Analyse · 26. maj 2026

← Forrige·Næste →

Reelt vs. tilsyneladende privatliv: de spørgsmål, man bør stille sig selv

Operationel syntese af cyklus 2: de spørgsmål, der adskiller en tjeneste med arkitektonisk privatliv fra en med deklarativt privatliv. Et spørgeskema til den europæiske fagperson, før vedkommende tager et digitalt værktøj til følsomme data i brug.

For at forstå hinanden: To tjenester med den samme juridiske meddelelse kan opføre sig meget forskelligt. Den ene beskytter ved teknisk design. Den anden beskytter ved kontraktligt løfte. Forskellen kan ikke læses i meddelelsen — den opdages ved at stille de konkrete spørgsmål. Svarenes kvalitet siger lige så meget om produktet som deres eget indhold.

Forskellen mellem arkitektonisk og deklarativt privatliv

I løbet af de syv foregående artikler i denne cyklus har vi bevæget os gennem forskellige lag af det samme emne. Retten om internationale overførsler med Schrems II. Den matematiske idé om den kryptografiske hash, der forsegler hver Cuaderno. Det arkitektoniske valg af kill switch og den institutionelle indfangning, der næsten altid ledsager den. Mekanismen i ende-til-ende-krypteringen og det operationelle spørgsmål om, hvor nøglerne befinder sig. Tilpasningen af incitamenterne efter forretningsmodellen. Den selvsuveræne kryptografiske identitet. Self-hosting som forholdsmæssig strategi. Hver artikel beskæftigede sig med én vinkel. Denne, den sidste i cyklussen, samler dem i et spørgeskema.

Den skelnen, det er værd at huske, er enkel: der er tjenester, hvis privatliv er *arkitektonisk*, og der er tjenester, hvis privatliv er *deklarativt*. Det første er indlejret i det tekniske design: visse krænkelser af privatlivsforpligtelsen er teknisk vanskelige eller umulige, fordi arkitekturen ikke tillader dem. Det andet er nedfældet i teksten i den juridiske meddelelse: visse krænkelser ville være kontraktligt sanktionerbare, hvis de indtræffer, men teknisk forhindrer intet dem. Begge modeller kan overholde GDPR; men den ene beskytter ved konstruktion og den anden beskytter ved løfte, og forskellen er operationelt enorm.

De følgende spørgsmål er udformet til at adskille det ene tilfælde fra det andet. Det er ikke avancerede tekniske spørgsmål. Det er de spørgsmål, som enhver ærlig udbyder kan besvare i sin offentlige dokumentation. Svarets kvalitet og præcision siger lige så meget om produktet som selve svaret. Spørgsmålene er grupperet i seks lag; det er godt at stille dem alle, før man tager tjenesten i brug til følsomme data, ikke kun dem, det første instinkt identificerer.

Lag 1: arkitektur

Lad os fastlægge et begreb, før vi går videre. Med *operatør* mener vi virksomheden, der leverer tjenesten: den enhed, der kontrollerer servere og software, ikke en bestemt person. Når det er sagt, er det grundlæggende arkitektoniske spørgsmål: hvad gør operatøren med indholdet mellem afsender og modtager? Der er tre mulige svar, og det er værd at kunne skelne mellem dem, for alle tre markedsføres undertiden med lignende ordforråd.

- Det første: indholdet passerer gennem en server hos operatøren i klartekst, hvor operatøren kan læse det, selv om han lover ikke at gøre det.
- Det andet: indholdet passerer krypteret gennem en server hos operatøren, hvor operatøren ikke kan læse det, hvis nøglerne udelukkende ligger på brugernes enheder.
- Det tredje: indholdet passerer ikke gennem nogen server hos operatøren, fordi der ikke findes en server hos operatøren i dette konkrete flow.

Forskellen mellem disse tre er ikke en forskel i grad: det er en forskel i type.

Det supplerende spørgsmål — allerede formuleret i Cuaderno om kryptering — er: hvem har de kryptografiske nøgler, der gør det muligt at læse indholdet? Hvis brugeren har dem og kun brugeren, er krypteringen reel. Hvis operatøren derudover har dem i nogen form — selv under navnet «kontogendannelse» eller «synkronisering mellem enheder» —, er krypteringen nominel. Spørgsmålet tillader ikke et ærligt mellemsvar.

Lag 2: forretningsmodel

Spørgsmålet om forretningsmodellen betyder lige så meget som det arkitektoniske spørgsmål, og af samme væsentlige grund: incitamenter frembringer over tid systematisk forskellige produkter, selv med identisk erklærede formål. Hvordan tjener operatøren penge i dag? En enkelt kilde, to, en blanding? Hvis finansieringen omfatter reklame eller datamonetisering, hvilke data monetiseres da, og på hvilket retsgrundlag i GDPR sker det? Dækker det formål, der er erklæret i den juridiske meddelelse, de tredjepartsdata, som fagpersonen agter at betro tjenesten?

Og spørgsmålet af anden orden, ikke altid formuleret: hvad er operatørens finansielle situation på tre til fem års sigt? En virksomhed i venturekapitalfasen opererer under et andet pres end en virksomhed med stabil rentabilitet. Ændringen af finansieringsmodellen er gentagne gange det øjeblik, hvor den implicitte kontrakt med brugerne omskrives uden forhandling.

Lag 3: jurisdiktion

For den europæiske fagperson er spørgsmålet om jurisdiktion ikke retorisk. I hvilken jurisdiktion er operatøren registreret? I hvilket land befinder de servere, der behandler dataene, sig fysisk? Er svaret på de to foregående spørgsmål det samme eller forskelligt, og hvis det adskiller sig, hvilken lovgivning gælder da? En europæisk region drevet af en amerikansk virksomhed er, hvad angår Schrems II, ikke et europæisk svar: virksomheden er underlagt FISA 702 uanset, hvor serverne befinder sig.

Det supplerende operationelle spørgsmål er: hvis der i morgen kom en efterretningsordre, der er gyldig i operatørens jurisdiktion, og som krævede udlevering af mine data eller mine kunders, hvad ville der så ske? Hvis det ærlige svar begynder med «virksomheden ville være forpligtet til at udlevere dem», beskytter tjenesten ikke mod den ordre, uanset hvor meget reklamen antyder det modsatte. Hvis det ærlige svar begynder med «virksomheden kunne ikke udlevere dem, fordi den ikke har dem i klartekst», beskytter tjenesten faktisk; og forskellen afhænger næsten udelukkende af de to første lag, ikke af privatlivspolitikkens kvalitet.

Lag 4: operatør og kill switch

Hvilken teknisk kapacitet bevarer operatøren til at suspendere, blokere, slette eller forringe tjenesten på afstand? Spørgsmålet er ikke paranoidt: det er operationelt. De digitale platforme har gentagne gange udøvet denne kapacitet i de senere år, undertiden på eget initiativ, undertiden efter ordre fra regeringer, undertiden efter ejerskifte eller politikændringer. Hvis kapaciteten findes, er det godt at vide, under hvilke kontraktligt erklærede forudsætninger den udøves, og at reservere en margin til de uerklærede forudsætninger, som de senere års praksis har vist at være lige så relevante: uventet retskendelse, international sanktion, ændring af virksomhedsledelse, opkøb af en enhed med en anden politik.

Søsterspørgsmålet er det om kontinuitetsplanen: hvis operatøren udøvede kapaciteten mod fagpersonen — uanset grunden, med rette eller ej —, hvor megen driftstid ville stadig være tilgængelig, hvilken procedure for eksport af data findes der, og til hvilken alternativ udbyder kunne man migrere? Hvis svaret begynder med «det burde ikke ske», er det ikke et operationelt svar; det er et løfte.

Lag 5: identitet og adgang

Hvem kontrollerer adgangsoplysningerne til tjenesten? Hvis operatøren kan nulstille brugerens adgang uden brugerens medvirken — en procedure typisk kaldet «kontogendannelse» —, er operatøren teknisk set kontoens forvalter og kan også overdrage den til den, der anmoder om det via den passende procedure. Hvis operatøren ikke kan nulstille adgangen, fordi identiteten ligger kryptografisk på brugerens enhed, kan operatøren heller ikke overdrage den, ikke engang efter ordre. Begge modaliteter er legitime afhængigt af konteksten; men, igen, de er forskellige, og det er godt at vide, hvilken man tager i brug.

Hvad sker der med fagpersonens data, hvis fagpersonen mister adgangen? Findes der gendannelsesmekanismer — for konto, fil, session — der afhænger af operatøren? Er disse mekanismer forenelige med branchens fagetik, hvis operatøren tvinges til at bruge dem?

Lag 6: fremtid

Dette sidste lag forsømmes ofte, fordi det kræver projektion. Hvad ville der ske, hvis tjenesten blev opkøbt af en anden virksomhed? Næsten alle opkøb medfører en revision af tjenestevilkårene i de følgende måneder. Hvad ville der ske, hvis de regulatoriske krav ændrede sig? Den europæiske ret har øget forpligtelserne til fjernelse og blokering siden 2022, ikke reduceret dem. Hvad ville der ske, hvis operatøren forsvandt? En betydelig del af cloud-tjenesterne har ingen dokumenteret exit-plan for det scenarie, hvor operatøren lukker; fagpersonen opdager problemet, når der ikke længere er tid til at forberede det.

Der er en formulering, det er værd at huske til dette lag: arkitekturer, der afhænger mindre af operatøren, er mere modstandsdygtige over for ændringer hos operatøren. Self-hosting i enhver af dens modaliteter, den selvsuveræne kryptografiske identitet, kommunikationen uden server imellem — alt dette reducerer den fremtidige risikoflade ved den procedure at reducere den nuværende afhængighedsflade. De eliminerer den ikke; de reducerer den.

Forskellen mellem struktur og løfte

Hvis vi skulle destillere cyklussen til en eneste sætning, ville det være denne: de strukturelle svar holder, selv om operatøren, forvaltningen eller lovgivningen ændrer sig; svarene per løfte holder, så længe den, der lover, kan og vil holde dem. Begge kan være korrekte i det øjeblik, de antages. Kun det ene af de to holder uafhængigt af tidens gang og omstændighedernes forandring.

Dette betyder ikke, at hver fagperson skal kræve strukturelle svar af alle de tjenester, vedkommende tager i brug. Forholdsmæssigheden er fortsat legitim: et regneark til intern bogføring behøver ikke det samme svar som en patients journal. Det betyder dog, at professionalisme består i at vide, hvilken slags svar man har accepteret i hvert enkelt tilfælde, og i bevidst at have besluttet, at den slags svar er forholdsmæssig i forhold til det konkrete data.

Spørgeskemaet, ordnet

Tolv konkrete spørgsmål, der sammenfatter cyklussen, ordnet således, at svaret på hvert enkelt informerer det næste:

1. Passerer indholdet gennem en server hos operatøren? Hvis ja: i klartekst, krypteret med operatørens nøgler eller krypteret med nøgler, der udelukkende tilhører brugeren?
2. Hvis ende-til-ende-kryptering påberåbes, hvor befinder de kryptografiske nøgler sig da? Kender eller opbevarer operatøren nogen del af dem i nogen form, herunder «gendannelse»?
3. Hvilke metadata genererer og opbevarer tjenesten? Hvor længe? For hvem er de synlige?
4. Hvordan finansieres operatøren? Hvis finansieringen omfatter reklame eller datamonetisering, dækker det erklærede formål da tredjeparts data betroet af fagpersonen?
5. Hvad er operatørens finansielle situation på tre til fem års sigt? Er der faktorer, der antyder en forestående modelændring (forestående børsnotering, finansieringsrunde ved at løbe tør, sandsynligt opkøb)?
6. I hvilken jurisdiktion er operatøren registreret? I hvilket land befinder serverne sig fysisk? Hvis de adskiller sig, hvilken national lovgivning gælder da for behandlingen?
7. Hvad ville der ske, hvis en efterretningsordre, der er gyldig i operatørens jurisdiktion, krævede udlevering af mine data? Ville virksomheden teknisk kunne efterkomme den?
8. Hvilken teknisk kapacitet bevarer operatøren til at suspendere, blokere eller slette tjenesten? Under hvilke kontraktlige forudsætninger? Under hvilke historisk dokumenterede ikke-kontraktlige forudsætninger?
9. Hvilken exit-plan findes der, hvis operatøren udøvede denne kapacitet mod mig, med rette eller urette? Findes der en dokumenteret procedure for eksport af data til en alternativ udbyder?
10. Hvem kontrollerer adgangsoplysningerne? Kan operatøren nulstille dem uden min medvirken? Beskytter det mig eller udsætter det mig?
11. Findes der et europæisk, selvhostet eller serverløst alternativ til denne konkrete funktion? Hvad er dens reelle omkostning sammenlignet med den vurderede risiko?
12. Hvis dagens beslutning om fem år blev undersøgt af en inspektør, en revisor eller en kunde ramt af et brud, ville det nuværende valg da være forsvarligt med de argumenter, der er til rådighed i dag, eller ville det kræve en undskyldning for ikke at have stillet rimelige spørgsmål?

Spørgsmålene venter ikke perfekte svar. De venter ærlige svar, som den ærlige operatør ved at give, og som den mindre ærlige operatør undgår at formulere præcist. Den operationelle forskel mellem de to slags operatører, det siger vi uden dramatik, mærkes som regel ved langsomt at læse de svar, de tilbyder frivilligt, allerede før man behøver at bede om mere.

Med denne artikel afslutter vi den anden cyklus af Cuadernos Lacre. Vi begyndte med den redaktionelle gæld arvet fra Schrems II og slutter med et operationelt spørgeskema. Undervejs har vi bevæget os gennem begreber — hash, kryptering, identitet — og anvendte analyser — kill switch, forretningsmodel, self-hosting. Publikationens erklærede redaktionelle hensigt var ikke at overvælde læseren med den udtømmende liste over problemer, men at give vedkommende værktøjer, så han over for enhver ny tjeneste kan skelne, hvilken slags svar han accepterer. Den skelnen — mellem arkitektur og løfte — er værktøjet. Resten vil hver fagperson stille til tjeneste for de data, som vedkommende i sin praksis anser for værdige til spørgsmålet.

Kilder og yderligere læsning

- Denne publikation, cyklus 2 (maj 2026) — *Schrems II, fem år senere*, *Hvad SHA-256 egentlig er*, *Kill switch og institutionel indfangning*, *Ende-til-ende-kryptering, forklaret for alvor*, *Forretningsmodellen som et tillidssignal*, *De 24 ord: hvad en kryptografisk identitet er*, *Self-hosting som professionel praksis*. De syv artikler, som dette spørgeskema hviler på.
- Forordning (EU) 2016/679 — Den generelle forordning om databeskyttelse. Juridisk referenceramme for alle de spørgsmål, spørgeskemaet rejser, navnlig artikel 5, 6, 25, 28, 32, 33 og kapitel V.
- Det Europæiske Databeskyttelsesråd — operationelle retningslinjer og udtalelser om Schrems II, internationale overførsler, konsekvensanalyser og proaktiv ansvarlighed (publikationer 2020-2024).
- Det spanske databeskyttelsesagentur — offentliggjorte sanktioner 2022-2024 mod dataansvarlige for uegnede overførselsinstrumenter eller for formelle konsekvensanalyser uden væsentligt indhold.
- noyb.eu — Det Europæiske Center for Digitale Rettigheder, ledet af Maximilian Schrems. Offentligt arkiv over klager, retsmidler og analyser om den reelle, ikke tilsyneladende overholdelse af de europæiske databeskyttelsesregler.

← ForrigeSelf-hosting som professionel praksisNæste →Hvad en underskrift ikke kan løse

Seneste læsning

- Refleksion · 29. juni 2026 Du er ikke anonym
- Refleksion · 27. maj 2026 Hvad en underskrift ikke kan løse
- Analyse · 25. maj 2026 Self-hosting som professionel praksis

Tag denne artikel med dig, hvor du har brug for den.

↓ Markdown ↓ Almindelig tekst ↓ PDF

Filen downloades til din enhed. Derfra kan du gemme den, importere den til Solo2 eller dele den, hvor du vil. Cuadernos beslutter ikke destinationen for dig.

Laksegl · SHA-256 d8ac6716cfcf67451f04b65d54bac7df97301391bb5e8820a51a6e9cd25a3e35

Cuadernos Lacre · En udgivelse fra Menzuri Gestión S.L. ·
skrevet af R.Eugenio · redigeret af holdet bag Solo2.