Reflectie · 16 mei 2026

← Vorige·Volgende →

Het beroepsgeheim in het digitale tijdperk

Wanneer de communicatie tussen de professional en zijn klant verloopt via een technisch ongeschikt kanaal, wordt het geheim niet gebroken op de dag van het lek. Het werd al veel eerder gebroken, op het moment dat de tool werd gekozen.

Een probleem dat bijna niemand ziet

Een advocaat ontvangt op zijn telefoon een gevoelig document van een klant. Een arts bespreekt met een collega een delicate diagnose. Een psycholoog coördineert met een psychiater de behandeling van een patiënt. Een belastingadviseur verstuurt de gegevens van een aangifte die nog moet worden herzien. Ze doen het allemaal via instant messaging. En bijna niemand staat erbij stil waar die berichten werkelijk terechtkomen.

Het antwoord is in de meeste gevallen hetzelfde: op een server die de professional niet controleert, in een land waarvan hij de wetgeving niet noodzakelijkerwijs kent, beheerd door een bedrijf wiens bedrijfsmodel is – in directe economische termen – om gegevens te verzamelen. Het bericht kan versleuteld zijn in transit. Maar zodra het de server bereikt, is het een kopie die is opgeslagen in de infrastructuur van een derde partij, onderworpen aan de operatieve, juridische en commerciële beslissingen van die derde partij. Niet van de professional.

Wat de wetgeving zegt

De Europese Algemene Verordening Gegevensbescherming is ondubbelzinnig in artikel 32: wie persoonsgegevens verwerkt, moet "passende" technische en organisatorische maatregelen nemen om een op het risico afgestemd beveiligingsniveau te waarborgen. De geschiktheid van de maatregelen wordt niet beoordeeld op basis van "wat de app zegt te doen", maar op basis van het werkelijke risico. Als de gegevens van een klant terechtkomen op een server waarvan de jurisdictie geen beschermingsniveau garandeert dat gelijkwaardig is aan dat van de Europese Economische Ruimte, neemt de verwerkingsverantwoordelijke – dat wil zeggen de professional – een risico waarvan hij zich waarschijnlijk niet volledig bewust is.

En het is niet alleen de AVG. Het beroepsgeheim, dat specifiek geregeld is voor advocaten, artsen, psychologen, auditors, journalisten en anderen, vereist dat de communicatie met de klant vertrouwelijk is. Niet "zo vertrouwelijk mogelijk". Vertrouwelijk zonder nuances. Als het gebruikte technische kanaal dit niet kan garanderen, neemt de professional een risico dat de deontologie van zijn beroep niet toestaat.

De paradox is dat het risico onzichtbaar is. Niemand auditeert de messaging van het kantoor. Niemand vraagt om het gegevensverwerkingscontract van de chatprovider. Het risico komt pas aan het licht als het al te laat is: een lek, een gepubliceerde inbreuk, een gerechtelijk bevel dat op een ander continent is uitgevoerd zonder kennisgeving aan de gebruiker.

Wat een professional technisch nodig heeft

Wat een professional met een beroepsgeheim nodig heeft, is eigenlijk verrassend eenvoudig vanuit het oogpunt van de vereisten:

- Een kanaal waar de berichten rechtstreeks van het apparaat van de verzender naar dat van de ontvanger gaan, zonder via een tussenliggende server te gaan die kopieën opslaat.
- Een infrastructuur waarvan de jurisdictie en het beleid door ontwerp in lijn zijn met de AVG, niet door verklaring.
- Een manier om zich te identificeren bij de gesprekspartner zonder professionele contacten (klantnamen, telefoonnummers, agenda) aan een derde te moeten overhandigen.
- Een verifieerbaar systeem – niet gebaseerd op het woord van de provider – om te bevestigen dat het bericht bij de juiste persoon is aangekomen.

Het is geen veeleisende lijst. Het is eigenlijk wat in de pre-digitale professionele communicatie als vanzelfsprekend werd beschouwd. Een aangetekende brief voldeed aan al die criteria. Een telefoongesprek van de kantoorcentrale naar die van de klant ook. Het vreemde is niet dat deze garanties vandaag de dag worden gevraagd: het vreemde is dat ze verloren zijn gegaan bij de overstap naar het digitale kanaal, zonder dat iemand het merkte.

Het verschil tussen versleutelen en niet opslaan

Er is een nuttige metafoor. Een bericht versleutelen en op een server opslaan is hetzelfde als een document in een kluis stoppen en de kluis bij een onbekende achterlaten. De kluis is goed. Het document kan in principe niet worden gelezen. Maar het document *bevindt zich nog steeds in het huis van een ander*. En die ander kan een gerechtelijk bevel ontvangen, een computeraanval ondergaan, zijn servicevoorwaarden wijzigen, worden gekocht door een ander bedrijf met een andere ethiek, of morgen verdwijnen.

Het structurele alternatief – niet procedureel, niet op basis van vertrouwen – is dat het document het kantoor nooit verlaat. Dat het rechtstreeks van de tafel van de professional naar de tafel van de klant reist, zonder tussenpersoon. Dat is wat point-to-point communicatie tussen apparaten technisch doet: het elimineert de tussenpersoon. Niet dat de tussenpersoon slecht is. Het is alleen zo dat, in het geval van het beroepsgeheim, de tussenpersoon *onnodig* is. En het onnodige moet in elk systeem dat veilig wil zijn, uit principe worden geëlimineerd.

De vraag over verantwoordelijkheid

Uiteindelijk is de vraag die elke professional met een geheimhoudingsplicht met een volmondig ja zou moeten kunnen beantwoorden de volgende:

> Als er morgen een gesprek met een van mijn klanten lekt en een rechtbank of een beroepsorganisatie vraagt me hoe ik de vertrouwelijkheid beheer, kan ik dan technisch bewijzen dat het kanaal dat ik gebruikte geen kopieën opslaat in de infrastructuur van derden? Kan ik bewijzen dat de gegevens de apparaten van de twee personen die aan het gesprek deelnamen nooit hebben verlaten? Kan ik bewijzen, zonder afhankelijk te zijn van het woord van een bedrijf van een ander continent, dat de vertrouwelijkheid werd gegarandeerd door de architectuur en niet door een belofte?

Als het antwoord nee is, is het probleem niet de tool op zich. Het probleem is dat er aan een tool een verantwoordelijkheid is gedelegeerd die de tool niet kon ondersteunen. Het is als het stoppen van vertrouwelijke dossiers in een transparante envelop en erop vertrouwen dat de postbode niet kijkt.

De tool die een professional kiest om met zijn klanten te communiceren, zegt veel over hoe hij hun vertrouwen waardeert. Er zijn tools die zo zijn ontworpen dat dat vertrouwen niet afhangt van beloftes, maar van de architectuur. En er zijn tools die dat niet zijn. Het verschil kennen is onderdeel van het werk.

Geciteerd wettelijk kader

- Verordening (EU) 2016/679 (AVG), in het bijzonder art. 5, 25 (gegevensbescherming door ontwerp) en 32 (beveiliging van de verwerking).
- Nederlandse wetgeving over het beroepsgeheim (o.a. art. 11a Advocatenwet, art. 88 Wet op de beroepen in de individuele gezondheidszorg).
- Wetboek van Strafrecht, art. 272 (schending van geheimen).
- Gedragsregels Advocatuur met betrekking tot vertrouwelijkheid en beroepsgeheim.

← VorigeVersleutelen is niet hetzelfde als privé zijn: wat metadata over u verteltVolgende →AVG en zakelijke messaging: waarom de meesten onbewust in overtreding zijn

Recente artikelen

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

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 c62b570adea79a2a541e7e888d3327fcb2193d210725f7673c8c97c37bddd053

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