Analyse · 16 mei 2026

← Vorige·Volgende →

AVG en zakelijke messaging: waarom de meesten onbewust in overtreding zijn

Bijna elk kantoor, elke praktijk of adviesbureau verstuurt documenten van klanten via applicaties waarvan de server zich buiten de Europese Economische Ruimte bevindt. Zonder kwade bedoelingen, maar in veel gevallen in strijd met de verordening zonder dat iemand hen heeft gewaarschuwd.

Het document dat verder reist dan u denkt

Een alledaagse situatie: een belastingadviseur ontvangt via messaging een document met klantgegevens. Een verkoper stuurt via chat een offerte door naar een collega. Een arts deelt via dezelfde weg een klinisch rapport met een collega. Niemand denkt er twee keer over na. Het is normaal. Het is handig. Het is wat elke dag in elk kantoor in elke stad in Europa wordt gedaan.

Maar dat document is in veel gevallen zojuist naar een server in de Verenigde Staten gereisd. Het is opgeslagen – al is het tijdelijk, al is het "versleuteld in rust" – in een cloud die noch de professional, noch zijn klant controleren. Het is door systemen gegaan die technisch metadata kunnen indexeren die aan de inhoud is gekoppeld. En de Europese Algemene Verordening Gegevensbescherming heeft daar iets heel duidelijks over te zeggen.

Wat de regelgeving vereist

De AVG – en bij uitbreiding de rechtspraak van het Hof van Justitie van de Europese Unie (met name het Schrems II-arrest, C-311/18, uit 2020) – stelt dat de persoonsgegevens van Europese burgers adequaat beschermd moeten zijn. Als die gegevens de Europese Economische Ruimte verlaten, moet de verwerkingsverantwoordelijke garanderen dat de ontvanger een beschermingsniveau biedt dat "wezenlijk gelijkwaardig" is aan het Europese. In de praktijk betekent dit dat het verzenden van klantgegevens via diensten waarvan de servers onder de jurisdictie van de VS vallen, zonder een effectbeoordeling te hebben uitgevoerd en aanvullende waarborgen te hebben geïmplementeerd – modelcontractbepalingen, aanvullende technische maatregelen zoals verifieerbare versleuteling, enz. – een schending van de verordening kan vormen. Ook al heeft niemand er tot nu toe iets over gezegd.

En het gaat niet alleen om de inhoud van de berichten. De metadata – wie wat naar wie stuurt, wanneer, hoe vaak, van waaruit – zijn volgens de regelgeving, volgens de herhaalde interpretatie van het Europees Comité voor gegevensbescherming, ook persoonsgegevens. Een dienst die metadata verzamelt van de professionele communicatie van een gebruiker, verwerkt persoonsgegevens van de klanten van die gebruiker, zonder dat deze daarvan op de hoogte zijn of enige toestemming hebben gegeven voor een dergelijke verwerking.

Het algemene denkschema – "ik gebruik de app alleen om te schrijven; de app is geen gegevensleverancier van mijn klant" – is juridisch onjuist. Als de gegevens van de klant door de infrastructuur van een derde gaan, verwerkt die derde die gegevens. En als hij ze verwerkt, moet er een rechtsgrondslag zijn, een verwerkersovereenkomst en passende waarborgen.

Wie verantwoordelijk is

De vraag wie de juridische verantwoordelijkheid draagt, is niet academisch. De AVG maakt onderscheid tussen de *verwerkingsverantwoordelijke* (wie beslist welke gegevens worden verwerkt en waarvoor) and de *verwerker* (wie dat feitelijk doet, namens de verantwoordelijke). De professional die klantdocumenten verstuurt, is de verantwoordelijke. De provider van de messaging-app is in veel gevallen feitelijk verwerker. Zonder verwerkersovereenkomst – en zonder de meeste bepalingen die een dergelijke overeenkomst zou moeten bevatten – heeft de verantwoordelijke niet aan zijn verplichting voldaan.

De milde interpretatie is: "de meeste professionals weten dit niet". De strikte interpretatie is: "onwetendheid ontslaat niet van naleving". En de interpretatie van elke hierover geraadpleegde gespecialiseerde advocaat in gegevensbescherming is over het algemeen de strikte.

Voor wie dit concreet van belang is

Voor elke professional of elk bedrijf dat, al is het maar incidenteel, persoonlijke informatie van derden verwerkt:

- Advocaten die documentatie van klanten ontvangen (contracten, dagvaardingen, verklaringen, vermogensrapporten).
- Artsen en andere zorgverleners die gezondheidsgegevens delen – die volgens art. 9 AVG als *bijzondere categorie* worden beschouwd, met een versterkt regime –.
- Belastingadviseurs en administratieve consulenten die identificatie-, fiscale en bankgegevens verwerken.
- HR-afdelingen die werk- and personeelsdocumentatie van werknemers beheren.
- Verkopers die contactgegevens en vaak gevoelige commerciële informatie van prospects en klanten ontvangen.

In alle gevallen wordt de informatie beschermd door de AVG. In alle gevallen gaat die informatie in de dagelijkse praktijk via kanalen waarvan de jurisdictie niet toestaat dat ze "wezenlijk gelijkwaardig" worden verklaard aan het Europese kader zonder aanvullende waarborgen. Niet uit kwade trouw. Uit gewoonte. En door een technologische infrastructuur die vijftien jaar lang gemak boven naleving heeft gesteld.

Het argument "iedereen doet het"

Het is raadzaam om vooruit te lopen op het meest voorkomende bezwaar: "als iedereen het doet, kan het geen echt probleem zijn". Het is een volkomen begrijpelijk argument en het heeft juridisch gezien geen enkele kracht. Het feit dat een praktijk wijdverspreid is, maakt deze nog niet in overeenstemming met de verordening. De toezichthouders hebben de afgelopen jaren verschillende bedrijven gesanctioneerd juist voor messaging-gebruik dat onschadelijk leek tot op het moment van de inspectie.

De huidige operatieve realiteit is dat het risico in termen van waarschijnlijkheid laag is – het komt zeer zelden voor dat een inspectie de specifieke messaging-tools van een middelgroot kantoor auditeert – maar hoog in termen van impact als het zich voordoet. Het is een risico dat de meesten nemen zonder te weten dat ze het nemen. Dat wil zeggen, zonder te hebben beoordeeld of de gebruikte tool in lijn is met de juridische verantwoordelijkheid van de verwerkingsverantwoordelijke.

Digitale sporen zijn retroactief

Er is een tweede argument, bijna symmetrisch aan het vorige, waarop we moeten anticiperen: *"als dit een serieus probleem was, was de overheid al lang begonnen met inspecteren"*. De huidige waargenomen realiteit geeft daar oppervlakkig gelijk in. Inspecties wegens oneigenlijk gebruik van messaging in kleine bedrijven en vooral bij zelfstandigen zijn tegenwoordig bijna onbestaand – niet omdat het gedrag is toegestaan, maar omdat het de

overheid, in Nederland en in een groot deel van de EU, ontbreekt aan de nodige menselijke middelen om miljoenen plichtigen te auditeren.

Dat is wat de vandaag waargenomen praktijk suggereert. Het is niet wat het volgende decennium suggereert. Twee factoren komen samen om het evenwicht op relatief korte termijn te veranderen.

Ten eerste: het digitale spoor is retroactief. Elk bericht dat wordt verzonden via een applicatie met een centrale server blijft geregistreerd – althans in metadata – in een infrastructuur die blijft bestaan. Wat zes maanden geleden werd verzonden, is vandaag technisch nog steeds auditeerbaar. Wat vandaag wordt verzonden, zal over vijf jaar nog steeds auditeerbaar zijn. De afwezigheid van een huidige inspectie is geen garantie voor de afwezigheid van een toekomstige inspectie. Het is een uitstel van de beoordeling, geen vrijstelling.

Ten tweede: de administratieve inspectiecapaciteit zal versneld groeien. De introductie van tools voor kunstmatige intelligentie in inspectieprocessen elimineert de menselijke bottleneck die tot nu toe – feitelijk, niet rechtens – kleine bedrijven en zelfstandigen heeft beschermd. Een systeem dat in staat is om massale metadata, belastingaangiften, handelsregisters and meldingsplichten van inbreuken te kruisen, heeft geen inspecteurs nodig: het heeft toegang nodig. En de toegang, via vorderingen bij providers met een juridische aanwezigheid in de EU, is perfect haalbaar onder het huidige wettelijke kader.

Daar komt een minder technische maar even doorslaggevende factor bij: de Europese staten bevinden zich in een proces van aanhoudende schuldenlast en moeten, bijna zonder uitzondering, hun belastinggrondslag verbreden. De administratieve sanctie die voortvloeit uit de niet-naleving van de AVG is, in puur fiscale termen, een groeiende en politiek comfortabele bron van inkomsten. Dat is geen vermoeden: het is een waarneembare trend in de jaarverslagen van de Europese gegevensbeschermingsautoriteiten, waar het totale volume aan sancties al meerdere opeenvolgende boekjaren stijgt.

De operatieve conclusie voor de verwerkingsverantwoordelijke is niet alarmistisch, maar nuchter: **de beslissing over hoe de communicatie met klanten vandaag wordt beheerd, wordt beoordeeld tegen de inspectiecapaciteit van het jaar waarin de inspectie plaatsvindt, niet tegen de huidige.** En die capaciteit zal op redelijke termijn wezenlijk anders zijn dan die van vandaag. Wie vandaag begint de dingen goed te doen, zal niet alleen vanaf vandaag in orde zijn: het spoor dat vanaf dit moment wordt gegenereerd zal consistent zijn met de regelgeving, and dat beschermt retroactief het traject dat komt. Wie doorgaat zoals tot nu toe, verzamelt een auditeerbaar spoor waarvan de conformiteit zal worden beoordeeld aan de hand van de standaarden – en de middelen – van de komende jaren.

Wat er verandert met een andere architectuur

Er bestaan technische alternatieven waarbij de gegevens niet worden opgeslagen in de infrastructuur van derden, maar rechtstreeks van het apparaat van de verzender naar dat van de ontvanger reizen. In die architectuur hangt de naleving van de AVG met betrekking tot internationale doorgifte niet af van modelcontractbepalingen, noch van de goede wil van de provider, noch van toekomstige audits. Het hangt ervan af dat er *geen doorgifte* is. En wat niet bestaat, kan niet worden overtreden.

Dit is geen exclusieve oplossing, noch de enig mogelijke. Maar het is structureel anders, en de naleving van de regelgeving is niet langer een procedurele bijlage, maar wordt een direct gevolg van het ontwerp. Voor een professional die zijn verantwoordelijkheid als verwerkingsverantwoordelijke serieus neemt, maakt dat verschil uit.

De volgende aflevering van Cuadernos zal in detail het Schrems II-arrest en de praktische implicaties daarvan analyseren voor kleine en middelgrote bedrijven die afhankelijk zijn van Amerikaanse clouddiensten, vijf jaar na de publicatie ervan.

Bronnen en wettelijk kader

- Verordening (EU) 2016/679 (AVG), in het bijzonder hoofdstuk V over internationale doorgifte.
- HvJEU C-311/18 ("Schrems II"), 16 juli 2020.
- EDPB – Aanbevelingen 01/2020 over maatregelen die de doorgifte-instrumenten aanvullen.
- Autoriteit Persoonsgegevens – Jaarverslagen met voorbeelden van sancties voor oneigenlijk gebruik van instant messaging in professionele omgevingen.

← VorigeHet beroepsgeheim in het digitale tijdperkVolgende →Wanneer er niemand in het midden is

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 eb73c842029d482aad914a8f45627661a058cbdd5f19dde21663136c7ab53638

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