Analyse · 26 mei 2026

← Vorige·Volgende →

Echte vs. schijnbare privacy: de vragen die je je het beste kunt stellen

Operationele synthese van cyclus 2: de vragen die een dienst met architectonische privacy onderscheiden van een dienst met declaratieve privacy. Een vragenlijst voor de Europese professional voordat hij een digitaal hulpmiddel voor gevoelige gegevens in gebruik neemt.

Om elkaar te begrijpen: Twee diensten met dezelfde juridische kennisgeving kunnen zich heel verschillend gedragen. De ene beschermt door technisch ontwerp. De andere beschermt door contractuele belofte. Het verschil is niet te lezen in de kennisgeving — het wordt ontdekt door de concrete vragen te stellen. De kwaliteit van de antwoorden zegt evenveel over het product als de eigen inhoud ervan.

Het verschil tussen architectonische en declaratieve privacy

In de loop van de zeven voorgaande artikelen van deze cyclus hebben we verschillende lagen van hetzelfde onderwerp doorlopen. Het recht van de internationale doorgiftes met Schrems II. Het wiskundige idee van de cryptografische hash die elk Cuaderno verzegelt. De architectonische keuze van de kill switch en de institutionele inbeslagname die deze bijna altijd vergezelt. Het mechanisme van de end-to-end-versleuteling en de operationele vraag waar de sleutels zich bevinden. De afstemming van de prikkels volgens het bedrijfsmodel. De zelfsoevereine cryptografische identiteit. De self-hosting als evenredige strategie. Elk artikel behandelde één invalshoek. Dit artikel, het laatste van de cyclus, brengt ze samen in een vragenlijst.

Het onderscheid dat het waard is te onthouden is eenvoudig: er zijn diensten waarvan de privacy *architectonisch* is en er zijn diensten waarvan de privacy *declaratief* is. De eerste is ingebed in het technische ontwerp: bepaalde schendingen van de privacyverbintenis zijn technisch moeilijk of onmogelijk omdat de architectuur ze niet toestaat. De tweede is neergelegd in de tekst van de juridische kennisgeving: bepaalde schendingen zouden contractueel sanctioneerbaar zijn als ze zich voordoen, maar technisch belet niets ze. Beide modellen kunnen aan de AVG voldoen; maar het ene beschermt door constructie en het andere beschermt door belofte, en het verschil is operationeel enorm.

De vragen die volgen zijn ontworpen om het ene geval van het andere te onderscheiden. Het zijn geen geavanceerde technische vragen. Het zijn de vragen die elke eerlijke aanbieder in zijn openbare documentatie kan beantwoorden. De kwaliteit en nauwkeurigheid van het antwoord zegt evenveel over het product als het antwoord zelf. De vragen zijn gegroepeerd in zes lagen; het is goed ze allemaal te stellen voordat men de dienst voor gevoelige gegevens in gebruik neemt, niet alleen die welke het eerste instinct herkent.

Laag 1: architectuur

Laten we eerst een term vastleggen. Met *operator* bedoelen we het bedrijf dat de dienst levert: de entiteit die de servers en de software beheert, niet een specifieke persoon. Nu dat duidelijk is, luidt de architectonische kernvraag: wat doet de operator met de inhoud tussen afzender en ontvanger? Er zijn drie mogelijke antwoorden en het loont de moeite ze te kunnen onderscheiden, want alle drie worden soms met vergelijkbare bewoordingen aangeprezen.

- Het eerste: de inhoud loopt in leesbare vorm via een server van de operator, waar de operator hem kan lezen ook al belooft hij dat niet te doen.
- Het tweede: de inhoud loopt versleuteld via een server van de operator, waar de operator hem niet kan lezen als de sleutels zich uitsluitend op de apparaten van de gebruikers bevinden.
- Het derde: de inhoud loopt via geen enkele server van de operator, omdat er in die concrete stroom geen server van de operator bestaat.

Het verschil tussen deze drie is niet een verschil van graad: het is een verschil van soort.

De aanvullende vraag — reeds geformuleerd in het Cuaderno over versleuteling — luidt: wie heeft de cryptografische sleutels die het lezen van de inhoud mogelijk maken? Als de gebruiker ze heeft en alleen de gebruiker, is de versleuteling echt. Als de operator ze daarnaast in welke vorm dan ook heeft — zelfs onder de naam «accountherstel» of «synchronisatie tussen apparaten» —, is de versleuteling nominaal. De vraag laat geen eerlijk tussenantwoord toe.

Laag 2: bedrijfsmodel

De vraag over het bedrijfsmodel is even belangrijk als de architectonische vraag, en om dezelfde wezenlijke reden: prikkels brengen in de loop van de tijd systematisch verschillende producten voort, zelfs met identiek verklaarde doeleinden. Hoe verdient de operator vandaag geld? Eén enkele bron, twee, een mengeling? Als de financiering reclame of het te gelde maken van gegevens omvat, welke gegevens worden te gelde gemaakt en op welke rechtsgrondslag van de AVG gebeurt dat? Dekt het in de juridische kennisgeving verklaarde doel de gegevens van derden die de professional aan de dienst wil toevertrouwen?

En de vraag van de tweede orde, niet altijd geformuleerd: wat is de financiële situatie van de operator op een termijn van drie tot vijf jaar? Een bedrijf in de durfkapitaalfase opereert onder andere druk dan een bedrijf met stabiele winstgevendheid. De wijziging van het financieringsmodel is bij herhaling het moment waarop het impliciete contract met de gebruikers zonder onderhandeling wordt herschreven.

Laag 3: jurisdictie

Voor de Europese professional is de vraag van de jurisdictie niet retorisch. In welke jurisdictie is de operator gevestigd? In welk land staan de servers die de gegevens verwerken fysiek? Is het antwoord op de twee voorgaande vragen hetzelfde of verschillend, en als het verschilt, welke wetgeving is dan van toepassing? Een door een Amerikaans bedrijf geëxploiteerde Europese regio is, voor de toepassing van Schrems II, geen Europees antwoord: het bedrijf is onderworpen aan FISA 702 ongeacht waar de servers staan.

De aanvullende operationele vraag luidt: als er morgen een in de jurisdictie van de operator geldig inlichtingenbevel zou komen dat eist mijn gegevens of die van mijn cliënten te overhandigen, wat zou er dan gebeuren? Als het eerlijke antwoord begint met «het bedrijf zou verplicht zijn ze te overhandigen», beschermt de dienst niet tegen dat bevel, hoezeer de reclame ook het tegendeel suggereert. Als het eerlijke antwoord begint met «het bedrijf zou ze niet kunnen overhandigen omdat het ze niet in leesbare vorm heeft», beschermt de dienst wel; en het verschil hangt bijna volledig af van de eerste twee lagen, niet van de kwaliteit van het privacybeleid.

Laag 4: operator en kill switch

Welke technische capaciteit behoudt de operator om de dienst op afstand op te schorten, te blokkeren, te verwijderen of te degraderen? De vraag is niet paranoïde: ze is operationeel. De digitale platforms hebben die capaciteit de afgelopen jaren herhaaldelijk uitgeoefend, soms op eigen initiatief, soms op bevel van regeringen, soms na wijzigingen van eigendom of beleid. Als de capaciteit bestaat, is het goed te weten onder welke contractueel verklaarde voorwaarden ze wordt uitgeoefend, en een marge te reserveren voor de niet-verklaarde

voorwaarden die de praktijk van de afgelopen jaren even relevant heeft getoond: onverwacht gerechtelijk bevel, internationale sanctie, wijziging van het bedrijfsbestuur, overname door een entiteit met een ander beleid.

De zustervraag is die van het continuïteitsplan: als de operator de capaciteit tegen de professional zou uitoefenen — om welke reden dan ook, terecht of niet —, hoeveel bedrijfstijd zou er dan beschikbaar blijven, welke procedure voor het exporteren van gegevens bestaat er, en naar welke alternatieve aanbieder zou men kunnen migreren? Als het antwoord begint met «dat zou niet mogen gebeuren», is het geen operationeel antwoord; het is een belofte.

Laag 5: identiteit en toegang

Wie beheert de toegangsgegevens van de dienst? Als de operator de toegang van de gebruiker opnieuw kan instellen zonder medewerking van de gebruiker — een procedure die doorgaans «accountherstel» wordt genoemd —, dan is de operator technisch gezien de bewaarder van het account en kan hij het ook overdragen aan wie het via de juiste procedure aanvraagt. Als de operator de toegang niet opnieuw kan instellen omdat de identiteit cryptografisch op het apparaat van de gebruiker ligt, kan de operator hem evenmin overdragen, zelfs niet op bevel. Beide modaliteiten zijn legitiem naargelang de context; maar, nogmaals, ze zijn verschillend, en het is goed te weten welke men in gebruik neemt.

Wat gebeurt er met de gegevens van de professional als de professional de toegang verliest? Bestaan er herstelmechanismen — voor account, bestand, sessie — die van de operator afhangen? Zijn die mechanismen verenigbaar met de beroepsdeontologie van de sector als de operator wordt gedwongen ze te gebruiken?

Laag 6: toekomst

Deze laatste laag wordt vaak verwaarloosd omdat ze projectie vereist. Wat zou er gebeuren als de dienst door een ander bedrijf zou worden overgenomen? Bijna alle overnames brengen in de daaropvolgende maanden een herziening van de gebruiksvoorwaarden met zich mee. Wat zou er gebeuren als de regelgevende eisen zouden veranderen? Het Europese recht heeft de verplichtingen tot verwijdering en blokkering sinds 2022 verhoogd, niet verlaagd. Wat zou er gebeuren als de operator zou verdwijnen? Een aanzienlijk deel van de clouddiensten heeft geen gedocumenteerd uitstapplan voor het scenario waarin de operator stopt; de professional ontdekt het probleem wanneer er geen tijd meer is om het voor te bereiden.

Er is een formulering die het waard is voor deze laag te onthouden: architecturen die minder van de operator afhangen, zijn veerkrachtiger tegen veranderingen van de operator. De self-hosting in al haar modaliteiten, de zelfsoevereine cryptografische identiteit, de communicatie zonder server ertussen, dit alles verkleint het toekomstige risico-oppervlak via de procedure van het verkleinen van het huidige afhankelijkheidsoppervlak. Ze elimineren het niet; ze verkleinen het.

Het verschil tussen structuur en belofte

Als we de cyclus tot één enkele zin moesten distilleren, zou het deze zijn: de structurele antwoorden blijven overeind ook al veranderen de operator, het bestuur of de wetgeving; de antwoorden per belofte blijven overeind zolang degene die belooft ze kan en wil nakomen. Beide kunnen juist zijn op het moment van aanvaarding. Slechts een van de twee houdt stand onafhankelijk van het verstrijken van de tijd en de verandering van de omstandigheden.

Dit betekent niet dat elke professional structurele antwoorden moet eisen van alle diensten die hij in gebruik neemt. De evenredigheid blijft legitiem: een spreadsheet voor interne boekhouding heeft niet hetzelfde antwoord nodig als het medisch dossier van een patiënt. Het betekent wel dat professionaliteit erin bestaat te weten welk soort antwoord men in elk geval heeft aanvaard, en bewust te hebben besloten dat dat soort antwoord evenredig is aan het concrete gegeven.

De vragenlijst, geordend

Twaalf concrete vragen die de cyclus samenvatten, geordend zodat het antwoord op elke vraag de volgende voedt:

1. Loopt de inhoud via een server van de operator? Zo ja: in leesbare vorm, versleuteld met sleutels van de operator, of versleuteld met sleutels die uitsluitend van de gebruiker zijn?
2. Als end-to-end-versleuteling wordt aangevoerd, waar bevinden de cryptografische sleutels zich dan? Kent of bewaart de operator er enig deel van in welke vorm dan ook, inclusief het «herstel»?
3. Welke metadata genereert en bewaart de dienst? Hoe lang? Voor wie zijn ze zichtbaar?
4. Hoe wordt de operator gefinancierd? Als de financiering reclame of het te gelde maken van gegevens omvat, dekt het verklaarde doel dan de door de professional toevertrouwde gegevens van derden?
5. Wat is de financiële situatie van de operator op een termijn van drie tot vijf jaar? Zijn er factoren die wijzen op een ophanden zijnde modelwijziging (aanstaande beursgang, opdrogende financieringsronde, waarschijnlijke overname)?
6. In welke jurisdictie is de operator gevestigd? In welk land staan de servers fysiek? Als ze verschillen, welke nationale wetgeving is dan van toepassing op de verwerking?
7. Wat zou er gebeuren als een in de jurisdictie van de operator geldig inlichtingenbevel zou eisen mijn gegevens te overhandigen? Zou het bedrijf daaraan technisch kunnen voldoen?
8. Welke technische capaciteit behoudt de operator om de dienst op te schorten, te blokkeren of te verwijderen? Onder welke contractuele voorwaarden? Onder welke historisch gedocumenteerde niet-contractuele voorwaarden?
9. Welk uitstapplan bestaat er als de operator die capaciteit tegen mij zou uitoefenen, terecht of onterecht? Is er een gedocumenteerde procedure voor het exporteren van gegevens naar een alternatieve aanbieder?
10. Wie beheert de toegangsgegevens? Kan de operator ze opnieuw instellen zonder mijn medewerking? Beschermt dat mij of stelt het mij bloot?
11. Bestaat er voor deze concrete functie een Europees, zelfgehost of serverloos alternatief? Wat zijn de werkelijke kosten ervan, vergeleken met het beoordeelde risico?
12. Als de beslissing van vandaag over vijf jaar zou worden onderzocht door een inspecteur, een auditor of een door een inbreuk getroffen klant, zou de huidige keuze dan verdedigbaar zijn met de vandaag beschikbare argumenten, of zou ze excuses vereisen voor het niet stellen van redelijke vragen?

De vragen verwachten geen perfecte antwoorden. Ze verwachten eerlijke antwoorden, die de eerlijke operator weet te geven en die de minder eerlijke operator vermijdt nauwkeurig te formuleren. Het operationele verschil tussen de twee soorten operator, dat zeggen we zonder dramatiek, valt meestal op door langzaam de antwoorden te lezen die ze vrijwillig aanbieden, nog voordat men om meer moet vragen.

Met dit artikel sluiten we de tweede cyclus van Cuadernos Lacre af. We begonnen met de van Schrems II geërfde redactionele schuld en eindigen met een operationele vragenlijst. Onderweg hebben we concepten doorlopen — hash, versleuteling, identiteit — en toegepaste analyses — kill switch, bedrijfsmodel, self-hosting. De verklaarde redactionele intentie van de publicatie was niet om de lezer te overstelpen met de uitputtende lijst van problemen, maar om hem hulpmiddelen te geven zodat hij bij elke nieuwe dienst kan onderscheiden welk soort antwoord hij aanvaardt. Dat onderscheid — tussen architectuur en belofte — is het hulpmiddel. De rest zal elke professional ten dienste stellen van de gegevens die hij in zijn praktijk de vraag waardig acht.

Bronnen und verdere lectuur

- Deze publicatie, cyclus 2 (mei 2026) — *Schrems II, vijf jaar later*, *Wat SHA-256 echt is*, *Kill switch en institutionele inbeslagname*, *End-to-end-versleuteling, echt uitgelegd*, *Het verdienmodel als vertrouwenssignaal*, *De 24 woorden: wat een cryptografische identiteit is*, *Self-hosting als professionele praktijk*. De zeven artikelen waarop deze vragenlijst rust.

- Verordening (EU) 2016/679 — Algemene verordening gegevensbescherming. Juridisch referentiekader voor alle vragen die de vragenlijst opwerpt, in het bijzonder de artikelen 5, 6, 25, 28, 32, 33 en hoofdstuk V.
- Europees Comité voor gegevensbescherming — operationele richtsnoeren en adviezen over Schrems II, internationale doorgiftes, effectbeoordelingen en proactieve verantwoording (publicaties 2020-2024).
- Spaanse gegevensbeschermingsautoriteit — gepubliceerde sancties 2022-2024 tegen verwerkingsverantwoordelijken wegens ongeschikte doorgifte-instrumenten of wegens formele effectbeoordelingen zonder wezenlijke inhoud.
- noyb.eu — Europees Centrum voor digitale rechten, geleid door Maximilian Schrems. Openbaar repository van klachten, beroepen en analyses over de werkelijke, niet schijnbare naleving van de Europese regels inzake gegevensbescherming.

← VorigeSelf-hosting als professionele praktijkVolgende →Wat een handtekening niet kan oplossen

Recente artikelen

- Reflectie · 29 juni 2026 Je bent niet anoniem
- Reflectie · 27 mei 2026 Wat een handtekening niet kan oplossen
- Analyse · 25 mei 2026 Self-hosting als professionele praktijk

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 1046c38b68c3958a126e9069c3397068b6a4c206f98ebbd7e0f3eb86e32c4f47

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