Analiza · 26. maj 2026

← Prejšnji·Naslednji →

Resnična proti navidezni zasebnosti: vprašanja, ki si jih je vredno zastaviti

Operativni povzetek 2. cikla: vprašanja, ki razlikujejo storitev z arhitekturno zasebnostjo od storitve z deklarativno zasebnostjo. Vprašalnik za evropskega strokovnjaka pred sprejetjem katerega koli digitalnega orodja za občutljive podatke.

Da se razumemo: Dve storitvi z enakim pravnim obvestilom se lahko obnašata zelo različno. Ena ščiti s tehnično zasnovo. Druga ščiti s pogodbeno obljubo. Razlike ne preberemo v obvestilu — odkrijemo jo z zastavljanjem konkretnih vprašanj. Kakovost odgovorov pove o izdelku prav toliko kot njihova lastna vsebina.

Razlika med arhitekturno zasebnostjo in deklarativno zasebnostjo

Skozi prejšnjih sedem člankov tega cikla smo prečkali različne plasti iste zadeve. Pravo mednarodnih prenosov s Schrems II. Matematično idejo kriptografske zgoščene vrednosti, ki zapečati vsak Cuaderno. Arhitekturno izbiro kill switcha in institucionalni zajem, ki ga skoraj vedno spremlja. Mehanizem šifriranja od konca do konca in operativno vprašanje, kje se nahajajo ključi. Uskladitev spodbud glede na poslovni model. Samosuvereno kriptografsko identiteto. Self-hosting kot sorazmerno strategijo. Vsak članek se je ukvarjal z enim zornim kotom. Ta, zadnji v ciklu, jih združuje v vprašalnik.

Razlikovanje, ki si ga je vredno zapomniti, je preprosto: obstajajo storitve, katerih zasebnost je *arhitekturna*, in obstajajo storitve, katerih zasebnost je *deklarativna*. Prva je vgrajena v tehnično zasnovo: nekatere kršitve zaveze k zasebnosti so tehnično težke ali nemogoče, ker jih arhitektura ne dopušča. Druga je položena v besedilo pravnega obvestila: nekatere kršitve bi bile pogodbeno sankcionirane, če bi se zgodile, vendar jih tehnično nič ne preprečuje. Oba modela lahko izpolnjujeta GDPR; toda eden ščiti po zasnovi, drugi pa ščiti z obljubo, in razlika je operativno ogromna.

Vprašanja, ki sledijo, so zasnovana tako, da razlikujejo en primer od drugega. Niso napredna tehnična vprašanja. So vprašanja, na katera lahko vsak pošten ponudnik odgovori v svoji javni dokumentaciji. Kakovost in natančnost odgovora pove o izdelku prav toliko kot odgovor sam. Vprašanja se združujejo v šest plasti; vredno jih je zastaviti vsa pred sprejetjem storitve za občutljive podatke, ne le tistih, ki jih prepozna prvi nagib.

1. plast: arhitektura

Pred nadaljevanjem opredelimo en pojem. Z *operaterjem* mislimo podjetje, ki opravlja storitev: subjekt, ki nadzoruje strežnike in programsko opremo, ne posameznika. Ko je to pojasnjeno, je temeljno arhitekturno vprašanje: kaj operater počne z vsebino med pošiljateljem in prejemnikom? Možni so trije odgovori in dobro jih je znati razlikovati, saj vse tri včasih oglašujejo s podobnim besediščem.

- Prvi: vsebina poteka skozi operaterjev strežnik v odprti obliki, kjer jo operater lahko bere, čeprav obljubi, da tega ne bo storil.
- Drugi: vsebina poteka skozi operaterjev strežnik šifrirana, kjer je operater ne more brati, če ključi prebivajo izključno v napravah uporabnikov.

- Tretji: vsebina ne poteka skozi noben operaterjev strežnik, ker v tem konkretnem toku operaterjev strežnik ne obstaja.

Razlika med temi tremi ni razlika v stopnji: je razlika v vrsti.

Dopolnilno vprašanje — že zastavljeno v Cuaderno o šifriranju — je: kdo ima kriptografske ključe, ki omogočajo branje vsebine? Če jih ima uporabnik in samo uporabnik, je šifriranje resnično. Če jih ima poleg tega operater v kakršni koli obliki — pa čeprav pod imenom „obnova računa" ali „sinhronizacija med napravami" —, je šifriranje nominalno. Vprašanje ne dopušča poštenega vmesnega odgovora.

2. plast: poslovni model

Vprašanje o poslovnem modelu je prav tako pomembno kot arhitekturno vprašanje, in to iz istega bistvenega razloga: spodbude skozi čas proizvajajo sistematično različne izdelke tudi ob enakih deklariranih namenih. Kako operater danes služi denar? En vir, dva, mešanica? Če financiranje vključuje oglaševanje ali monetizacijo podatkov, kateri podatki se monetizirajo in na kateri pravni podlagi GDPR se to počne? Ali namen, deklariran v pravnem obvestilu, zajema podatke tretjih oseb, ki jih namerava strokovnjak zaupati storitvi?

In vprašanje drugega reda, ki ni vedno zastavljeno: kakšen je finančni položaj operaterja v obdobju treh do petih let? Podjetje v fazi tveganega kapitala deluje pod drugačnimi pritiski kot podjetje s stabilno donosnostjo. Sprememba modela financiranja je vedno znova trenutek, ko se implicitna pogodba z uporabniki napiše na novo brez pogajanj.

3. plast: jurisdikcija

Za evropskega strokovnjaka vprašanje jurisdikcije ni retorično. V kateri jurisdikciji je operater registriran? V kateri državi se fizično nahajajo strežniki, ki obdelujejo podatke? Ali je odgovor na obe prejšnji vprašanji isti ali različen, in če se razlikuje, katera zakonodaja velja? Evropska regija, ki jo upravlja ameriško podjetje, za namene Schrems II ni evropski odgovor: podjetje je podvrženo FISA 702 ne glede na to, kje se strežniki nahajajo.

Dopolnilno operativno vprašanje je: če bi jutri prispela obveščevalna odredba, veljavna v jurisdikciji operaterja, ki bi zahtevala izročitev mojih podatkov ali podatkov mojih strank, kaj bi se zgodilo? Če se pošten odgovor začne z „podjetje bi jih bilo dolžno izročiti", storitev pred to odredbo ne ščiti, naj oglaševanje namiguje na nasprotno, kolikor hoče. Če se pošten odgovor začne z „podjetje jih ne bi moglo izročiti, ker jih nima v odprti obliki", storitev ščiti; in razlika je odvisna skoraj v celoti od prvih dveh plasti, ne od kakovosti politike zasebnosti.

4. plast: operater in kill switch

Katero tehnično zmožnost operater ohranja za daljinsko začasno ustavitev, blokiranje, odstranitev ali poslabšanje storitve? Vprašanje ni paranoično: je operativno. Digitalne platforme so to zmožnost v zadnjih letih večkrat uveljavile, včasih na lastno pobudo, drugič po odredbi vlad, spet drugič po spremembah lastništva ali politike. Če zmožnost obstaja, je vredno vedeti, pod katerimi pogodbeno deklariranimi predpostavkami se uveljavlja, in si pridržati rezervo za nedeklarirane predpostavke, ki jih je praksa zadnjih let pokazala kot enako pomembne: nepričakovana sodna odredba, mednarodna sankcija, sprememba korporativnega upravljanja, prevzem s strani subjekta z drugačno politiko.

Sestrsko vprašanje je vprašanje načrta neprekinjenega delovanja: če bi operater to zmožnost uveljavil proti strokovnjaku — iz kakršnega koli razloga, upravičenega ali ne —, koliko časa delovanja bi ostalo na voljo, kakšen postopek izvoza podatkov obstaja in h kateremu alternativnemu ponudniku bi bilo mogoče preseliti? Če se odgovor začne z „to se ne bi smelo zgoditi", to ni operativni odgovor; to je obljuba.

5. plast: identiteta in dostop

Kdo nadzira poverilnice za dostop do storitve? Če operater lahko ponovno vzpostavi dostop uporabnika brez udeležbe uporabnika — postopek, ki se običajno imenuje „obnova računa” —, je operater tehnično skrbnik računa in ga lahko tudi odstopi tistemu, ki to zahteva po ustreznem postopku. Če operater ne more ponovno vzpostaviti dostopa, ker identiteta kriptografsko prebiva v uporabnikovi napravi, je operater tudi ne more odstopiti, niti po odredbi. Oba načina sta glede na kontekst legitimna; toda, še enkrat, sta različna in vredno je vedeti, kateri se sprejema.

Kaj se zgodi s podatki strokovnjaka, če strokovnjak izgubi dostop? Ali obstajajo mehanizmi obnove — računa, datoteke, seje —, ki so odvisni od operaterja? Ali so ti mehanizmi združljivi s poklicno deontologijo panoge, če je operater prisiljen, da jih uporabi?

6. plast: prihodnost

Ta zadnja plast se pogosto zanemarja, ker zahteva projekcijo. Kaj bi se zgodilo, če bi storitev prevzelo drugo podjetje? Skoraj vsi prevzemi s seboj v naslednjih mesecih prinašajo revizijo pogojev storitve. Kaj bi se zgodilo, če bi se regulativne zahteve spremenile? Evropsko pravo je od leta 2022 obveznosti odstranjevanja in blokiranja povečalo, ne zmanjšalo. Kaj bi se zgodilo, če bi operater izginil? Pomemben del oblačnih storitev nima dokumentiranega izhodnega načrta za scenarij prenehanja delovanja operaterja; strokovnjak odkrije težavo, ko ni več časa, da bi se nanjo pripravil.

Obstaja formulacija, ki si jo je za to plast vredno zapomniti: arhitekture, ki so manj odvisne od operaterja, so odpornejše proti spremembam operaterja. Self-hosting v kateri koli od svojih oblik, samosuverena kriptografska identiteta, komunikacija brez vmesnega strežnika — vse to zmanjšuje prihodnjo površino tveganja s postopkom zmanjševanja sedanje površine odvisnosti. Ne odpravlja je; zmanjšuje jo.

Razlika med strukturo in obljubo

Če bi morali ves cikel zgostiti v en sam stavek, bi se ta glasil: strukturni odgovori se ohranjajo, čeprav se operater, uprava ali zakonodaja spremenijo; odgovori, ki temeljijo na obljubi, se ohranjajo, dokler tisti, ki obljublja, more in želi obljubo držati. Oba sta lahko v trenutku sprejetja pravilna. Le eden od njiju se ohrani neodvisno od poteka časa in spremembe okoliščin.

To ne pomeni, da mora vsak strokovnjak zahtevati strukturne odgovore od vseh storitev, ki jih sprejema. Sorazmernost ostaja legitimna: preglednica za interno računovodstvo ne potrebuje istega odgovora kot zdravstveni karton pacienta. Pomeni pa, da je strokovnost v tem, da veš, kakšno vrsto odgovora si v vsakem primeru sprejel, in da si zavestno odločil, da je ta vrsta odgovora sorazmerna konkretnemu podatku.

Vprašalnik, urejen

Dvanajst konkretnih vprašanj, ki povzemajo cikel, urejenih tako, da odgovor na vsako od njih oblikuje naslednje:

1. Ali vsebina poteka skozi operaterjev strežnik? Če poteka: v odprti obliki, šifrirana z operaterjevimi ključi ali šifrirana s ključi izključno uporabnika?
2. Če se sklicuje na šifriranje od konca do konca (end-to-end), kje se nahajajo kriptografski ključi? Ali operater pozna ali hrani kateri koli njihov del v kateri koli obliki, vključno z „obnovo”?
3. Katere metapodatke storitev ustvarja in hrani? Kako dolgo? Komu so vidni?
4. Kako se operater financira? Če financiranje vključuje oglaševanje ali monetizacijo podatkov, ali deklarirani namen zajema podatke tretjih oseb, ki jih zaupa strokovnjak?
5. Kakšen je finančni položaj operaterja v obdobju treh do petih let? Ali obstajajo dejavniki, ki nakazujejo neposredno spremembo modela (čakajoča uvrstitev na borzo, krog financiranja, ki se izteka, verjeten

prevzem)?
6. V kateri jurisdikciji je operater registriran? V kateri državi se fizično nahajajo strežniki? Če se razlikujeta, katera nacionalna zakonodaja velja za obdelavo?
7. Kaj bi se zgodilo, če bi obveščevalna odredba, veljavna v jurisdikciji operaterja, zahtevala izročitev mojih podatkov? Ali bi jo podjetje lahko tehnično izpolnilo?
8. Katero tehnično zmožnost operater ohranja za začasno ustavitev, blokiranje ali odstranitev storitve? Pod katerimi pogodbenimi predpostavkami? Pod katerimi nepogodbenimi, zgodovinsko dokumentiranimi predpostavkami?
9. Kakšen izhodni načrt obstaja, če bi operater to zmožnost uveljavil proti meni, upravičeno ali neupravičeno? Ali obstaja dokumentiran postopek izvoza podatkov k alternativnemu ponudniku?
10. Kdo nadzira poverilnice za dostop? Ali jih operater lahko ponastavi brez moje udeležbe? Ali me to ščiti ali me izpostavlja?
11. Ali za to konkretno funkcijo obstaja evropska, samostojno gostovana alternativa ali alternativa brez vmesnega strežnika? Kakšen je njen dejanski strošek v primerjavi z ovrednotenim tveganjem?
12. Če bi današnjo odločitev čez pet let preučeval inšpektor, revizor ali stranka, prizadeta zaradi vdora, ali bi bilo sedanjo izbiro mogoče zagovarjati z argumenti, ki so na voljo danes, ali bi zahtevala opravičilo, ker niso bila zastavljena razumna vprašanja?

Vprašanja ne pričakujejo popolnih odgovorov. Pričakujejo poštene odgovore, ki jih pošten operater zna dati, manj pošten operater pa se izogiba njihovi natančni formulaciji. Operativno razliko med obema vrstama operaterjev, povejmo to brez dramatiziranja, je običajno mogoče zaznati ob počasnem branju odgovorov, ki jih ponujajo prostovoljno, še preden je treba prositi za več.

S tem člankom zaključujemo drugi cikel Cuadernos Lacre. Začeli smo z uredniškim dolgom, podedovanim po Schrems II, in končujemo z operativnim vprašalnikom. Po poti smo prečkali pojme — zgoščeno vrednost, šifriranje, identiteto — in uporabne analize — kill switch, poslovni model, self-hosting. Deklarirana uredniška namera publikacije ni bila preplaviti bralca z izčrpnim seznamom težav, temveč mu izročiti orodja, da pri vsaki novi storitvi razloči, kakšno vrsto odgovora sprejema. To razlikovanje — med arhitekturo in obljubo — je tisto orodje. Preostalo bo vsak strokovnjak podredil tistim podatkom, ki jih v svoji praksi šteje za vredne tega vprašanja.

Viri in nadaljnje branje

- Ta publikacija, 2. cikel (maj 2026) — *Schrems II pet let pozneje*, *Kaj je SHA-256 v resnici*, *Kill switch in institucionalni zajem*, *Šifriranje od konca do konca, zares pojasnjeno*, *Poslovni model kot signal zaupanja*, *24 besed: kaj je kriptografska identiteta*, *Self-hosting kot poklicna praksa*. Sedem člankov, na katerih ta vprašalnik temelji.
- Uredba (EU) 2016/679 — Splošna uredba o varstvu podatkov. Referenčni pravni okvir za vsa vprašanja, ki jih vprašalnik zastavlja, zlasti člene 5, 6, 25, 28, 32, 33 in poglavje V.
- Evropski odbor za varstvo podatkov — smernice in operativna mnenja o Schrems II, mednarodnih prenosih, ocenah učinka in proaktivni odgovornosti (objave 2020–2024).
- Španska agencija za varstvo podatkov — sankcije, objavljene v letih 2022–2024 proti upravljavcem za neustrezne instrumente prenosa ali za formalne ocene učinka brez vsebinske vsebine.
- noyb.eu — Evropski center za digitalne pravice, ki ga vodi Maximilian Schrems. Javno odložišče pritožb, pravnih sredstev in analiz o resničnem, ne navideznem spoštovanju evropskih norm varstva podatkov.

← PrejšnjiSelf-hosting kot profesionalna praksaNaslednji →Česa podpis ne more popraviti

Zadnja branja

- Razmislek · 29. junij 2026 Nisi anonimen
- Razmislek · 27. maj 2026 Česa podpis ne more popraviti
- Analiza · 25. maj 2026 Self-hosting kot profesionalna praksa

Vzemite ta članek s seboj, kamor koli ga potrebujete.

↓ Markdown ↓ Navadno besedilo ↓ PDF

Datoteka bo prenesena v vašo napravo. Od tam jo lahko shranite, uvozite v Solo2 ali delite, kjer koli želite. Cuadernos ne odloča o cilju namesto vas.

Voščeni pečat · SHA-256 42f895d216e931a537fe7a1cecc47ea750b5ecba734959870a6c8cc9a0fa5f43

Cuadernos Lacre · Publikacija podjetja Menzuri Gestión S.L. ·
napisal R.Eugenio · uredila ekipa Solo2.