# Self-hosting als professionele praktijk

Een server is niets meer dan een computer. De vraag is niet of u er een moet hebben, maar waar de gegevens van uw klanten staan, wie ze beheert and wie de verantwoordelijkheid draagt als er iets misgaat.

**Om het even duidelijk te zeggen:** Uw gegevens leven altijd in iemands computer: in die van een gigant die u alles toevertrouwt, in een gehuurde die u beheert, of in de uwe eigen. Hoe meer controle u wilt, hoe meer verantwoordelijkheid u op u neemt. Delegeren aan een grote derde partij stelt gerust, maar ontslaat niet: de informatie is van u —and van uw klanten—, and de verantwoordelijke bent u.

## De vraag tussen de cloud en de kelder

Het is goed om te beginnen met het demystificeren van een woord dat onnodig afschrikt: server. Een server is geen mysterieuze machine in een gekoelde ruimte. Het is simpelweg de computer van iemand anders —of die van jezelf— die informatie opslaat en deze levert aan degene die erom vraagt. Decennialang bewaarden we de gegevens van onze klanten in een map, in een archiefkast, op het bureau, en niemand lag daar wakker van. Informatie was niet eng omdat het op papier stond; het hoeft ook niet eng te zijn omdat het op een schijf staat.

De «cloud» is ook niet vluchtig. Het is de computer van een bedrijf, bijna altijd ver weg en bijna altijd van iemand anders. Ik leerde dit onbedoeld op de dag dat ik, in het volste vertrouwen dat mijn bestanden veilig op Google Drive stonden, ontdekte dat de map op mijn computer niet mijn documenten bevatte, maar snelkoppelingen naar documenten die ergens anders stonden. Als die andere plek zou besluiten te sluiten, de prijs te wijzigen of de dienst op te zeggen, zou mijn gemoedsrust ermee verdwijnen. Ik bezat mijn spullen niet; ik had toestemming om ze te raadplegen.

Daaruit ontstaat de vraag van dit Schrift, eenvoudiger te stellen dan te beantwoorden: waar zouden de gegevens van uw klanten moeten wonen? En uw eigen gegevens? Het publieke gesprek stelt het voor alsof er maar twee tegengestelde antwoorden zijn — de cloud van de grote platforms of het zelf opzetten —, bijna een kwestie van welk kamp je kiest. Maar het zijn geen twee wegen: het zijn er drie, en geen ervan is een geloofsdaad. Rustig gelezen hebben ze meer nuances en vragen ze meer dan het lijkt.

## Dit gaat u aan, wat u ook verkoopt

Het is gemakkelijk om te denken dat vertrouwelijkheid een zaak is van advocaten, artsen of journalisten, and dat de rest niets te verbergen heeft. Dat is een fout, and een dure ook. Bijna elk bedrijf bewaart klantgegevens die onder de wet vallen, and velen bewaren, zonder het te weten, informatie die veel gevoeliger is dan het lijkt.

Een bankenwinkel noteert de naam, het adres en het telefoonnummer van wie er koopt; bij financiering ook diens financiële gegevens. Een verbouwings- of decoratiebedrijf bewaart foto's van het interieur van de huizen van zijn klanten en de volledige plattegronden van hun woningen. Een schoonmaakbedrijf hanteert de plattegronden van de kantoren die het schoonmaakt, vaak gemarkeerd met kleuren en cijfers die aangeven welke werknemer waar binnenkomt, op welk uur en met welke sleutel. Niets daarvan lijkt veel voor te stellen totdat je je afvraagt voor wie het nog meer waarde zou hebben: die schoonmaakplattegronden zijn, door andere ogen bekeken, de perfecte kaart voor wie wil inbreken om te stelen.

Dat een bedrijf klein is, of sofa's verkoopt in plaats van rechtszaken verdedigt, maakt de gegevens niet waardeloos and zorgt er niet voor dat de wet niet meer van toepassing is. Het zorgt er alleen voor dat de eigenaar er meestal minder over nadenkt. And weinig nadenken over iets dat uw verantwoordelijkheid is, is precies waar de problemen beginnen.

## Waar staan uw gegevens?

Op die vraag zijn er in essentie drie antwoorden. En het is goed om te onthouden dat “de gegevens” niet alleen het dossier van een klant of het pak facturen en offertes zijn: het zijn ook uw gesprekken met hem — via WhatsApp, via een professionele chatdienst, via Solo2. De drie antwoorden die volgen zijn geen gradaties van zuiverheid, noch een ladder van goed naar slecht: het zijn drie manieren om hetzelfde te verdelen, de controle en de verantwoordelijkheid.

**Alles aan een aanbieder uitbesteden.** Het is het meest gebruikelijke, en voor de meesten is het het enige wat ze kennen. Ik zet alles in Google Workspace of in Microsoft 365 en vertrouw het volledig toe aan de aanbieder. Ik betaal mijn abonnement en hoef er niet meer over na te denken. De meest extreme vorm hiervan zijn de diensten waarbij u niet eens uw eigen gegevens in handen krijgt: bepaalde facturatieprogramma's in de cloud bewaren bijvoorbeeld uw facturen en offertes — en werken heel goed —, maar de informatie leeft in hun systeem, niet in het uwe. Zolang u betaalt, hebt u toegang; de dag dat u vertrekt, ontdekt u dat het meenemen van uw eigen historie moeilijk of onmogelijk is. Uw gegevens half in gijzeling houden is voor meer dan één aanbieder precies wat verhindert dat u naar de concurrentie vertrekt. In ruil voor gemak geef ik de controle uit handen en — zonder het hardop te zeggen — het gevoel dat de verantwoordelijkheid niet meer de mijne is. Hier past een nuance die bijna nooit wordt gemaakt: uitbesteden is niet synoniem met Amerikaans. Ik kan alles net zo gemakkelijk uitbesteden aan een Europese aanbieder — Infomaniak, bijvoorbeeld — en in één klap een groot deel van de twijfels over internationale doorgiften oplossen die we bij “Schrems II” zagen, zonder iets zelf te hosten. Het is niet de Verenigde Staten tegen de rest van het universum: binnen de zuivere uitbesteding zijn er al beslissingen die ertoe doen.

**Uw eigen server huren en beheren.** Ik heb hetzelfde als wat Microsoft of Google me zouden geven, maar ik richt het zelf in. Ik huur een server bij een Europese provider —Hetzner, OVH, Scaleway—, installeer vrije software (bijvoorbeeld Nextcloud voor bestanden) and beheer zelf het resultaat. Ik krijg echte controle: ik weet wat er draait, waar en waarom. Maar de machine bevindt zich nog steeds in het datacenter van een derde partij en bovenal verandert wie de gevolgen draagt. Door te delegeren heb je iemand om de schuld te geven als er iets misgaat. Door het zelf te beheren is de kans groot dat de schuld bij jou ligt.

**Het op uw eigen computer hebben.** Dit is de optie die bijna niemand vertelt, en het is het hart van dit Cahier. Je hebt geen enorme server nodig die vierentwintig uur per dag aan staat in een macro-datacenter om je spullen te hosten. Je computer op kantoor is al een server: hij dient jou. Je laat hem op kantoor aan staan en maakt er verbinding mee vanaf je laptop bij een klant, of vanaf je mobiel als je thuis bent. We noemen het «de computer op kantoor», niet «de server», maar hij doet precies hetzelfde als de twee vorige opties. De controle is maximaal en de nabijheid ook: uw gegevens zijn waar u bent. De keerzijde, onverbloemd gezegd, is dat de verantwoordelijkheid ook maximaal is. Als de stroom uitvalt, is er geen storingsmonteur in Neurenberg: jij moet zelf de zekering omhoog zetten. En om die computer van buitenaf toegankelijk te maken, is er iets nodig dat de brug slaat tussen uw laptop en die computer. Dat is geen magie, en het is goed om dat te weten voordat u voor dit pad kiest.

En je hoeft niet eens de kantoorcomputer te hergebruiken: er bestaat een apparaat dat precies hiervoor is ontworpen, de NAS (gemaakt door Synology, QNAP en anderen). Zoals bijna alles wat we in deze Cuadernos hebben gezien, zit er vanbinnen geen magie: het is een gespecialiseerde computer, hetzelfde type machine dat je in een datacenter zou huren, alleen gebouwd om gegevens op te slaan en ze via het netwerk te leveren, zonder monitor of toetsenbord ertussen. Sluit er een scherm en een toetsenbord op aan en je hebt een gewone computer; installeer de juiste software op je pc en je hebt een NAS. Het verschil is dat de NAS klaar voor gebruik wordt geleverd. Je koopt hem, je sluit hem thuis of op kantoor aan, en hij is van jou. Je betaalt geen maandelijks abonnement; je betaalt één keer en hij is van jou, zoals elk ander gereedschap van je bedrijf. Je zet hem aan, je

zet hem uit, je neemt hem desgewenst mee naar een andere plek. En omdat hij van jou is, weerhoudt niets je ervan er twee te hebben —een thuis, een op kantoor— of drie, door er een toe te voegen op een veilige plek, onderling gesynchroniseerd: je eigen redundantie, zonder afhankelijk te zijn van een derde partij die het onderhoudt. Zelfhosting is uiteindelijk niet één ding: het is een combinatie van machines, van eigendom, van locaties en van software.

Hier is het onvermijdelijk om te benoemen wat wij doen, en we doen het zonder vermomming: bij Solo2 wordt die brug door de applicatie zelf geslagen. De computer op uw kantoor blijft alleen toegankelijk voor uw vertrouwde apparaten, en altijd versleuteld, en uw overige apparaten verbinden er zelf weer mee. Wanneer een klant met u praat, is het uw computer — niet die van een derde — die met de klant praat. Wij lossen de stroomstoring niet op; wij lossen de brug op. En wij zijn niet de enigen: voor bijna elke behoefte bestaan er tegenwoordig programma's — vrij of propriëtair — die precies dit mogelijk maken, de gegevens op uw eigen apparaat hebben en er van buitenaf bij komen. Het onze is een voorbeeld; wat telt is het idee, niet het merk.

## Redundantie is geen superkracht

Hier rijst het onmiddellijke bezwaar, and dat is redelijk: als ik alles op mijn computer op kantoor heb, wat gebeurt er dan als hij kapot gaat? De vraag is goed. Het antwoord is dat het vangnet dat we ons voorstellen bij de grote providers bescheidener is —and gemakkelijker na te bootsen— dan het lijkt.

Wanneer ik mijn gegevens achterlaat in het datacenter van een multinational, vertrouw ik erop dat deze op meerdere plaatsen kopieën heeft. And waarschijnlijk heeft hij die ook: op een tweede locatie, misschien op een derde. Maar die redundantie is niet oneindig and bovenal is zij niet van mij: het blijft een harde schijf waarvan ik niet de eigenaar ben, beheerd door iemand in wie ik een geloof stel dat ik bijna nooit verifieer.

Datzelfde netwerk kan ik zelf weven, and met een doorslaggevend voordeel. Mijn dagelijkse dienst staat op de computer op kantoor. Vandaaruit bewaar ik een versleutelde kopie op de computer van een bevriend bedrijf —een vakgenoot, een ander vertrouwd kantoor— and een andere versleutelde kopie, als ik dat wil, bij diezelfde Europese provider waar we het over hadden. Het verschil is alles: wat ik buiten laat staan is niet mijn dienst of mijn gegevens in klare taal, maar een versleutelde kopie die alleen ik kan openen. De externe provider bewaart een gesloten kist waarvan hij de sleutel niet heeft. Ik vertrouw hem mijn informatie niet toe: ik vertrouw hem enkele bytes toe die zonder mij niets betekenen.

## Het was veilig totdat het dat niet meer was

Staat u mij een persoonlijk verhaal toe, want dit illustreert de zaak beter dan welk argument ook. Meer dan tien jaar lang was ik een trouwe klant van CrashPlan, een technisch buitengewone back-updienst. Ik maakte in hun cloud een back-up van al mijn computers en die van mijn gezin —van de zaak en van thuis, alles—, met versies die ik met elke gewenste frequentie kon herstellen, waarbij ik terug in de tijd reisde naar een specifiek bestand van maanden geleden. Na de eerste kopie verzond het alleen de wijzigingen, versleuteld en gecomprimeerd, zodat ik zonder noemenswaardige inspanning een enorme back-up up-to-date hield. Het heeft me vele malen gered, van een onbeduidend document tot een hele schijf. De prijs steeg in de loop der jaren en het maakte me niet uit: ik betaalde met plezier.

Wat ik niet wist, was dat CrashPlan een rekenfout had gemaakt: ze hadden contractueel onbeperkte opslag beloofd, zowel in ruimte als in tijd. En ruimte vermenigvuldigd met tijd —jaren geschiedenis, versies om de paar minuten— groeit totdat het onhoudbaar wordt. Op een dag kregen we allemaal te horen dat de dienst stopte. Ze deden dit met elegantie en met een royale termijn, bijna een jaar, en gaven ons de middelen om onze gegevens te downloaden. Maar waar ga je heen met meer dan tien jaar aan versie-kopieën van al je schijven? Daar ontdek je dat je noch de manier hebt om alles te downloaden, noch een plek hebt om het te laten, en dat, zelfs als het zou kunnen, het nieuwe magazijn een fortuin zou kosten.

Ik redde vier onmisbare dingen. De rest verdween toen ze de schakelaar omlegden. Ik was gerust, mijn informatie was veilig... totdat ze dat niet meer was. En niet door verraad: CrashPlan gedroeg zich onberispelijk — anders dan Evernote, dat zich jaren later schandelijk gedroeg —; heel eenvoudig besloot mijn beschermengel in de cloud, met alle recht, om dat niet langer te zijn. Het resultaat was voor mij identiek: wat ik veilig waande, verdween.

Wat dit verhaal echt leert, heeft meer met de menselijke natuur te maken dan met technologie. Wanneer iemand voelt dat iets zijn eigen verantwoordelijkheid is, handelt hij preventief: hij maakt kopieën, dekt zich in, is wantrouwend met een goed oordeelsvermogen. Wanneer hij —ten onrechte— gelooft dat de verantwoordelijkheid wordt gedragen door een grote en solvabele derde partij, ontspant hij en laat hij het beloop. Die gedelegeerde rust is geen wijsheid: het is, onverbloemd, een vorm van onverantwoordelijkheid.

## Betalen is niet hetzelfde als voldoen

Die rustige onverantwoordelijkheid lijkt veel op die van ouders die hun zoon inschrijven op de duurste school, daarna een master voor hem betalen en daarmee geloven dat ze aan hun plicht hebben voldaan. Ze hebben niet aan hun plicht voldaan. Ouder zijn is je zorgen maken over wat hij vandaag heeft geleerd, over wat hij niet begrijpt, over zijn waarden, over zijn zelfvertrouwen. Als die zoon op vijfentwintigjarige leeftijd niet weet hoe hij moet werken of zich moet gedragen, ligt de schuld niet bij de school die het geld heeft geïncasseerd: die ligt bij degene die delegeerde en betaalde in de overtuiging dat dat genoeg was. Een derde partij betalen ontslaat niet van verantwoordelijkheid. Dat heeft het nooit gedaan.

Met gegevens gaat het precies zo, en de recente geschiedenis bevestigt het. Vijftig of honderd jaar geleden bewaarde een professional de zaken van zijn klanten in mappen, op kantoor of thuis, en voelde zich daarvoor verantwoordelijk. Er ging zelden iets verloren. We zijn de digitale wereld binnengestapt en uploaden, met verbluffend gemak, alles naar “de cloud” — die niets meer is dan de computer van een multinational — en maken ons geen zorgen meer. En vaak gebeuren er ongelukken, en zijn er bedrijven die alles verliezen, en dan wordt er gezegd: het was de schuld van Google, het was de schuld van Microsoft. Nee. De informatie is van u, of van uw klanten, maar de verantwoordelijke bent u.

Uw eigen hosting is geen technische gril: het is het terugkrijgen van die sereniteit van decennia geleden, die van weten waar elk ding is en waarom. De gegevensbescherming heeft ondertussen een abrupte slingerbeweging meegemaakt —van de afwezigheid van enige norm, toen iedereen zonder nadenken klantgegevens tentoonstelde, naar een eis die met onevenredige hardheid op de kleinste valt, de zzp'er die het telefoonnummer van een klant aan de bezorger geeft. Ik discussieer niet over het doel; ik observeer de discrepantie. Maar de discrepantie ontslaat ons niet: de dag dat de overheid de middelen heeft om op grote schaal te traceren en te sanctioneren, zal omvang niemand meer beschermen, en het is verstandig om die dag niet af te wachten met een ongeorganiseerd huis. De gegevens onder eigen controle hebben helpt om te voldoen en helpt om dat aan te tonen. En bovenal zet het de zaken terug op hun plaats: wanneer de informatie van u is, is de verantwoordelijkheid volledig van u —er is geen derde partij om de schuld te geven, noch een derde partij wiens falen u blootstelt—.

## Verantwoordelijkheid beschermt ook

Het zou oneerlijk zijn dit zonder schaduwzijden te schilderen. De plaats van de tussenpersoon innemen betekent dat je het zijne moet dragen: back-ups bijhouden, updates toepassen en een wettelijke verantwoordelijkheid — die van de RGPD — die in werkelijkheid nooit helemaal heeft opgehouden de uwe te zijn (de voetnootverwijzingen geven de artikelen in detail). Er is werk, en er is een dag waarop er iets op een ongelegen moment misgaat. We verbergen het niet.

Maar de angst die rond dat woord, verantwoordelijkheid, hangt, is verkeerd afgesteld. Het is veel gemakkelijker om uw bestanden te verliezen in een clouddienst die de deuren sluit, of uw foto's in Google Foto's, dan om die map met belangrijke documenten te verliezen die u op uw eigen computer hebt: die waarvan u weet waar hij

staat en waarvan u het ontbreken zou merken zodra hij verdween. Wat u als het uwe voelt, verzorgt u; wat u veilig waant in handen van een ander, verwaarloost u.

Denk aan de fotoalbums van vroeger, die van ontwikkeld papier, bewaard in een la. Hebt u ooit iemand horen zeggen dat hij zijn familiealbum “kwijt” is? Je hoort over het huis dat afbrandde met het album erin; het zomaar verliezen, nee. En daarentegen mensen die al hun foto's in Google Foto's of in Apple Foto's hadden en met niets achterbleven: dat verhaal keert om de paar maanden terug, omdat ze dachten dat het veilig was. Google Foto's verzorgt uw foto's, jazeker; maar het verzorgt ze niet zoals ouders het album verzorgen waarin hun kinderen en kleinkinderen staan. Dat verschil lost geen enkel datacenter op: verantwoordelijkheid, wanneer ze de uwe is, is niet alleen een last; ze is ook de beste garantie.

# Vier vragen voor het beslissen

Als u overweegt de stap te zetten, in welke vorm dan ook, is het goed om eerst vier vragen met nuchtere eerlijkheid te beantwoorden:

1. Welk deel van uw gegevens zou pijn doen om te verliezen, of niet te kunnen meenemen? En pas op met het afdoen van het “routinematige”: de factuurhistorie lijkt het prozaïschste ter wereld totdat u van programma wisselt en ontdekt dat die facturen van de aanbieder waren, niet van u — dat u ze hooguit als PDF kunt afdrukken, zonder er nog in te kunnen zoeken. Het is niet alleen een kwestie van gevoeligheid: het gaat erom van wie datgene wat u moet bewaren werkelijk is.
2. Welke optie is in verhouding tot uw werkelijke technische kunde? Een goed onderhouden eigen computer is binnen ieders bereik; een hele server beheren, een stuk minder. Wees eerlijk over wat u wel en niet weet. En onthoud dat er tussen het opzetten van een hele server en alles uitbesteden een heel redelijk middenterrein ligt: programma's — vrij of propriëtair — die uw gegevens op uw eigen apparaat bewaren en u er van buitenaf bij laten. Voor veel mensen is dat het beste evenwicht.
3. Wat is uw plan voor de slechtste dag? Een inbreuk, een schijf die sterft, een provider die sluit, de technicus in de ziektewet. Als het plan begint met «het zou niet mogen gebeuren», is het geen plan.
4. Zou u weten hoe u kunt bewijzen dat u aan de regels voldoet als u morgen wordt gecontroleerd? Het goed doen en kunnen bewijzen dat u het goed doet zijn niet hetzelfde. De wet vraagt om het tweede.

Er is geen universeel antwoord. Er is een proportioneel antwoord, aangenomen met eerlijkheid over wat er gewonnen wordt en wat er geërfd wordt. En boven de techniek staat een eenvoudige zekerheid: uw gegevens leven in iemands computer. De enige vraag die er echt toe doet, is van wie u wilt dat die computer is.

---

*Self-hosting is noch een deugd noch een ondeugd: het is een instrument met een concrete voetafdruk van capaciteiten en verantwoordelijkheden. De vraag was nooit of u de uwe moest hosten, maar wat, hoe en met welk ondersteuningsnetwerk. Het terugkrijgen van de controle over gegevens is niet terugkeren naar de kelder noch alles wantrouwen: het is terugkeren naar het zich verantwoordelijk voelen voor wat van ons is, zoals wanneer die gegevens in een map op tafel leefden. Die verantwoordelijkheid, mits goed begrepen, is de werkelijke dienst die een professional aan zijn klanten verleent.*

## Bronnen und verdere lectuur

- Verordening (EU) 2016/679 — artikel 28 (verwerker), artikel 32 (beveiliging van de verwerking), artikel 33 (melding van een inbreuk), artikel 37 (aanwijzing van de functionaris voor gegevensbescherming).
- Spaans Agentschap voor Gegevensbescherming — *Praktische gids voor risicoanalyse bij de verwerking van persoonsgegevens* (huidige revisie). Kader voor verwerkingsverantwoordelijken die eigen technische functies op zich nemen.
- Europees Comité voor Gegevensbescherming — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Ook toepasbaar op de proportionaliteitstoets bij beslissingen over eigen infrastructuur.

- Europese Commissie — openbaar register van aanbieders van informatiediensten die gevestigd zijn in Europese jurisdictie. Administratief startpunt voor het identificeren van Europese managed hosting opties.
- Nextcloud GmbH (Duitsland) — *Nextcloud Enterprise architecture and compliance documentation*. Gedocumenteerde casus van vrije software met self-hosted en door een Europese provider beheerde modaliteiten; nuttig als technische referentie van een project dat sinds 2016 in Europese jurisdictie wordt onderhouden.

← VorigeDe 24 woorden: wat een cryptografische identiteit isVolgende →Echte vs. schijnbare privacy: de vragen die men zich moet stellen

## Recente artikelen


- Reflectie · 29 juni 2026 Je bent niet anoniem
- Reflectie · 27 mei 2026 Wat een handtekening niet kan oplossen
- Analyse · 26 mei 2026 Echte vs. schijnbare privacy: de vragen die men zich moet stellen


Neem dit artikel mee naar waar u het nodig heeft.

↓ Markdown ↓ Platte tekst ↓ PDF

Het bestand wordt gedownload naar uw apparaat. Van daaruit kunt u het opslaan, importeren in Solo2 of delen waar u maar wilt. Cuadernos beslist niet voor u over de bestemming.

Lakzegel · SHA-256 d4dc5fdb6142203deb355e8f9450577f09922c4411487e1276e73c2e079963eb



Cuadernos Lacre · Een uitgave van Menzuri Gestión S.L. ·
geschreven door R.Eugenio · geredigeerd door het team van Solo2.