Reāls vs šķietams privātums: jautājumi, kurus ir vērts sev uzdot

2. cikla operatīvā sintēze: jautājumi, kas atšķir pakalpojumu ar arhitektonisku privātumu no pakalpojuma ar deklaratīvu privātumu. Anketa Eiropas speciālistam pirms jebkura digitāla rīka pieņemšanas sensitīviem datiem.

Lai saprastos: Divi pakalpojumi ar vienu un to pašu juridisko paziņojumu var uzvesties ļoti atšķirīgi. Viens aizsargā ar tehnisko dizainu. Otrs aizsargā ar līgumisku solījumu. Atšķirība nav nolasāma paziņojumā — tā tiek atklāta, uzdodot konkrētus jautājumus. Atbilžu kvalitāte par produktu pasaka tikpat daudz, cik to saturs.

Atšķirība starp arhitektonisku privātumu un deklaratīvu privātumu

Septiņu iepriekšējo šī cikla rakstu gaitā esam izgājuši cauri dažādiem viena un tā paša jautājuma slāņiem. Starptautisko pārsūtījumu tiesībām ar Schrems II. Kriptogrāfiskā hash matemātiskajai idejai, kas aizzīmogo katru Cuaderno. Arhitektoniskajai kill switch izvēlei un institucionālajai sagrābšanai, kas to gandrīz vienmēr pavada. Galašifrēšanas mehānismam un operatīvajam jautājumam par to, kur atrodas atslēgas. Stimulu saskaņošanai atbilstoši biznesa modelim. Pašsuverēnajai kriptogrāfiskajai identitātei. Self-hosting kā proporcionālai stratēģijai. Katrs raksts aplūkoja vienu rakursu. Šis, pēdējais ciklā, tos apvieno anketā.

Atšķirība, kuru ir vērts paturēt prātā, ir vienkārša: ir pakalpojumi, kuru privātums ir *arhitektonisks*, un ir pakalpojumi, kuru privātums ir *deklaratīvs*. Pirmais ir iestrādāts tehniskajā dizainā: noteikti privātuma saistību pārkāpumi ir tehniski grūti vai neiespējami, jo arhitektūra tos nepieļauj. Otrais ir noguldīts juridiskā paziņojuma tekstā: noteikti pārkāpumi būtu līgumiski sodāmi, ja notiktu, bet tehniski nekas tos nekavē. Abi modeļi var atbilst VDAR; bet viens aizsargā ar konstrukciju, bet otrs aizsargā ar solījumu, un atšķirība operatīvi ir milzīga.

Tālāk sekojošie jautājumi ir izstrādāti, lai atšķirtu vienu gadījumu no otra. Tie nav uzlaboti tehniski jautājumi. Tie ir jautājumi, uz kuriem jebkurš godīgs pakalpojumu sniedzējs var atbildēt savā publiskajā dokumentācijā. Atbildes kvalitāte un precizitāte par produktu pasaka tikpat daudz, cik pati atbilde. Jautājumi ir sagrupēti sešos slāņos; tos visus ir vērts uzdot pirms pakalpojuma pieņemšanas sensitīviem datiem, ne tikai tos, kurus identificē pirmais instinkts.

1. slānis: arhitektūra

Pirms turpinām, nostiprināsim vienu jēdzienu. Ar *operatoru* mēs saprotam uzņēmumu, kas sniedz pakalpojumu: subjektu, kas kontrolē serverus un programmatūru, nevis konkrētu personu. Kad tas ir noskaidrots, galvenais arhitektūras jautājums ir: ko operators dara ar saturu starp sūtītāju un saņēmēju? Iespējamas trīs atbildes, un tās ir vērts prast atšķirt, jo visas trīs reizēm reklamē ar līdzīgu vārdu krājumu.

- Pirmā: saturs iziet caur operatora serveri atklātā tekstā, kur operators var to lasīt, pat ja sola to nedarīt.
- Otrā: saturs iziet caur operatora serveri šifrēts, kur operators nevar to lasīt, ja atslēgas atrodas tikai lietotāju ierīcēs.
- Trešā: saturs neiziet caur nevienu operatora serveri, jo šajā konkrētajā plūsmā operatora servera nav.

Atšķirība starp šīm trim nav pakāpes: tā ir veida.

Papildu jautājums — jau formulēts Cuaderno par šifrēšanu — ir: kuram ir kriptogrāfiskās atslēgas, kas ļauj lasīt saturu? Ja tās ir lietotājam un tikai lietotājam, šifrēšana ir reāla. Ja tās jebkādā formā ir arī operatoram — pat ar nosaukumu „konta atjaunošana“ vai „sinhronizācija starp ierīcēm“ — šifrēšana ir nomināla. Jautājums nepieļauj godīgu starpposma atbildi.

2. slānis: biznesa modelis

Jautājums par biznesa modeli ir tikpat svarīgs kā arhitektoniskais jautājums, un tā paša būtiskā iemesla dēļ: stimuli laika gaitā rada sistemātiski atšķirīgus produktus pat ar identiskiem deklarētiem mērķiem. Kā operators šodien pelna naudu? Viens avots, divi, sajaukums? Ja finansējums ietver reklāmu vai datu monetizāciju, kādi dati tiek monetizēti un uz kāda VDAR juridiskā pamata tas tiek darīts? Vai juridiskajā paziņojumā deklarētais mērķis aptver trešo personu datus, ko speciālists plāno uzticēt pakalpojumam?

Un otrās kārtas jautājums, ne vienmēr formulēts: kāds ir operatora finansiālais stāvoklis trīs vai piecu gadu perspektīvā? Riska kapitāla fāzē esošs uzņēmums darbojas zem cita spiediena nekā stabilas rentabilitātes uzņēmums. Finansēšanas modeļa maiņa atkārtoti ir tas brīdis, kad netiešais līgums ar lietotājiem tiek pārrakstīts bez sarunām.

3. slānis: jurisdikcija

Eiropas speciālistam jurisdikcijas jautājums nav retorisks. Kurā jurisdikcijā operators ir reģistrēts? Kurā valstī fiziski atrodas serveri, kas apstrādā datus? Vai atbilde uz abiem iepriekšējiem jautājumiem ir vienāda vai atšķirīga, un, ja atšķiras, kāds likums attiecas? Eiropas reģions, ko vada ASV uzņēmums, Schrems II nolūkos nav eiropeiska atbilde: uzņēmumam tiek piemērots FISA 702 neatkarīgi no tā, kur atrodas serveri.

Papildu operatīvais jautājums ir: ja rīt pienāktu operatora jurisdikcijā spēkā esošs izlūkošanas rīkojums, kas pieprasa nodot manus vai manu klientu datus, kas notiktu? Ja godīgā atbilde sākas ar „uzņēmumam būtu pienākums tos nodot“, pakalpojums neaizsargā pret šo rīkojumu, lai cik reklāma liktu domāt pretējo. Ja godīgā atbilde sākas ar „uzņēmums tos nevarētu nodot, jo tam tie nav atklātā tekstā“, pakalpojums aizsargā; un atšķirība gandrīz pilnībā ir atkarīga no abiem pirmajiem slāņiem, nevis no privātuma politikas kvalitātes.

4. slānis: operators un kill switch

Kādu tehnisko spēju operators saglabā, lai attālināti apturētu, bloķētu, dzēstu vai pasliktinātu pakalpojumu? Jautājums nav paranojisks: tas ir operatīvs. Digitālās platformas pēdējos gados šo spēju ir izmantojušas atkārtoti — dažkārt pēc pašu iniciatīvas, citreiz pēc valdību rīkojuma, citreiz pēc īpašumtiesību vai politikas maiņas. Ja spēja pastāv, ir vērts zināt, pie kādiem līgumiski deklarētiem pieņēmumiem tā tiek izmantota, un atstāt rezervi nedeklarētiem pieņēmumiem, kurus pēdējo gadu prakse ir parādījusi tikpat būtiskus: negaidīts tiesas rīkojums, starptautiska sankcija, korporatīvās pārvaldības maiņa, iegāde no struktūras ar citu politiku.

Māsas jautājums ir par nepārtrauktības plānu: ja operators izmantotu šo spēju pret speciālistu — jebkāda iemesla dēļ, taisnīga vai ne — cik darbības laika joprojām būtu pieejams, kāda datu eksporta procedūra pastāv un uz kuru alternatīvu pakalpojumu sniedzēju varētu migrēt? Ja atbilde sākas ar „tam nevajadzētu notikt“, tā nav operatīva atbilde; tas ir solījums.

5. slānis: identitāte un piekļuve

Kurš kontrolē piekļuves akreditācijas datus pakalpojumam? Ja operators var atjaunot lietotāja piekļuvi bez lietotāja līdzdalības — procedūra, ko parasti dēvē par „konta atjaunošanu“ — operators tehniski ir konta turētājs un var to arī nodot tam, kurš to pieprasa ar atbilstošu procedūru. Ja operators nevar atjaunot piekļuvi, jo

identitāte kriptogrāfiski atrodas lietotāja ierīcē, operators arī nevar to nodot, pat ne pēc rīkojuma. Abi veidi ir leģitīmi atkarībā no konteksta; bet, atkal, tie ir atšķirīgi, un ir vērts zināt, kuru pieņem.

Kas notiek ar speciālista datiem, ja speciālists zaudē piekļuvi? Vai pastāv atjaunošanas mehānismi — konta, faila, sesijas — kas ir atkarīgi no operatora? Vai šie mehānismi ir saderīgi ar nozares profesionālo deontoloģiju, ja operators tiktu piespiests tos izmantot?

6. slānis: nākotne

Šo pēdējo slāni mēdz atstāt novārtā, jo tas prasa projekciju. Kas notiktu, ja pakalpojumu iegādātos cits uzņēmums? Gandrīz visas iegādes nākamo mēnešu laikā nes līdzi pakalpojuma noteikumu pārskatīšanu. Kas notiktu, ja regulatīvās prasības mainītos? Eiropas tiesības kopš 2022. gada ir palielinājušas izņemšanas un bloķēšanas pienākumus, nevis tos samazinājušas. Kas notiktu, ja operators pazustu? Ievērojama daļa mākoņpakalpojumu nav dokumentēta iziešanas plāna operatora slēgšanas scenārijam; speciālists problēmu atklāj tad, kad sagatavoties tai vairs nav laika.

Šim slānim ir vērts paturēt prātā vienu formulējumu: arhitektūras, kas mazāk atkarīgas no operatora, ir noturīgākas pret operatora izmaiņām. Self-hosting jebkurā no tā veidiem, pašsuverēnā kriptogrāfiskā identitāte, komunikācijas bez servera vidū — tas viss samazina nākotnes riska virsmu, samazinot pašreizējo atkarības virsmu. Tas to nelikvidē; tas to samazina.

Atšķirība starp struktūru un solījumu

Ja mums šis cikls būtu jādestilē vienā teikumā, tas būtu šāds: strukturālās atbildes saglabājas pat tad, ja operators, administrācija vai likumdošana mainās; solījuma atbildes saglabājas, kamēr tas, kurš sola, var un grib tās uzturēt. Abas var būt pareizas pieņemšanas brīdī. Tikai viena no tām noturas neatkarīgi no laika gaitas un apstākļu maiņas.

Tas nenozīmē, ka katram speciālistam jāprasa strukturālas atbildes no visiem pakalpojumiem, ko viņš pieņem. Proporcionalitāte joprojām ir leģitīma: iekšējās grāmatvedības izklājlapai nav vajadzīga tā pati atbilde kā pacienta klīniskajai lietai. Tas gan nozīmē, ka profesionalitāte ir zināt, kāda veida atbilde katrā gadījumā ir pieņemta, un apzināti būt izlēmušam, ka šī veida atbilde ir proporcionāla konkrētajam datam.

Anketa, sakārtota pēc kārtas

Divpadsmit konkrēti jautājumi, kas sintezē ciklu, sakārtoti tā, lai atbilde uz katru no tiem informētu nākamo:

1. Vai saturs iziet caur operatora serveri? Ja iziet: atklātā tekstā, šifrēts ar operatora atslēgām vai šifrēts ar atslēgām, kas pieder tikai lietotājam?
2. Ja tiek minēta galašifrēšana, kur atrodas kriptogrāfiskās atslēgas? Vai operators zina vai glabā kādu to daļu jebkādā formā, ieskaitot „atjaunošanu“?
3. Kādus metadatus pakalpojums ģenerē un glabā? Cik ilgi? Kam tie ir redzami?
4. Kā operators tiek finansēts? Ja finansējums ietver reklāmu vai datu monetizāciju, vai deklarētais mērķis aptver trešo personu datus, kurus speciālists uzticējis?
5. Kāds ir operatora finansiālais stāvoklis trīs vai piecu gadu perspektīvā? Vai ir faktori, kas liecina par drīzu modeļa maiņu (gaidāmā iziešana biržā, izsīkstoša finansēšanas kārta, iespējama iegāde)?
6. Kurā jurisdikcijā operators ir reģistrēts? Kurā valstī fiziski atrodas serveri? Ja tie atšķiras, kāds nacionālais likums attiecas uz apstrādi?
7. Kas notiktu, ja operatora jurisdikcijā spēkā esošs izlūkošanas rīkojums pieprasītu nodot manus datus? Vai uzņēmums to varētu izpildīt tehniski?
8. Kādu tehnisko spēju operators saglabā, lai apturētu, bloķētu vai dzēstu pakalpojumu? Pie kādiem līgumiskiem pieņēmumiem? Pie kādiem vēsturiski dokumentētiem nelīgumiskiem pieņēmumiem?

9. Kāds iziešanas plāns pastāv, ja operators izmantotu šo spēju pret mani, taisnīgi vai netaisnīgi? Vai pastāv dokumentēta datu eksporta procedūra uz alternatīvu pakalpojumu sniedzēju?
10. Kurš kontrolē piekļuves akreditācijas datus? Vai operators var tos atjaunot bez manas līdzdalības? Vai tas mani aizsargā vai pakļauj?
11. Vai šai konkrētajai funkcijai pastāv eiropeiska, pašmitināta vai bez servera vidū alternatīva? Kādas ir tās reālās izmaksas, salīdzinot ar novērtēto risku?
12. Ja šodienas lēmumu pēc pieciem gadiem izvērtētu inspektors, auditors vai klients, ko skāris pārkāpums, vai pašreizējā izvēle būtu aizstāvama ar šodien pieejamajiem argumentiem, vai arī būtu jāatvainojas par to, ka netika uzdoti saprātīgi jautājumi?

Jautājumi negaida perfektas atbildes. Tie gaida godīgas atbildes, ko godīgs operators prot sniegt un mazāk godīgs operators izvairās precīzi formulēt. Operatīvo atšķirību starp abām operatoru klasēm, sakām to bez dramatisma, parasti var saskatīt, lēni lasot atbildes, ko tie sniedz brīvprātīgi, pat pirms nākas prasīt vairāk.

Ar šo rakstu noslēdzam otro Cuadernos Lacre ciklu. Sākām ar redakcionālo saistību, kas mantota no Schrems II, un beidzam ar operatīvu anketu. Pa ceļam esam izgājuši cauri jēdzieniem — hash, šifrēšana, identitāte — un lietišķām analīzēm — kill switch, biznesa modelis, self-hosting. Izdevuma deklarētais redakcionālais nodoms nebija nomākt lasītāju ar izsmeļošu problēmu sarakstu, bet gan sniegt viņam rīkus, lai viņš, sastopoties ar jebkuru jaunu pakalpojumu, atšķirtu, kāda veida atbildi pieņem. Šī atšķirība — starp arhitektūru un solījumu — ir tas rīks. Pārējo katrs speciālists liks lietā to datu labā, kurus savā praksē uzskata par cienīgiem šim jautājumam.

Avoti un papildu literatūra

- Šis izdevums, 2. cikls (2026. gada maijs) — *Schrems II, piecus gadus vēlāk*, *Kas ir SHA-256 patiesībā*, *Kill switch un institucionālā sagrābšana*, *Galašifrēšana, izskaidrota pa īstam*, *Biznesa modelis kā uzticības signāls*, *24 vārdi: kas ir kriptogrāfiskā identitāte*, *Self-hosting kā profesionāla prakse*. Septiņi raksti, uz kuriem balstās šī anketa.
- Regula (ES) 2016/679 — Vispārīgā datu aizsardzības regula. Atsauces juridiskais ietvars visiem jautājumiem, ko anketa izvirza, jo īpaši 5., 6., 25., 28., 32., 33. pantam un V nodaļai.
- Eiropas Datu aizsardzības kolēģija — operatīvās vadlīnijas un atzinumi par Schrems II, starptautiskajiem pārsūtījumiem, ietekmes novērtējumiem un proaktīvo atbildību (2020.–2024. gada publikācijas).
- Spānijas Datu aizsardzības aģentūra — 2022.–2024. gadā publicētās sankcijas datu pārziņiem par neatbilstošiem pārsūtīšanas instrumentiem vai par formāliem ietekmes novērtējumiem bez būtiska satura.
- noyb.eu — Eiropas Digitālo tiesību centrs, ko vada Maximilian Schrems. Publisks sūdzību, pārsūdzību un analīžu repozitorijs par reālu, nevis šķietamu Eiropas datu aizsardzības normu ievērošanu.

← IepriekšējaisSelf-hosting kā profesionāla prakseNākamais →Tas, ko paraksts nevar atrisināt

Jaunākie lasījumi

- Pārdomas · 2026. gada 29. jūnijs Tu neesi anonīms
- Pārdomas · 2026. gada 27. maijs Tas, ko paraksts nevar atrisināt
- Analīze · 2026. gada 25. maijs Self-hosting kā profesionāla prakse

Paņemiet šo rakstu līdzi tur, kur jums nepieciešams.

↓ Markdown ↓ Parasts teksts ↓ PDF

Fails tiks lejupielādēts jūsu ierīcē. No turienes varat to saglabāt, importēt Solo2 vai kopīgot jebkur. Cuadernos nepieņem lēmumu par galamērķi jūsu vietā.

Vaska zīmogs · SHA-256 ca021182c25833e1200a1dc355d9b89a2ad1da345266c241814f35bb56baff63

Cuadernos Lacre · Menzuri Gestión S.L. publikācija ·
autors R.Eugenio · rediģējusi Solo2 komanda.