravděpodobná akvizice)?
6. V jaké jurisdikci je operátor zapsán? Ve které zemi se fyzicky nacházejí servery? Pokud se liší, jaké vnitrostátní právo se na zpracování vztahuje?

7. Co by se stalo, kdyby zpravodajský příkaz platný v jurisdikci operátora požadoval vydání mých dat? Mohla by ho firma technicky splnit?
8. Jakou technickou schopnost si operátor ponechává k pozastavení, zablokování nebo zrušení služby? Za jakých smluvních předpokladů? Za jakých nesmluvních, historicky zdokumentovaných předpokladů?
9. Jaký plán odchodu existuje, kdyby operátor tuto schopnost uplatnil proti mně, ať už oprávněně, nebo neoprávněně? Existuje zdokumentovaný postup exportu dat k alternativnímu poskytovateli?
10. Kdo ovládá přístupové údaje? Může je operátor obnovit bez mé účasti? Chrání mě to, nebo mě to vystavuje riziku?
11. Existuje pro tuto konkrétní funkci evropská, self-hostovaná alternativa nebo alternativa bez serveru uprostřed? Jaké jsou její skutečné náklady ve srovnání s vyhodnoceným rizikem?
12. Kdyby dnešní rozhodnutí za pět let zkoumal inspektor, auditor nebo klient zasažený únikem dat, byla by současná volba obhajitelná argumenty dostupnými dnes, nebo by vyžadovala omluvu za to, že nebyly položeny rozumné otázky?

Otázky neočekávají dokonalé odpovědi. Očekávají odpovědi poctivé, které poctivý operátor umí dát a méně poctivý operátor se vyhýbá tomu, aby je přesně formuloval. Operativní rozdíl mezi oběma třídami operátorů, říkáme to bez dramatizování, lze obvykle vnímat při pomalém čtení odpovědí, které poskytují dobrovolně, ještě než je nutné žádat o víc.

Tímto článkem uzavíráme druhý cyklus Cuadernos Lacre. Začali jsme redakčním dluhem zděděným po Schrems II a končíme operativním dotazníkem. Cestou jsme prošli pojmy — hash, šifrování, identita — i aplikovanými rozbory — kill switch, obchodní model, self-hosting. Deklarovaným redakčním záměrem publikace nebylo zahltit čtenáře vyčerpávajícím seznamem problémů, ale předat mu nástroje, aby u jakékoli nové služby rozlišil, jaký druh odpovědi přijímá. Toto rozlišení — mezi architekturou a slibem — je oním nástrojem. Zbytek každý profesionál vloží do služby těm datům, která ve své praxi uzná za hodná té otázky.

Zdroje a další čtení

- Tato publikace, cyklus 2 (květen 2026) — *Schrems II pět let poté*, *Co je SHA-256 doopravdy*, *Kill switch a institucionální zajetí*, *Koncové šifrování vysvětlené doopravdy*, *Obchodní model jako signál důvěry*, *24 slov: co je kryptografická identita*, *Self-hosting jako profesní praxe*. Sedm článků, na nichž tento dotazník spočívá.
- Nařízení (EU) 2016/679 — Obecné nařízení o ochraně osobních údajů. Referenční právní rámec pro všechny otázky, které dotazník klade, zejména články 5, 6, 25, 28, 32, 33 a kapitola V.
- Evropský sbor pro ochranu osobních údajů — pokyny a operativní stanoviska k Schrems II, mezinárodním přenosům, posouzením vlivu a proaktivní odpovědnosti (publikace 2020–2024).
- Španělský úřad pro ochranu osobních údajů — sankce zveřejněné v letech 2022–2024 vůči správcům za nevhodné nástroje přenosu nebo za formální posouzení vlivu bez věcného obsahu.
- noyb.eu — Evropské centrum pro digitální práva, vedené Maximilianem Schremsem. Veřejné úložiště stížností, opravných prostředků a analýz o skutečném, nikoli zdánlivém dodržování evropských norem ochrany osobních údajů.

← PředchozíSelf-hosting jako profesionální praxeDalší →Co podpis nemůže napravit

Nedávné čtení

- Zamyšlení · 29. června 2026 Nejste anonymní
- Zamyšlení · 27. května 2026 Co podpis nemůže napravit
- Analýza · 25. května 2026 Self-hosting jako profesionální praxe

Vezměte si tento článek tam, kam potřebujete.

↓ Markdown ↓ Prostý text ↓ PDF

Soubor se stáhne do vašeho zařízení. Odtud si jej můžete uložit, importovat do Solo2 nebo sdílet, kdekoli chcete. Cuadernos za vás o cíli nerozhoduje.

Pečeť · SHA-256 91a9c297fef12f5c5ea22a7aded92ba36350fba8758e31423a53bdcaca488822

Cuadernos Lacre · Publikace Menzuri Gestión S.L. ·
napsal R.Eugenio · rediguje tým Solo2.