Analüüs · 26. mai 2026

← Eelmine·Järgmine →

# Tõeline vs näiline privaatsus: küsimused, mida tasub endalt küsida

Teise tsükli operatiivne kokkuvõte: küsimused, mis eristavad arhitektuurilise privaatsusega teenust deklaratiivse privaatsusega teenusest. Küsimustik Euroopa spetsialistile enne mis tahes digitaalse tööriista kasutuselevõttu tundlike andmete jaoks.

**Selguse mõttes:** Kaks teenust, millel on samad kasutustingimused, võivad käituda väga erinevalt. Üks kaitseb tehnilise disaini kaudu. Teine kaitseb lepingulise lubaduse kaudu. Erinevust ei loe tingimustest — see avastatakse konkreetseid küsimusi esitades. Vastuste kvaliteet ütleb toote kohta sama palju kui nende oma sisu.

## Erinevus arhitektuurilise ja deklaratiivse privaatsuse vahel

Selle tsükli seitsme eelmise artikli jooksul oleme läbinud sama teema erinevad kihid. Rahvusvaheliste edastuste õigus Schrems II kaudu. Krüptograafilise räsi matemaatiline idee, mis pitseerib iga Cuaderno. Kill switchi arhitektuuriline valik ja institutsionaalne hõivamine, mis sellega peaaegu alati kaasneb. Otsast lõpuni krüpteerimise mehhanism ja operatiivne küsimus selle kohta, kus võtmed asuvad. Stiimulite joondumine ärimudeli järgi. Isemajandav krüptograafiline identiteet. Self-hosting kui proportsionaalne strateegia. Iga artikkel käsitles üht nurka. See, tsükli viimane, koondab need küsimustikuks.

Eristus, mida tasub meeles pidada, on lihtne: on teenuseid, mille privaatsus on *arhitektuuriline*, ja on teenuseid, mille privaatsus on *deklaratiivne*. Esimene on sisse ehitatud tehnilisse disaini: teatud privaatsuskohustuse rikkumised on tehniliselt rasked või võimatud, sest arhitektuur ei luba neid. Teine on talletatud kasutustingimuste teksti: teatud rikkumised oleksid lepinguliselt karistatavad, kui need aset leiavad, kuid tehniliselt ei takista neid miski. Mõlemad mudelid võivad GDPR-i täita; kuid üks kaitseb konstruktsiooni kaudu ja teine lubaduse kaudu, ja erinevus on operatiivselt tohutu.

Järgnevad küsimused on kavandatud ühe juhtumi teisest eristamiseks. Need ei ole edasijõudnud tehnilised küsimused. Need on küsimused, millele iga aus teenusepakkuja saab oma avalikus dokumentatsioonis vastata. Vastuse kvaliteet ja täpsus ütleb toote kohta sama palju kui vastus ise. Küsimused rühmitatakse kuude kihti; kõik need tasub esitada enne teenuse kasutuselevõttu tundlike andmete jaoks, mitte ainult neid, mille esimene instinkt tuvastab.

## Kiht 1: arhitektuur

Fikseerime enne jätkamist ühe mõiste. *Operaatori* all mõtleme ettevõtet, kes teenust osutab: üksust, kes kontrollib servereid ja tarkvara, mitte konkreetset isikut. Seda täpsustades on põhiline arhitektuuriline küsimus: mida teeb operaator saatja ja saaja vahelise sisuga? Võimalikke vastuseid on kolm ja neid tasub osata eristada, sest kõiki kolme reklaamitakse mõnikord sarnase sõnavaraga.

- Esimene: sisu läbib operaatori serveri avatekstina, kus operaator saab seda lugeda, ehkki ta lubab mitte teha.

- Teine: sisu läbib operaatori serveri krüpteerituna, kus operaator ei saa seda lugeda, kui võtmed asuvad ainult kasutajate seadmetes.
- Kolmas: sisu ei läbi ühtegi operaatori serverit, sest selles konkreetses voos ei ole operaatori serverit.

Erinevus nende kolme vahel ei ole astme erinevus: see on tüübi erinevus.

Täiendav küsimus —juba sõnastatud krüpteerimist käsitlevas Cuadernos— on: kellel on krüptograafilised võtmed, mis võimaldavad sisu lugeda? Kui need on kasutajal ja ainult kasutajal, on krüpteerimine tõeline. Kui need on lisaks operaatoril mis tahes kujul —isegi nime all »konto taastamine» või »seadmetevaheline sünkroonimine»—, on krüpteerimine nominaalne. Küsimus ei luba ausat vahepealset vastust.

# Kiht 2: ärimudel

Ärimudeli küsimus on sama oluline kui arhitektuuriline küsimus, ja samal sisulisel põhjusel: stiimulid toodavad aja jooksul süstemaatiliselt erinevaid tooteid, isegi identsete deklareeritud eesmärkidega. Kuidas operaator täna raha teenib? Üks allikas, kaks, segu? Kui rahastus hõlmab reklaami või andmete rahaks muutmist, milliseid andmeid rahaks muudetakse ja millisel GDPR-i õiguslikul alusel seda tehakse? Kas kasutustingimustes deklareeritud eesmärk katab kolmandate isikute andmed, mida spetsialist kavatseb teenusele usaldada?

Ja teise järgu küsimus, mida alati ei sõnastata: milline on operaatori finantsolukord kolme või viie aasta vaates? Riskikapitali faasis olev ettevõte tegutseb teistsuguse surve all kui stabiilselt kasumlik ettevõte. Rahastusmudeli muutus on korduvalt see hetk, mil kasutajatega sõlmitud kaudne leping kirjutatakse läbirääkimisteta ümber.

# Kiht 3: jurisdiktsioon

Euroopa spetsialistile ei ole jurisdiktsiooni küsimus retooriline. Millises jurisdiktsioonis on operaator registreeritud? Millises riigis asuvad füüsiliselt serverid, mis andmeid töötlevad? Kas vastus kahele eelmisele küsimusele on sama või erinev, ja kui erineb, milline õigusakt kohaldub? USA ettevõtte hallatav Euroopa piirkond ei ole Schrems II mõttes Euroopa vastus: ettevõte allub FISA 702-le sõltumata sellest, kus serverid asuvad.

Täiendav operatiivne küsimus on: kui homme saabuks operaatori jurisdiktsioonis kehtiv luurekorraldus, mis nõuaks minu või mu klientide andmete väljaandmist, mis juhtuks? Kui aus vastus algab sõnadega »ettevõte oleks kohustatud need väljastama», ei kaitse teenus selle korralduse vastu, ükskõik kui palju reklaam vastupidist vihjab. Kui aus vastus algab sõnadega »ettevõte ei saaks neid väljastada, sest tal pole neid avatekstina», siis teenus kaitseb; ja erinevus sõltub peaaegu täielikult kahest esimesest kihist, mitte privaatsuspoliitika kvaliteedist.

# Kiht 4: operaator ja kill switch

Millise tehnilise võime säilitab operaator teenuse peatamiseks, blokeerimiseks, kustutamiseks või eemalt halvendamiseks? Küsimus ei ole paranoiline: see on operatiivne. Digiplatvormid on seda võimet viimastel aastatel korduvalt kasutanud, vahel omal algatusel, vahel valitsuste korralduse alusel, vahel pärast omandi- või poliitikamuutusi. Kui võime on olemas, on hea teada, milliste lepinguliselt deklareeritud eelduste alusel seda kasutatakse, ja jätta varu deklareerimata eeldustele, mille viimaste aastate praktika on näidanud sama olulistena: ootamatu kohtukorraldus, rahvusvaheline sanktsioon, ühingu juhtimise muutus, ülevõtmine teistsuguse poliitikaga üksuse poolt.

Õdekuküsimus puudutab jätkuvuskava: kui operaator kasutaks seda võimet spetsialisti vastu —mis tahes põhjusel, õigustatult või mitte—, kui palju tööaega jääks veel saadavaks, milline andmete ekspordi kord on olemas ja millisele alternatiivsele teenusepakkujale saaks üle minna? Kui vastus algab sõnadega »seda ei tohiks juhtuda», ei ole see operatiivne vastus; see on lubadus.

## Kiht 5: identiteet ja juurdepääs

Kes kontrollib teenuse juurdepääsu mandaate? Kui operaator saab lähtestada kasutaja juurdepääsu ilma kasutaja osaluseta —kord, mida tüüpiliselt nimetatakse »konto taastamiseks»—, on operaator tehniliselt konto hoidja ja saab selle ka loovutada sellele, kes seda asjakohase korra kaudu taotleb. Kui operaator ei saa juurdepääsu lähtestada, sest identiteet asub krüptograafiliselt kasutaja seadmes, ei saa operaator seda ka loovutada, isegi mitte korralduse alusel. Mõlemad viisid on kontekstist olenevalt legitiimsed; kuid taas kord, need on erinevad, ja on hea teada, kumba kasutusele võetakse.

Mis juhtub spetsialisti andmetega, kui spetsialist kaotab juurdepääsu? Kas on olemas taastamismehhanisme — konto, faili, seansi— mis sõltuvad operaatorist? Kas need mehhanismid on kooskõlas sektori kutse-eetikaga, kui operaatorit sunnitakse neid kasutama?

## Kiht 6: tulevik

See viimane kiht jääb sageli tähelepanuta, sest see nõuab ettenägemist. Mis juhtuks, kui teenuse ostaks teine ettevõte? Peaaegu kõigi ülevõtmistega kaasneb järgnevatel kuudel teenusetingimuste ülevaatamine. Mis juhtuks, kui regulatiivsed nõuded muutuksid? Euroopa õigus on alates 2022. aastast suurendanud eemaldamis- ja blokeerimiskohustusi, mitte vähendanud neid. Mis juhtuks, kui operaator kaoks? Märkimisväärsel osal pilveteenustest puudub dokumenteeritud väljumiskava operaatori sulgemise stsenaariumiks; spetsialist avastab probleemi siis, kui selle ettevalmistamiseks pole enam aega.

On üks sõnastus, mida tasub selle kihi puhul meeles pidada: arhitektuurid, mis sõltuvad operaatorist vähem, on operaatori muutuste suhtes vastupidavamad. Self-hosting mis tahes oma vormis, isemajandav krüptograafiline identiteet, ilma vahepealse serverita side, kõik need vähendavad tulevast riskipinda, vähendades praegust sõltuvuspinda. Need ei kõrvalda seda; need vähendavad seda.

## Erinevus struktuuri ja lubaduse vahel

Kui peaksime tsükli ühte lausesse destilleerima, oleks see järgmine: struktuursed vastused püsivad ka siis, kui operaator, haldus või õigusaktid muutuvad; lubadusel põhinevad vastused püsivad seni, kuni lubaja saab ja tahab neid pidada. Mõlemad võivad kasutuselevõtu hetkel olla õiged. Vaid üks neist püsib sõltumata aja kulgemisest ja asjaolude muutumisest.

See ei tähenda, et iga spetsialist peaks nõudma struktuurseid vastuseid kõigilt teenustelt, mida ta kasutusele võtab. Proportsionaalsus jääb legitiimseks: sisemise raamatupidamise arvutustabel ei vaja sama vastust kui patsiendi kliiniline toimik. See tähendab küll, et professionaalsus seisneb teadmises, millist laadi vastuse on igal juhul vastu võtnud, ja selles, et on teadlikult otsustanud, et seda laadi vastus on proportsionaalne konkreetse andmega.

## Küsimustik, korrastatuna

Kaksteist konkreetset küsimust, mis tsükli kokku võtavad, korrastatuna nii, et vastus igaühele annab teavet järgmise jaoks:

1. Kas sisu läbib operaatori serveri? Kui läbib: avatekstina, operaatori võtmetega krüpteerituna või ainult kasutaja võtmetega krüpteerituna?
2. Kui viidatakse otsast lõpuni krüpteerimisele, kus asuvad krüptograafilised võtmed? Kas operaator teab või säilitab mõnda osa neist mis tahes kujul, sealhulgas »taastamisena»?
3. Milliseid metaandmeid teenus loob ja säilitab? Kui kaua? Kellele need on nähtavad?
4. Kuidas operaator end rahastab? Kui rahastus hõlmab reklaami või andmete rahaks muutmist, kas deklareeritud eesmärk katab kolmandate isikute andmed, mille spetsialist on teenusele usaldanud?

5. Milline on operaatori finantsolukord kolme või viie aasta vaates? Kas on tegureid, mis viitavad mudeli peatsele muutusele (ootel börsileminek, ammenduv rahastusvoor, tõenäoline ülevõtmine)?
6. Millises jurisdiktsioonis on operaator registreeritud? Millises riigis asuvad serverid füüsiliselt? Kui need erinevad, milline riiklik õigusakt töötlemisele kohaldub?
7. Mis juhtuks, kui operaatori jurisdiktsioonis kehtiv luurekorraldus nõuaks minu andmete väljaandmist? Kas ettevõte saaks seda tehniliselt täita?
8. Millise tehnilise võime säilitab operaator teenuse peatamiseks, blokeerimiseks või kustutamiseks? Milliste lepinguliste eelduste alusel? Milliste ajalooliselt dokumenteeritud lepinguväliste eelduste alusel?
9. Milline väljumiskava on olemas, kui operaator kasutaks seda võimet minu vastu, õigustatult või õigustamatult? Kas on dokumenteeritud kord andmete eksportimiseks alternatiivsele teenusepakkujale?
10. Kes kontrollib juurdepääsu mandaate? Kas operaator saab need lähtestada ilma minu osaluseta? Kas see kaitseb mind või seab mind ohtu?
11. Kas selle konkreetse funktsiooni jaoks on olemas Euroopa, ise majutatud või ilma vahepealse serverita alternatiiv? Milline on selle tegelik kulu võrreldes hinnatud riskiga?
12. Kui tänast otsust uuriks viie aasta pärast inspektor, audiitor või rikkumisest mõjutatud klient, kas praegune valik oleks kaitstav tänase päeva argumentidega, või nõuaks see vabandust selle eest, et mõistlikke küsimusi ei esitatud?

Küsimused ei oota täiuslikke vastuseid. Need ootavad ausaid vastuseid, mida aus operaator oskab anda ja mida vähem aus operaator väldib täpselt sõnastamast. Operatiivset erinevust nende kahe operaatoritüübi vahel, ütleme seda ilma dramaatikata, märkab tavaliselt aeglaselt lugedes vastuseid, mida nad vabatahtlikult pakuvad, juba enne kui on vaja rohkemat küsida.

---

*Selle artikliga lõpetame Cuadernos Lacre teise tsükli. Alustasime Schrems II-st päritud toimetusliku võlaga ja lõpetame operatiivse küsimustikuga. Teel oleme läbinud mõisteid —räsi, krüpteerimine, identiteet— ja rakenduslikke analüüse —kill switch, ärimudel, self-hosting—. Väljaande deklareeritud toimetuslik kavatsus ei olnud lugejat üle koormata ammendava probleemide loendiga, vaid anda talle tööriistad, et ta eristaks mis tahes uue teenuse ees, millist laadi vastust ta on nõustumas vastu võtma. See eristus —arhitektuuri ja lubaduse vahel— ongi see tööriist. Ülejäänu seab iga spetsialist nende andmete teenistusse, mida ta oma praktikas peab küsimust väärivaks.*

## Allikad ja täiendav lugemine

- See väljaanne, tsükkel 2 (mai 2026) — *Schrems II, viis aastat hiljem*, *Mis SHA-256 tegelikult on*, *Kill switch ja institutsionaalne hõivamine*, *Otsast lõpuni krüpteerimine, päriselt seletatud*, *Ärimudel kui usalduse signaal*, *Need 24 sõna: mis on krüptograafiline identiteet*, *Self-hosting kui professionaalne praktika*. Need seitse artiklit, millele see küsimustik tugineb.
- Määrus (EL) 2016/679 — isikuandmete kaitse üldmäärus. Õiguslik viiteraamistik kõigile küsimustele, mida küsimustik tõstatab, eelkõige artiklid 5, 6, 25, 28, 32, 33 ja V peatükk.
- Euroopa Andmekaitsenõukogu — operatiivsed suunised ja arvamused Schrems II, rahvusvaheliste edastuste, mõjuhinnangute ja proaktiivse vastutuse kohta (väljaanded 2020–2024).
- Hispaania Andmekaitseamet — aastatel 2022–2024 avaldatud sanktsioonid vastutavatele töötlejatele ebapiisavate edastusvahendite või sisuliselt tühjade formaalsete mõjuhinnangute eest.
- noyb.eu — Euroopa Digitaalõiguste Keskus, mida juhib Maximilian Schrems. Avalik hoidla kaebustest, kaebustest ja analüüsidest Euroopa andmekaitse-eeskirjade tegeliku, mitte näilise järgimise kohta.

← EelmineSelf-hosting kui professionaalne praktikaJärgmine →Mida allkiri ei saa parandada

## Viimased lugemised


- Mõtisklus · 29. juuni 2026 Sa ei ole anonüümne
- Refleksioon · 27. mai 2026 Mida allkiri ei saa parandada
- Analüüs · 25. mai 2026 Self-hosting kui professionaalne praktika

Võtke see artikkel endaga kaasa kuhu iganes vaja.

↓ Markdown ↓ Lihttekst ↓ PDF

Fail laaditakse alla teie seadmesse. Sealt saate selle salvestada, importida Solo2-sse või jagada kus iganes soovite. Cuadernos ei otsusta sihtkohta teie eest.

Lakipitsat · SHA-256 0dea1409818484e47a9d73b631e3299deef6023752e0296e4b9c5316dd248db6



Cuadernos Lacre · Ettevõtte Menzuri Gestión S.L. väljaanne ·
kirjutanud R.Eugenio · toimetanud Solo2 meeskond.