Analyse · 25. mai 2026

← Forrige·Neste →

Self-hosting som profesjonell praksis

En server er ikke noe mer enn en datamaskin. Spørsmålet er ikke om man skal ha en, men hvor kundenes data bor, hvem som opprettholder dem og hvem som bærer ansvaret når noe svikter.

Kort fortalt: Dine data bor alltid på noens datamaskin: på en gigants, som du betror alt til, på en leid som du selv administrerer, eller på din egen. Jo mer kontroll du ønsker, jo mer ansvar påtar du deg. Å delegere til en stor tredjepart beroliger, men fritar ikke: informasjonen er din —og dine kunders—, og den ansvarlige er du.

Spørsmålet mellom skyen og kjelleren

Det er lurt å starte med å deaktivere et ord som skremmer uten grunn: server. En server er ikke en mystisk maskin i et kjølt rom. Det er slett og rett en annen persons datamaskin —eller din egen— som lagrer informasjon og leverer den til dem som ber om den. I tiår lagret vi kundenes informasjon i en mappe, i et arkivskap, på skrivebordet, og ingen lå søvnløs over det. Informasjon var ikke skremmende fordi den var på papir; den trenger heller ikke være det fordi den er på en disk.

«Skyen» er heller ikke eterisk. Det er en bedrifts datamaskin, nesten alltid langt unna og nesten alltid noen andres. Jeg lærte det utilsiktet den dagen da jeg, i tillit til at filene mine var i trygg forvaring i Google Drive, oppdaget at mappen på datamaskinen min ikke inneholdt dokumentene mine, men snarveier til dokumenter som bodde et annet sted. Hvis det andre stedet bestemte seg for å stenge, endre pris eller si opp tjenesten, ville min ro forsvunnet med det. Jeg eide ikke tingene mine; jeg hadde tillatelse til å få tilgang til dem.

Derfra springer spørsmålet i dette Heftet ut, enklere å formulere enn å besvare: hvor bør klientenes dine data bo? Og dine egne? Den offentlige samtalen stiller det opp som om det bare fantes to motstridende svar — de store plattformenes sky eller å sette det opp selv —, nesten et spørsmål om hvilken leir man tilhører. Men det er ikke to veier: det er tre, og ingen av dem er en trosakt. Lest i ro og mak har de flere nyanser og krever mer enn det ser ut til.

Dette angår deg, uansett hva du selger

Det er lett å tro at konfidensialitet er noe for advokater, leger eller journalister, og at resten ikke har noe å skjule. Det er en feil, og en av de dyre. Nesten enhver virksomhet lagrer data om kundene sine som er underlagt loven, og mange lagrer, uten å vite det, informasjon som er langt mer sensitiv enn det ser ut til.

En sofabutikk noterer navnet, adressen og telefonnummeret til den som kjøper; er det finansiering, også vedkommendes økonomiske opplysninger. Et oppussings- eller innredningsfirma oppbevarer bilder av innsiden av klientenes hjem og de fullstendige plantegningene av boligene deres. Et rengjøringsfirma håndterer plantegningene over kontorene det vasker, ofte merket med farger og tall som angir hvilken ansatt som kommer inn hvor, til hvilken tid og med hvilken nøkkel. Ingenting av dette virker som stort før man spør seg for hvem ellers det ville hatt verdi: disse rengjøringsplanene er, sett med andre øyne, det perfekte kartet for den som vil bryte seg inn for å stjele.

At en virksomhet er liten, eller at den selger sofaer i stedet for å føre rettssaker, gjør ikke dens data mindre verdifulle eller at loven slutter å gjelde for den. Det gjør bare at eieren pleier å tenke mindre over det. Og å tenke lite over noe som er ditt ansvar, er nettopp der problemene starter.

Hvor bor dine data?

På det spørsmålet finnes det i bunn og grunn tre svar. Og det er verdt å huske at «dataene» ikke bare er en klients dossier eller bunken med fakturaer og tilbud: det er også samtalene dine med ham — via WhatsApp, via en profesjonell chattjeneste, via Solo2. De tre svarene som følger er ikke renhetsgrader eller en stige fra gode til onde: de er tre måter å fordele det samme på, kontrollen og ansvaret.

Å delegere alt til en leverandør. Det er det vanligste, og for de fleste er det det eneste de kjenner til. Jeg legger alt i Google Workspace eller Microsoft 365 og overlater det helt til leverandøren. Jeg betaler avgiften min og slutter å tenke på det. Den mest ekstreme formen for dette er tjenestene der du ikke engang får ha dine egne data: visse faktureringsprogrammer i skyen lagrer for eksempel fakturaene og tilbudene dine — og fungerer veldig godt —, men informasjonen lever i deres system, ikke i ditt. Så lenge du betaler, har du tilgang; den dagen du drar, oppdager du at det er vanskelig eller umulig å ta med deg din egen historikk. Å holde dataene dine halvt som gissel er for mer enn én leverandør nettopp det som hindrer deg i å gå til konkurrenten. I bytte mot bekvemmelighet gir jeg fra meg kontrollen og — uten å si det høyt — følelsen av at ansvaret ikke lenger er mitt. Her er det plass til en nyanse som nesten aldri gjøres: å delegere er ikke synonymt med amerikansk. Jeg kan delegere alt like bekvemt til en europeisk leverandør — Infomaniak, for eksempel — og med ett slag løse en stor del av tvilen om internasjonale overføringer som vi så i «Schrems II», uten å hoste noe selv. Det er ikke USA mot resten av universet: innenfor den rene delegeringen finnes det allerede beslutninger som betyr noe.

Leie og administrere din egen server. Jeg har det samme som Microsoft eller Google ville gitt meg, men jeg setter det opp selv. Jeg leier en server hos en europeisk leverandør —Hetzner, OVH, Scaleway—, installerer fri programvare (Nextcloud for filer, for eksempel) og administrerer resultatet selv. Jeg får reell kontroll: jeg vet hva som kjører, hvor og hvorfor. Men maskinen befinner seg fortsatt i datasenteret til en tredjepart, og fremfor alt endres det hvem som bærer konsekvensene. Ved å delegere har du noen å klandre hvis noe går galt. Ved å administrere det selv, er det mest sannsynlig at feilen er din.

Ha det på din egen datamaskin. Dette er alternativet som nesten ingen forteller om, og det er hjertet i dette heftet. Man trenger ikke en enorm server som står på tjuefire timer i døgnet i et makro-datasenter for å hoste tingene sine. Kontordatamaskinen din er allerede en server: den tjener deg. Du lar den stå på på kontoret og kobler deg til den fra den bærbare datamaskinen hos en kunde, eller fra mobilen når du er hjemme. Vi kaller den «kontordatamaskinen», ikke «serveren», men den gjør nøyaktig det samme som de to foregående alternativene. Kontrollen er maksimal og nærheten likeså: dataene dine er der du er. Baksiden, sagt uten omsvøp, er at ansvaret også er maksimalt. Hvis strømmen går, er det ingen tekniker på vakt i Nürnberg: det er din jobb å vippe opp sikringen. Og for at den datamaskinen skal være tilgjelig utenfra, trengs det noe som bygger bro mellom din bærbare datamaskin og den. Det er ikke magi, og det er greit å vite før man velger denne veien.

Og du trenger ikke engang å gjenbruke kontormaskinen: det finnes en enhet laget nettopp for dette, NAS-en (laget av Synology, QNAP og andre). Som nesten alt vi har sett i disse Cuadernos, er det ingen magi inni: det er en spesialisert datamaskin, samme type maskin som du ville leid i et datasenter, bare bygd for å lagre data og levere dem over nettverket, uten skjerm eller tastatur imellom. Koble til en skjerm og et tastatur, og du har en vanlig datamaskin; installer riktig programvare på PC-en din, og du har en NAS. Forskjellen er at NAS-en kommer klar til bruk. Du kjøper den, du kobler den til hjemme eller på kontoret, og den er din. Du betaler ingen månedlig avgift; du betaler én gang, og den tilhører deg, som ethvert annet verktøy i bedriften din. Du slår den på, slår den av, tar den med deg et annet sted hvis du vil. Og siden den er din, er det ingenting som hindrer deg i å ha to —en hjemme, en på kontoret— eller tre, ved å legge til en på et trygt sted, synkronisert med hverandre: din egen redundans, uten å være avhengig av at en tredjepart vedlikeholder den. Selvhosting er til syvende og sist ikke én enkelt ting: det er en kombinasjon av maskiner, av eierskap, av plasseringer og av programvare.

Her er det uunngåelig å nevne det vi gjør, og vi gjør det uten forkledning: hos Solo2 er det selve applikasjonen som slår den broen. Datamaskinen på kontoret ditt forblir tilgjengelig bare for de betrodde enhetene dine, og alltid under kryptering, og de øvrige apparatene dine kobler seg til den igjen av seg selv. Når en klient snakker med deg, er det datamaskinen din — ikke en tredjeparts — som snakker med klienten. Vi løser ikke strømbruddet; vi løser broen. Og vi er ikke de eneste: for nesten ethvert behov finnes det i dag programmer — frie eller proprietære — som tillater nettopp dette, å ha dataene på ditt eget utstyr og nå dem utenfra. Vårt er et eksempel; det viktige er idéen, ikke merket.

Redundans er ikke en superkraft

Her oppstår den umiddelbare innvendingen, og den er rimelig: hvis jeg har alt på kontordatamaskinen min, hva skjer hvis den går i stykker? Spørsmålet er godt. Svaret er at sikkerhetsnettet vi ser for oss hos de store leverandørene er mer beskjedent —og lettere å etterligne— enn det ser ut til.

Når jeg legger igjen dataene mine i datasenteret til et flernasjonalt selskap, stoler jeg på at de har kopier på flere steder. Og sannsynligvis har de det: på en annen lokasjon, kanskje på en tredje. Men den redundansen er ikke uendelig og fremfor alt er den ikke min: det forblir en harddisk som jeg ikke eier, administrert av noen som jeg viser en tillit jeg nesten aldri verifiserer.

Det samme nettet kan jeg veve selv, og med en avgjørende fordel. Min daglige tjeneste bor på kontordatamaskinen. Derfra lagrer jeg en kryptert kopi på en vennligsinnet bedrifts datamaskin —en kollega i faget, et annet betrodd kontor— og en annen kryptert kopi, hvis jeg vil, hos den samme europeiske leverandøren som vi snakket om. Forskjellen er alt: det jeg etterlater ute er ikke min tjeneste eller mine data i klartekst, men en kryptert kopi som bare jeg kan åpne. Den eksterne leverandøren oppbevarer en lukket kiste som vedkommende ikke har nøkkelen til. Jeg betror ham ikke informasjonen min: jeg betror ham noen bytes som uten meg ikke betyr noe.

Det var trygt helt til det ikke var det lenger

La meg fortelle en personlig historie, for den illustrerer dette bedre enn noe argument. I mer enn ti år var jeg en trofast kunde av CrashPlan, en teknisk sett ekstraordinær sikkerhetskopieringstjeneste. Jeg sikkerhetskopierte alle mine datamaskiner og familiens datamaskiner —firmaets og hjemmets, alt— til deres sky, med versjoner som jeg kunne gjenopprette med den hyppigheten jeg ønsket, og reise tilbake i tid til en spesifikk fil fra måneder tilbake. Etter den første kopien overførte den bare endringene, kryptert og komprimert, slik at jeg holdt en enorm sikkerhetskopi oppdatert med nesten ingen innsats. Det reddet meg mange ganger, fra et dumt dokument til en hel disk. Prisen steg med årene og jeg brydde meg ikke: jeg betalte med glede.

Det jeg ikke visste var at CrashPlan hadde gjort en beregningsfeil: de hadde lovet ubegrenset lagring ved kontrakt, både i plass og tid. Og plass multiplisert med tid —år med historikk, versjoner hvert par minutter— vokser til det blir uholdbart. En dag meddelte de oss alle at tjenesten opphørte. De gjorde det med eleganse og med en generøs frist, nesten et år, og de ga oss midler til å laste ned vårt eget. Men hvor går man med mer enn ti år med versjonerte kopier av alle diskene sine? Der oppdager man at man verken har en måte å laste ned alt på eller et sted å gjøre av det, og at selv om man kunne, ville det nye lageret kostet en formue.

Jeg reddet fire uunnværlige ting. Resten forsvant da de slo av bryteren. Jeg var rolig, informasjonen min var i sikkerhet... helt til den sluttet å være det. Og ikke på grunn av et svik: CrashPlan oppførte seg upåklagelig — i motsetning til Evernote, som år senere oppførte seg skammelig —; ganske enkelt bestemte skytsengelen min i skyen seg, med full rett, for å slutte å være det. Resultatet var for meg identisk: det jeg trodde var trygt, forsvant.

Det denne historien virkelig lærer oss har mer med menneskelig natur å gjøre enn med teknologi. Når man føler at noe er ens eget ansvar, handler man forebyggende: man tar kopier, sikrer ryggen sin, er mistroisk med godt skjønn. Når man —feilaktig— tror at ansvaret bæres av en stor og solid tredjepart, slapper man av og lar det stå til. Den delegerte roen er ikke forsiktighet: det er, uten sminke, en form for ansvarsløshet.

Å betale er ikke det samme som å overholde regler

Den stille ansvarsløsheten ligner mye på foreldre som skriver inn sønnen sin på den dyreste skolen, betaler for en mastergrad etterpå, og med det tror de har oppfylt sin plikt. De har ikke oppfylt sin plikt. Å være forelder er å bekymre seg for hva han lærte i dag, om det han ikke forstår, om hans verdier, om hans selvtillit. Hvis den sønnen som 25-åring ikke vet hvordan man jobber eller oppfører seg, er skylden ikke skolens som tok pengene: den ligger hos den som delegerte og betalte i den tro at det var nok. Å betale en tredjepart fritar ikke for ansvar. Det har det aldri gjort.

Med data er det likedan, og den nyere historien bekrefter det. For femti eller hundre år siden oppbevarte en fagperson klientenes ting i mapper, på kontoret eller hjemme, og følte seg ansvarlig for dem. Sjelden gikk noe tapt. Vi har gått over til den digitale verdenen og laster, med forbløffende letthet, opp alt til «skyen» — som ikke er noe annet enn datamaskinen til et multinasjonalt selskap — og slutter å bekymre oss. Og ofte skjer det uhell, og det finnes bedrifter som mister alt, og da sies det: det var Googles skyld, det var Microsofts skyld. Nei. Informasjonen er din, eller klientenes dine, men den ansvarlige er deg.

Å hoste sine egne ting er ikke et teknisk lune: det er å gjenvinne den roen fra tiår tilbake, den ved å vite hvor hver ting er og hvorfor. Personvern har i mellomtiden opplevd et brått pendelsving —fra å ikke ha noen regler i det hele tatt, da hvem som helst eksponerte en kundes data uten å tenke, til et krav som faller med uforholdsmessig hardhet på den minste, den selvstendig næringsdrivende som gir en kundes telefonnummer til budet. Jeg diskuterer ikke målet; jeg observerer misforholdet. Men misforholdet fritar oss ikke: den dagen myndighetene har midler til å spore og sanksjonere i stor skala, vil størrelse slutte å beskytte noen, og det er klokt å ikke vente på den dagen med et uorganisert hus. Å ha dataene under egen kontroll hjelper med å overholde regler og hjelper med å bevise det. Og fremfor alt bringer det tingene tilbake på plass: når informasjonen er din, er ansvaret fullt ut ditt —det finnes ingen tredjepart å klandre, heller ikke en tredjepart hvis feil eksponerer deg—.

Ansvar beskytter også

Det ville være uærlig å male dette uten skygger. Å innta mellomleddets plass betyr å bære dets byrde: å holde sikkerhetskopier oppdaterte, å bruke oppdateringer og et juridisk ansvar — RGPD-ets — som i virkeligheten aldri helt sluttet å være ditt (fotnotehenvisningene angir artiklene i detalj). Det er arbeid, og det er en dag da noe svikter på et ubeleilig tidspunkt. Vi skjuler det ikke.

Men frykten som omgir det ordet, ansvar, er feilkalibrert. Det er mye lettere å miste filene dine i en skytjeneste som stenger, eller bildene dine i Google Foto, enn å miste den mappen med viktige dokumenter du har på din egen datamaskin: den du vet hvor er, og hvis fravær du ville lagt merke til så snart den forsvant. Det du føler er ditt, tar du vare på; det du tror er trygt i en annens hender, forsømmer du.

Tenk på fortidens fotoalbum, de av fremkalt papir oppbevart i en skuff. Har du noen gang hørt noen si at de «mistet» familiealbumet sitt? Man hører om huset som brant ned med albumet inni; bare å miste det sånn, nei. Og derimot, folk som hadde alle bildene sine i Google Foto eller i Apple Bilder og satt igjen med ingenting: den historien kommer tilbake med noen måneders mellomrom, fordi de trodde det var trygt. Google Foto tar vare på bildene dine, ja visst; men det tar ikke vare på dem slik foreldre tar vare på albumet der barna og barnebarna deres er. Den forskjellen utbedres ikke av noe datasenter: ansvar, når det er ditt, er ikke bare en byrde; det er også den beste garantien.

Fire spørsmål før du bestemmer deg

Hvis du vurderer å ta skrittet, i en hvilken som helst form, er det lurt å først svare på fire spørsmål med nøktern ærlighet:

1. Hvilken del av dataene dine ville det gjøre vondt å miste, eller å ikke kunne ta med deg? Og pass deg for å avfeie det «rutinemessige»: fakturahistorikken virker som det mest prosaiske i verden helt til du bytter program og oppdager at de fakturaene tilhørte leverandøren, ikke deg — at du i beste fall kan skrive dem ut til PDF, uten lenger å kunne søke inni dem. Det er ikke bare et spørsmål om følsomhet: det handler om hvem det du trenger å bevare i virkeligheten tilhører.
2. Hvilket alternativ står i forhold til din virkelige tekniske evne? En velholdt egen datamaskin er innen rekkevidde for hvem som helst; å administrere en hel server, ikke like mye. Vær ærlig om hva du kan og hva du ikke kan. Og husk at mellom det å sette opp en hel server og det å delegere alt finnes det et veldig fornuftig mellomområde: programmer — frie eller proprietære — som lagrer dataene dine på ditt eget utstyr og lar deg nå dem utenfra. For mange mennesker er det den beste balansen.
3. Hvilken plan har du for den verste dagen? Et databrudd, en disk som dør, en leverandør som stenger, teknikeren er sykemeldt. Hvis planen starter med «det burde ikke skje», er det ikke en plan.
4. Ville du vite hvordan du beviser at du overholder reglene hvis du ble inspisert i morgen? Å gjøre det bra og å kunne bevise at man gjør det bra, er ikke det samme. Loven krever det siste.

Det finnes intet universelt svar. Det finnes et proporsjonalt svar, vedtatt med ærlighet om hva som vinnes og hva som arves. Og hevet over teknikken, en enkel visshet: dine data bor på noens datamaskin. Det eneste spørsmålet som virkelig betyr noe er hvem du ønsker skal eie den datamaskinen.

Selvhosting er hverken en dyd eller en last: det er et verktøy med et konkret avtrykk av kapasiteter og ansvar. Spørsmålet var aldri om du skulle hoste dine egne data, men hvilke data, hvordan og med hvilket støttenettverk. Å gjenvinne kontrollen over data er ikke å vende tilbake til kjelleren eller å mistro alt: det er å begynne å føle seg ansvarlig for det som er vårt igjen, slik som da dataene bodde i en mappe på bordet. Dette ansvaret, riktig forstått, er den virkelige tjenesten som en profesjonell yder sine kunder.

Kilder og videre lesing

- Forordning (EU) 2016/679 — artikkel 28 (databehandler), artikkel 32 (behandlingssikkerhet), artikkel 33 (varsling om brudd), artikkel 37 (utpeking av personvernombud).
- Det spanske datatilsynet (AEPD) — *Guía práctica para análisis de riesgos en el tratamiento de datos personales* (gjeldende revisjon). Rammeverk for behandlingsansvarlige som påtar seg egne tekniske funksjoner.
- Det europeiske personvernrådet — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Gjelder også for proporsjonalitetsvurdering ved beslutninger om egen infrastruktur.
- Europakommisjonen — offentlig fortegnelse over leverandører av informasjonssamfunnstjenester etablert i europeisk jurisdiksjon. Administrativt utgangspunkt for identifikasjon av europeiske administrerte hosting-muligheter.
- Nextcloud GmbH (Tyskland) — *Nextcloud Enterprise architecture and compliance documentation*. Dokumentert tilfelle av fri programvare med selvhostede og administrerte løsninger via europeisk leverandør; nyttig som teknisk referanse for et prosjekt støttet i europeisk jurisdiksjon siden 2016.

← ForrigeDe 24 ordene: hva en kryptografisk identitet erNeste →Reelt vs. tilsynelatende personvern: Spørsmålene man bør stille seg selv

Siste lesninger

- Refleksjon · 29. juni 2026 Du er ikke anonym
- Refleksjon · 27. mai 2026 Det en signatur ikke kan fikse
- Analyse · 26. mai 2026 Reelt vs. tilsynelatende personvern: Spørsmålene man bør stille seg selv

Ta med deg denne artikkelen dit du trenger den.

↓ Markdown ↓ Klartekst ↓ PDF

Filen lastes ned til enheten din. Derfra kan du lagre den, importere den til Solo2 eller dele den hvor du vil. Cuadernos bestemmer ikke destinasjonen for deg.

Lakksegl · SHA-256 4cfdf3fd80207a054f8ff72d7af3b4cb6bca8a25d22d39fcc8a98fcbbf8a6ee6

Cuadernos Lacre · En utgivelse fra Menzuri Gestión S.L. ·
skrevet av R.Eugenio · redigert av teamet bak Solo2.

Dette nettstedet bruker ikke informasjonskapsler. Alt som nettleseren din laster inn, er skrevet eller overvåket av oss og plassert på våre europeiske servere: den anonyme besøkstelleren (Umami, selvhostet) og det minimale JavaScript som kreves for språkvelgeren og innstillingen din for lyst eller mørkt tema, som lagres på din egen enhet. Ingen ressurser fra eksterne selskaper, ingen trackere, ingen profilering, ingen deling av data. Hvis du vil følge oss: RSS.