

Tikras vs tariamas privatumas: klausimai, kuriuos verta sau užduoti

Operacinė 2 ciklo sintezė: klausimai, kurie atskiria paslaugą su architektūrine privatumo apsauga nuo paslaugos su deklaratyvia privatumo apsauga. Klausimynas Europos specialistui prieš pasirenkant bet kokį skaitmeninį įrankį jautriems duomenims.

Kad suprastume: Dvi paslaugos su tuo pačiu teisiniu pranešimu gali elgtis labai skirtingai. Viena apsaugo per techninį dizainą. Kita apsaugo per sutartinį pažadą. Skirtumas neperskaitomas pranešime — jis atrandamas užduodant konkrečius klausimus. Atsakymų kokybė apie produktą pasako tiek pat, kiek ir jų turinys.

Skirtumas tarp architektūrinio privatumo ir deklaratyvaus privatumo

Per septynis ankstesnius šio ciklo straipsnius perėjome skirtingus to paties dalyko sluoksnius. Tarptautinių perdavimų teisę su Schrems II. Matematinę kriptografinio hash idėją, kuri užantspauduoja kiekvieną Cuaderno. Architektūrinį kill switch pasirinkimą ir institucinį užvaldymą, kuris jį beveik visada lydi. Ištinio šifravimo mechanizmą ir operacinį klausimą apie tai, kur yra raktai. Paskatų suderinimą pagal verslo modelį. Savarankišką kriptografinę tapatybę. Self-hosting kaip proporcingą strategiją. Kiekvienas straipsnis nagrinėjo vieną kampą. Šis, paskutinis cikle, juos sujungia į klausimyną.

Skirtumas, kurį verta įsiminti, yra paprastas: yra paslaugų, kurių privatumas yra *architektūrinis*, ir yra paslaugų, kurių privatumas yra *deklaratyvus*. Pirmasis yra įmontuotas į techninį dizainą: tam tikri privatumo įsipareigojimo pažeidimai yra techniškai sunkūs ar neįmanomi, nes architektūra jų neleidžia. Antrasis yra įdėtas į teisinio pranešimo tekstą: tam tikri pažeidimai būtų sutartiškai baudžiami, jei įvyktų, bet techniškai niekas jų nestabdo. Abu modeliai gali atitikti BDAR; bet vienas apsaugo per konstrukciją, o kitas apsaugo per pažadą, ir skirtumas operaciniu požiūriu yra milžiniškas.

Toliau pateikti klausimai sukurti tam, kad atskirtų vieną atvejį nuo kito. Tai nėra pažangūs techniniai klausimai. Tai klausimai, į kuriuos bet kuris sąžiningas tiekėjas gali atsakyti savo viešojoje dokumentacijoje. Atsakymo kokybė ir tikslumas apie produktą pasako tiek pat, kiek ir pats atsakymas. Klausimai suskirstyti į šešis sluoksnius; visus juos verta užduoti prieš pasirenkant paslaugą jautriems duomenims, ne tik tuos, kuriuos identifikuoja pirmasis instinktas.

1 sluoksnis: architektūra

Prieš tęsdami, apibrėžkime vieną sąvoką. *Operatoriumi* vadiname įmonę, teikiančią paslaugą: subjektą, kontroliuojantį serverius ir programinę įrangą, o ne konkretų asmenį. Tai išsiaiškinus, pagrindinis architektūrinis klausimas yra: ką operatorius daro su turiniu tarp siuntėjo ir gavėjo? Galimi trys atsakymai ir verta mokėti juos atskirti, nes visi trys kartais reklamuojami panašiais žodžiais.

- Pirmasis: turinys praeina per operatoriaus serverį atviru tekstu, kur operatorius gali jį skaityti, net jei žada to nedaryti.

- Antrasis: turinys praeina per operatoriaus serverį užšifruotas, kur operatorius negali jo skaityti, jei raktai yra išskirtinai naudotojų įrenginiuose.
- Trečiasis: turinys nepraeina per joki operatoriaus serverį, nes tame konkrečiame sraute operatoriaus serverio nėra.

Skirtumas tarp šių trijų nėra laipsnio: jis yra rūšies.

Papildomas klausimas — jau suformuluotas Cuaderno apie šifravimą — yra: kas turi kriptografinius raktus, leidžiančius skaityti turinį? Jei juos turi naudotojas ir tik naudotojas, šifravimas yra tikras. Jei juos bet kokia forma turi ir operatorius — net ir pavadinimu „paskyros atkūrimas“ ar „synchronizavimas tarp įrenginių“ — šifravimas yra nominalus. Klausimas neturi sąžiningo tarpinio atsakymo.

2 sluoksnis: verslo modelis

Klausimas apie verslo modelį svarbus tiek pat, kiek ir architektūrinis klausimas, ir dėl tos pačios esminės priežasties: paskatos laikui bėgant sukuria sistemiškai skirtingus produktus, net ir esant identiškiems deklaruotiems tikslams. Kaip operatorius šiandien uždirba pinigus? Vienas šaltinis, du, mišinys? Jei finansavimas apima reklamą ar duomenų monetizavimą, kokie duomenys monetizuojami ir koku BDAR teisiniu pagrindu tai daroma? Ar teisiniame pranešime deklaruotas tikslas apima trečiųjų šalių duomenis, kuriuos specialistas ketina patikėti paslaugai?

Ir antros eilės klausimas, ne visada suformuluojamas: kokia yra operatoriaus finansinė padėtis trejų ar penkerių metų perspektyvoje? Rizikos kapitalo etape esanti įmonė veikia esant kitokiam spaudimui nei stabilus pelningumo įmonė. Finansavimo modelio pokytis yra, ne kartą, tas momentas, kai numanomas kontraktas su naudotojais perrašomas be derybų.

3 sluoksnis: jurisdikcija

Europos specialistui jurisdikcijos klausimas nėra retorinis. Kokioje jurisdikcijoje operatorius yra registruotas? Kurioje šalyje fiziškai yra serveriai, apdorojantys duomenis? Ar atsakymas į du ankstesnius klausimus yra tas pats, ar skirtingas, ir jei skiriasi, kokia teisė taikoma? Europinis regionas, valdomas JAV įmonės, Schrems II požiūriu nėra europinis atsakymas: įmonei taikoma FISA 702 nepriklausomai nuo to, kur yra serveriai.

Papildomas operacinis klausimas yra: jei rytoj atkeliautų operatoriaus jurisdikcijoje galiojantis žvalgybos nurodymas, reikalaujantis atiduoti mano arba mano klientų duomenis, kas atsitiktų? Jei sąžiningas atsakymas prasideda „įmonė būtų įpareigota juos atiduoti“, paslauga neapsaugo nuo to nurodymo, kad ir ką reklama teigtų priešingai. Jei sąžiningas atsakymas prasideda „įmonė negalėtų jų atiduoti, nes neturi jų atviru tekstu“, paslauga apsaugo; ir skirtumas beveik vien priklauso nuo dviejų pirmųjų sluoksnių, o ne nuo privatumo politikos kokybės.

4 sluoksnis: operatorius ir kill switch

Kokius techninius pajėgumus operatorius išlaiko, kad nuotoliniu būdu sustabdytų, užblokuotų, pašalintų ar pablogintų paslaugą? Klausimas nėra paranojiškas: jis operacinis. Skaitmeninės platformos pastaraisiais metais ne kartą pasinaudojo šiuo pajėgumu — kartais savo iniciatyva, kartais Vyriausybės nurodymu, kartais po nuosavybės ar politikos pokyčių. Jei pajėgumas egzistuoja, verta žinoti, kokiomis sutartiškai deklaruotomis prielaidomis jis naudojamas, ir palikti rezervą nedeklaruotoms prielaidoms, kurias pastarųjų metų praktika parodė esant ne mažiau reikšmingas: netikėtas teismo nurodymas, tarptautinė sankcija, įmonės valdymo pokytis, įsigijimas kitokios politikos subjekto.

Klausimas-sesuo yra apie tęstinumo planą: jei operatorius pasinaudotų pajėgumu prieš specialistą — dėl bet kokios priežasties, teisingos ar ne — kiek veiklos laiko liktų prieinama, kokia duomenų eksporto procedūra

egzistuoja ir prie kokio alternatyvaus tiekėjo būtų galima migruoti? Jei atsakymas prasideda „taip neturėtų atsitikti“, tai nėra operacinis atsakymas; tai pažadas.

5 sluoksnis: tapatybė ir prieiga

Kas valdo prieigos prie paslaugos kredencialus? Jei operatorius gali atstatyti naudotojo prieigą be naudotojo dalyvavimo — procedūra paprastai vadinama „paskyros atkūrimu“ — operatorius techniškai yra paskyros saugotojas ir gali ją perduoti tam, kas to paprašo per atitinkamą procedūrą. Jei operatorius negali atstatyti prieigos, nes tapatybė kriptografiškai yra naudotojo įrenginyje, operatorius taip pat negali jos perduoti, net ir gavęs nurodymą. Abu būdai yra teisėti, priklausomai nuo konteksto; bet, dar kartą, jie skirtingi, ir verta žinoti, kuris pasirenkamas.

Kas atsitiks su specialisto duomenimis, jei specialistas praras prieigą? Ar egzistuoja atkūrimo mechanizmai — paskyros, failo, sesijos — kurie priklauso nuo operatoriaus? Ar tie mechanizmai suderinami su sektoriaus profesine deontologija, jei operatorius būtų priverstas jais pasinaudoti?

6 sluoksnis: ateitis

Šis paskutinis sluoksnis dažnai apleidžiamas, nes reikalauja projekcijos. Kas atsitiktų, jei paslaugą įsigytų kita įmonė? Beveik visus įsigijimus per ateinančius mėnesius lydi paslaugos sąlygų peržiūra. Kas atsitiktų, jei reguliaciniai reikalavimai pasikeistų? Europos teisė nuo 2022 m. padidino pašalinimo ir blokavimo pareigas, o ne jas sumažino. Kas atsitiktų, jei operatorius išnyktų? Reikšminga dalis debesijos paslaugų neturi dokumentuoto pasitraukimo plano operatoriaus uždarymo scenarijui; specialistas problemą atranda, kai paruošti jai jau nebėra laiko.

Šiam sluoksniui verta įsiminti vieną formuluotę: architektūros, kurios mažiau priklauso nuo operatoriaus, yra atsparesnės operatoriaus pokyčiams. Self-hosting bet kuria iš jo formų, savarankiška kriptografinė tapatybė, serverio tarpe neturinčios komunikacijos — visa tai mažina būsimą rizikos paviršių mažindamos esamą priklausomybės paviršių. Jo nepanaikina; jį sumažina.

Skirtumas tarp struktūros ir pažado

Jei tektų šį ciklą sutraukti į vieną sakinį, jis būtų toks: struktūriniai atsakymai išlieka, net jei operatorius, administracija ar teisės aktai pasikeičia; pažadu pagrįsti atsakymai išlieka tol, kol pažadą davęs gali ir nori jį išlaikyti. Abu gali būti teisingi priėmimo momentu. Tačiau tik vienas iš jų išsilaiko nepriklausomai nuo laiko tėkmės ir aplinkybių pokyčio.

Tai nereiškia, kad kiekvienas specialistas turi reikalauti struktūrinių atsakymų iš visų pasirenkamų paslaugų. Proporcingumas tebėra teisėtas: vidaus buhalterijos skaičiuoklei nereikia to paties atsakymo kaip paciento klinikinei bylai. Tai reiškia, kad profesionalumas yra žinoti, kokio tipo atsakymas buvo priimtas kiekvienu atveju, ir sąmoningai nuspręsti, kad tas atsakymo tipas yra proporcingas konkrečiam duomeniui.

Klausimynas, sudėliotas iš eilės

Dvylika konkrečių klausimų, kurie sintezuoja ciklą, sudėliotų taip, kad atsakymas į kiekvieną informuotų kitą:

1. Ar turinys praeina per operatoriaus serverį? Jei praeina: atviru tekstu, užšifruotas operatoriaus raktais ar užšifruotas išskirtinai naudotojo raktais?
2. Jei remiamasi ištisiniu šifravimu, kur yra kriptografiniai raktai? Ar operatorius žino ar saugo bet kokią jų dalį bet kokia forma, įskaitant „atkūrimą“?
3. Kokius metaduomenis paslauga generuoja ir saugo? Kiek laiko? Kam jie matomi?

4. Kaip operatorius finansuojamas? Jei finansavimas apima reklamą ar duomenų monetizavimą, ar deklaruotas tikslas apima trečiųjų šalių duomenis, kuriuos specialistas patikėjo?
5. Kokia yra operatoriaus finansinė padėtis trejų ar penkerių metų perspektyvoje? Ar yra veiksmų, kurie rodytų neišvengiamą modelio pokytį (laukiantis išėjimas į biržą, besibaigiantis finansavimo etapas, tikėtinas įsigijimas)?
6. Kokioje jurisdikcijoje operatorius yra registruotas? Kurioje šalyje fiziškai yra serveriai? Jei jos skiriasi, kokia nacionalinė teisė taikoma tvarkymui?
7. Kas atsitiktų, jei operatoriaus jurisdikcijoje galiojantis žvalgybos nurodymas pareikalautų atiduoti mano duomenis? Ar įmonė galėtų jį techniškai įvykdyti?
8. Kokius techninius pajėgumus operatorius išlaiko, kad sustabdytų, užblokuotų ar pašalintų paslaugą? Kokiomis sutartinėmis prielaidomis? Kokiomis istoriškai dokumentuotomis nesutartinėmis prielaidomis?
9. Koks pasitraukimo planas egzistuoja, jei operatorius pasinaudotų tuo pajėgumu prieš mane, teisingai ar neteisingai? Ar yra dokumentuota duomenų eksporto pas alternatyvų tiekėją procedūra?
10. Kas valdo prieigos kredencialus? Ar operatorius gali juos atstatyti be mano dalyvavimo? Ar tai mane apsaugo, ar atskleidžia?
11. Ar šiai konkrečiai funkcijai egzistuoja europinė, savarankiškai talpinama ar serverio tarpe neturinti alternatyva? Kokia jos tikroji kaina, palyginti su įvertinta rizika?
12. Jei šiandienos sprendimą po penkerių metų nagrinėtų inspektorius, auditorius ar klientas, nukentėjęs nuo pažeidimo, ar dabartinis pasirinkimas būtų pagrindžiamas šiandien turimais argumentais, ar reikėtų atsiprašyti, kad neuždavėte pagrįstų klausimų?

Klausimai nelaukia tobulų atsakymų. Jie laukia sąžiningų atsakymų, kuriuos sąžiningas operatorius moka pateikti, o mažiau sąžiningas operatorius vengia tiksliai suformuluoti. Operacinis skirtumas tarp dviejų operatorių klasių, sakome tai be dramatisms, paprastai pastebimas lėtai skaitant atsakymus, kuriuos jie pateikia savanoriškai, dar net neprireikus prašyti daugiau.

Šiuo straipsniu užbaigiame antrąjį Cuadernos Lacre ciklą. Pradėjome nuo redakcinio įsipareigojimo, paveldėto iš Schrems II, ir baigiame operaciniu klausimynu. Pakeliui perėjome sąvokas — hash, šifravimą, tapatybę — ir taikomas analizes — kill switch, verslo modelį, self-hosting. Paskelbtas leidinio redakcinis ketinimas buvo ne užgriūti skaitytoją išsamiumi problemų sąrašu, o suteikti jam įrankius, kad jis, susidūręs su bet kokia nauja paslauga, atskirtų, kokio pobūdžio atsakymą priima. Tas atskyrimas — tarp architektūros ir pažado — ir yra įrankis. Visa kita kiekvienas specialistas pritaikys tų duomenų labui, kuriuos savo praktikoje laiko vertais šio klausimo.

Šaltiniai ir papildomas skaitymas

- Šis leidinys, 2 ciklas (2026 m. gegužė) — Schrems II, praėjus penkeriems metams, Kas iš tikrųjų yra SHA-256, Kill switch ir institucinis užvaldymas, Išsisinis šifravimas, paaiškinta tikrai, Verslo modelis kaip pasitikėjimo ženklas, 24 žodžiai: kas yra kriptografinė tapatybė, Self-hosting kaip profesinė praktika. Septyni straipsniai, ant kurių remiasi šis klausimynas.
- Reglamentas (ES) 2016/679 — Bendrasis duomenų apsaugos reglamentas. Atskaitos teisinis pagrindas visiems klausimynas keliamiems klausimams, ypač 5, 6, 25, 28, 32, 33 straipsniams ir V skyriui.
- Europos duomenų apsaugos valdyba — operacinės gairės ir nuomonės dėl Schrems II, tarptautinių perdavimų, poveikio vertinimų ir proaktyvios atsakomybės (2020–2024 m. publikacijos).
- Ispanijos duomenų apsaugos agentūra — 2022–2024 m. paskelbtos sankcijos duomenų valdytojams už netinkamus perdavimo instrumentus arba už formalius poveikio vertinimus be esminio turinio.
- noyb.eu — Europos skaitmeninių teisių centras, vadovaujamas Maximilian Schrems. Viešas skundų, apeliacijų ir analizių apie tikrą, o ne tariamą Europos duomenų apsaugos normų laikymąsi saugykla.

[← Ankstesnis Self-hosting kaip profesinė praktika](#) [Kitas → Ko parašas negali ištaisyti](#)

Naujausi skaitiniai

- [Apmąstymas · 2026 m. birželio 29 d. Jūs nesate anonimiškas](#)
- [Refleksija · 2026 m. gegužės 27 d. Ko parašas negali ištaisyti](#)
- [Analizė · 2026 m. gegužės 25 d. Self-hosting kaip profesinė praktika](#)

Pasiimkite šį straipsnį su savimi ten, kur jums reikia.

[↓ Markdown](#) [↓ Paprastas tekstas](#) [↓ PDF](#)

Failas bus atsisiųstas į jūsų įrenginį. Iš ten galite jį išsaugoti, importuoti į Solo2 arba bendrinti bet kur. Cuadernos nusprendžia ne jūsų naudai dėl paskirties vietos.

Vaško antspaudas · SHA-256 bdc07296033e5fad297f9910696b6d14b7f3b489df4f046a25b27a72ae21c927

[Funkcijos](#) [Naujienos](#) [Tinklaraštis](#) [Pagalba](#) [Apie mus](#) [Kontaktai](#)
[Skaidrumas](#) [Tikrinimas](#) [Privatumas](#) [Sąlygos](#) [Slapukai](#)

Cuadernos Lacre · [Menzuri Gestión S.L.](#) leidinys ·
parašė R.Eugenio · redagavo [Solo2](#) komanda.

Ši svetainė nenaudoja slapukų. Viskas, ką įkelia jūsų naršyklė, yra mūsų parašyta arba prižiūrima ir priglobta mūsų Europos serveriuose: anoniminis lankytojų skaitiklis („Umami“, savarankiškai priglobtas) ir minimalus „JavaScript“, reikalingas kalbos pasirinkimui ir jūsų šviesios/tamsios temos nustatymui, kuris išsaugomas jūsų pačių įrenginyje. Be trečiųjų šalių išteklių, be seklių, be profiliavimo, be dalijimosi duomenimis. Jei norite mus sekti: [RSS](#).