



Digitale soevereiniteit

Hoe soeverein wil je zijn?

Inhoudsopgave

1. Executive summary
2. Inleiding
3. Wat is digitale soevereiniteit?
 - 3.1 De juridische dimensie
 - 3.2 De technologische dimensie
 - 3.3 De strategische en organisatorische dimensie
4. De definitie die Pegamento hanteert
5. Hoe soeverein is een soevereine cloud?
6. Zo kan het ook
7. Waar begin je?
8. Conclusie
9. Bronnen



1. Executive summary

Digitale soevereiniteit staat hoog op de Europese en Nederlandse agenda, maar in de praktijk blijft het begrip vaag. In deze paper beschrijven we wat digitale soevereiniteit inhoudt, welke definitie Pegamento hanteert en waarom een soevereine cloud van een Amerikaanse hyperscaler niet automatisch soeverein is. Aan de hand van onze eigen keuzes voor open source en Nederlandse hosting laten we zien dat er een werkbaar alternatief bestaat. We sluiten af met een aanpak waarmee iedere organisatie zelf kan bepalen waar afhankelijkheid acceptabel is en waar niet.

2. Inleiding

Digitale soevereiniteit is in korte tijd uitgegroeid tot een centraal thema in het Europese technologie- en beleidsdebat. Overheden, bedrijven en instellingen willen minder afhankelijk worden van buitenlandse technologiebedrijven en meer controle krijgen over hun data, digitale infrastructuur en software. Tegelijkertijd groeit juist de afhankelijkheid van een klein aantal grote cloud- en softwareleveranciers, vrijwel allemaal uit de Verenigde Staten. Veel Europese organisaties draaien hun kritieke systemen inmiddels op platforms van Amazon, Microsoft en Google.

Die afhankelijkheid roept vragen op over controle en jurisdictie. Data die fysiek in Europa staat, kan juridisch alsnog onder Amerikaanse wetgeving vallen. Ook in Nederland speelt dit steeds nadrukkelijker. Onderzoek laat zien dat een groot deel van de digitale infrastructuur waarop publieke diensten draaien wordt geleverd door Amerikaanse technologiebedrijven, met juridische en geopolitieke risico's voor de zeggenschap over data als gevolg (Strop & Verlaan, 2024).

De aantrekkingskracht van deze platforms is goed te verklaren. Ze bieden schaalbaarheid, flexibiliteit en snelle toegang tot nieuwe diensten zoals geavanceerde AI-toepassingen. Uitbesteden helpt organisaties om sneller te ontwikkelen en kosten te verlagen. Daar staat tegenover dat een organisatie met elke uitbestede laag ook een stuk controle over data, technologie en besluitvorming uit handen geeft.

In deze paper verkennen we het begrip digitale soevereiniteit, lichten we toe welke definitie Pegamento hanteert en onderzoeken we aan de hand van voorbeelden uit de praktijk waar de grenzen liggen. De centrale vraag luidt: in hoeverre zijn organisaties bereid het gemak en de brede technologische adoptie van big tech in te leveren voor een echt soevereine oplossing?



Hoofdstuk 3 en 4 gaan over het begrip zelf en over onze definitie. Hoofdstuk 5 laat aan de hand van een actueel voorbeeld zien hoe rekbaar de term soevereine cloud is. In hoofdstuk 6 beschrijven we hoe wij het zelf hebben ingericht, en in hoofdstuk 7 en 8 vertalen we dat naar een aanpak en een antwoord op de centrale vraag.

3. Waarom dit onderwerp nu relevant is

In de context van digitale technologie verwijst soevereiniteit naar de mate waarin een organisatie controle heeft over haar digitale infrastructuur, data en software. Het gaat daarbij niet alleen om de plek waar data fysiek staat, maar ook om wie de technologie ontwikkelt, beheert en juridisch controleert (Europees Parlement, 2020). Wij onderscheiden drie dimensies.

3.1 De juridische dimensie

Wie clouddiensten afneemt van een internationaal technologiebedrijf, krijgt te maken met de wetgeving van het land waar dat bedrijf gevestigd is. Amerikaanse wetgeving zoals de CLOUD Act en FISA 702 geeft Amerikaanse autoriteiten de mogelijkheid om bedrijven te verplichten toegang te geven tot data die zij beheren, ongeacht waar die data staat. Daarnaast kunnen Amerikaanse sancties een leverancier dwingen om de toegang tot systemen en data juist te blokkeren. Het zijn twee verschillende mechanismen met hetzelfde gevolg. De zeggenschap over de data ligt buiten de eigen organisatie en buiten Europa, ook als de data in Europa is opgeslagen (Strop & Verlaan, 2024).

3.2 De technologische dimensie

Moderne digitale diensten zijn ketens van softwarelagen, cloudplatforms en AI-modellen. Een applicatie die op het eerste gezicht Europees oogt, kan onder de motorkap afhankelijk zijn van niet-Europese infrastructuur of componenten. Onderzoek naar cloudbaseerde contactcenterplatforms laat bijvoorbeeld zien dat veel Europese oplossingen draaien op internationale cloudinfrastructuur of gebruik maken van onderliggende technologie die buiten Europa wordt ontwikkeld (ZipTone, 2025). Zo ontstaan verborgen afhankelijkheden in de infrastructuur waarop organisaties vertrouwen.

3.3 De strategische en organisatorische dimensie

Wie afhankelijk is van een specifiek platform, is ook afhankelijk van de prijsmodellen, functionaliteit en contractvoorwaarden van dat platform. Overstappen naar een alternatief is vaak complex en kostbaar, omdat systemen sterk verweven raken met een specifieke cloudomgeving. Dat beperkt de flexibiliteit en de beslissingsvrijheid van de organisatie.

Deze factoren maken digitale soevereiniteit tot een complex vraagstuk. In een wereldwijd digitaal ecosysteem is volledige technologische onafhankelijkheid vaak niet haalbaar. Organisaties staan daarom voor een afweging tussen enerzijds controle over data, infrastructuur en technologie, en anderzijds de voordelen van schaalbaarheid, innovatie en gebruiksgemak die internationale technologieplatforms bieden.

Het concept digitale soevereiniteit draait daarmee uiteindelijk om de vraag in hoeverre organisaties controle willen en kunnen behouden over hun digitale infrastructuur, en welke afhankelijkheden zij bereid zijn te accepteren in ruil voor toegang tot innovatieve technologie en schaalbare digitale diensten.

4. De definitie die Pegamento hanteert

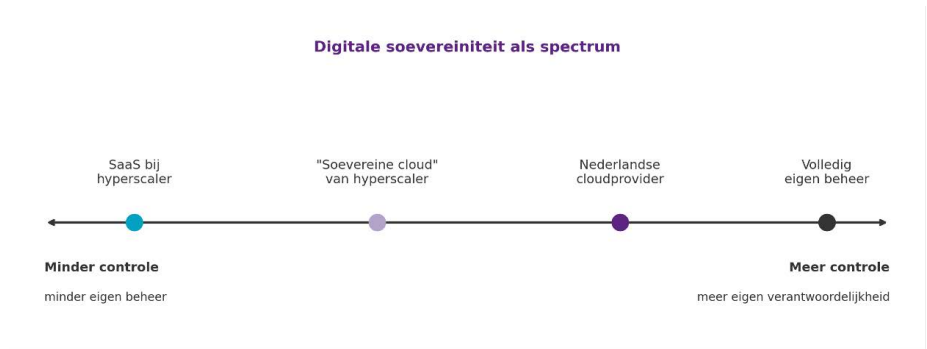
Binnen het brede en soms abstracte debat kiest Pegamento bewust voor een pragmatische benadering. Wij definiëren digitale soevereiniteit als de mate waarin een organisatie daadwerkelijk controle heeft over haar data, infrastructuur en kritieke technologie, en in staat is om bewust met afhankelijkheden om te gaan.

In deze visie draait het niet om het volledig vermijden van externe technologie. Dat is in de huidige digitale werkelijkheid niet realistisch. Vrijwel iedere organisatie gebruikt software, cloudplatforms of componenten van derden. De kern ligt in het kennen en beheersen van afhankelijkheden. Een organisatie moet weten waar die zitten, wat de risico's zijn en hoeveel invloed zij er zelf nog op heeft.

Wij zien digitale soevereiniteit daarom als een spectrum. Aan het ene uiteinde staan oplossingen waarbij vrijwel alles is uitbesteed aan grote cloudleveranciers en de controle grotendeels buiten de organisatie ligt. Aan het andere uiteinde staan omgevingen die volledig in eigen beheer draaien, met maximale controle maar ook een grotere eigen verantwoordelijkheid voor beheer, beveiliging en doorontwikkeling.



De meeste organisaties zitten daar ergens tussenin en maken per systeem een andere keuze.



Figuur 1. Digitale soevereiniteit als spectrum, met enkele herkenbare posities.

Om een positie op dit spectrum te bepalen kijken we naar de drie vormen van controle uit hoofdstuk 2. Welke wetgeving is van toepassing en wie kan toegang tot de data afdwingen of afsluiten. Welke systemen en afhankelijkheden zitten er onder de oppervlakte van een oplossing en wie beheert die. En in hoeverre kan de organisatie zelf sturen, aanpassen of overstappen wanneer dat nodig is.

Deze definitie sluit aan bij de praktijk waarin organisaties opereren. Ze voorkomt een ideologische discussie over volledige onafhankelijkheid en maakt ruimte voor realistische keuzes. Per situatie kan worden bepaald hoeveel controle nodig is en waar afhankelijkheid van externe partijen acceptabel is, bijvoorbeeld vanwege snelheid, innovatie of schaalvoordelen. De kernvraag verschuift daarmee van de vraag of een organisatie volledig soeverein is naar de vraag waar zij bewust controle wil houden en waar niet.

5. Hoe soeverein is een soevereine cloud?

Hoe lastig dit in de praktijk ligt, laat de opkomst van de zogeheten soevereine cloud zien. In februari 2026 kondigde Genesys aan zijn contactcenterplatform beschikbaar te maken via de AWS European Sovereign Cloud, een omgeving die specifiek is ingericht om te voldoen aan Europese eisen rond dataresidentie en governance. De nieuwe regio komt in Brandenburg, Duitsland. Data wordt binnen de EU opgeslagen en verwerkt, de toegang is beperkt tot personeel binnen de EU en de dienstverlening volgt Europese compliance-eisen (Genesys, 2026; No Jitter, 2026).

Op het eerste gezicht is dat een duidelijke stap richting soevereiniteit. Toch laat dit voorbeeld zien dat een soevereine cloud niet hetzelfde is als volledige soevereiniteit. De onderliggende technologie blijft afkomstig van een Amerikaanse hyperscaler. De controle over de infrastructuurlaag en de doorontwikkeling ervan ligt daarmee nog steeds buiten de organisatie die de dienst afneemt, en de betrokken bedrijven blijven onderdeel van een Amerikaans moederbedrijf. Daarmee blijft ook de vraag bestaan hoe extraterritoriale wetgeving op deze omgevingen doorwerkt. Dat leveranciers zo nadrukkelijk op deze zorgen inspelen, bevestigt dat de risico's onderdeel van de afweging blijven.

Er is bovendien sprake van gelaagde afhankelijkheid. Genesys Cloud draait op AWS-infrastructuur, die op haar beurt wordt beheerd en doorontwikkeld door Amazon. Voor de eindgebruiker is die keten zelden volledig inzichtelijk, waardoor een oplossing als soeverein in de markt kan worden gezet terwijl de onderliggende afhankelijkheden gewoon blijven bestaan.



Figuur 2. De gelaagde afhankelijkheid achter een soevereine cloud van een hyperscaler.

Soevereiniteit is in de context van cloudgebruik dus relatief. Leveranciers zetten stappen om beter aan te sluiten bij Europese eisen, maar de fundamentele afhankelijkheid van internationale technologieplatforms verdwijnt niet. De vraag verschuift daarmee van de vraag of een oplossing volledig soeverein is naar de vraag of zij soeverein genoeg is voor de specifieke toepassing.



6. Zo kan het ook

Softwareontwikkeling brengt een breed scala aan beheertaken met zich mee. Developers gebruiken gereedschap dat bijdraagt aan stabiliteit, ontwikkelsnelheid, dataopslag, back-ups en beschikbaarheid van applicaties. De afgelopen decennia bewoog die wereld van bare metal naar virtualisatie, en daarna werden ook de hardware en de virtualisatielaag zelf uitbesteed.

Vrijwel alles werd een dienst, van infrastructuur, platform, netwerk en database tot disaster recovery en serverless computing. Het beheer van dit soort oplossingen is eenvoudig uit te besteden, waardoor organisaties zich niet langer met de onderliggende infrastructuur hoeven bezig te houden.

Dat gemak heeft een keerzijde. Wie bedrijfskritische systemen volledig onderbrengt bij een niet-Europese leverancier, loopt het risico om door sancties of andere maatregelen de toegang tot data en intellectueel eigendom te verliezen. Dat is geen hypothetisch scenario. Bij het faillissement van de Amsterdam Trade Bank in 2022 sloten Microsoft en Amazon vanwege Amerikaanse sancties de cloudomgevingen van de bank af. De curatoren konden niet meer bij essentiële data. Pas nadat de Amsterdamse voorzieningenrechter Microsoft dwong, onder dreiging van dwangsommen die tot honderd miljoen euro konden oplopen, kwam de data beschikbaar (Computable, 2022; Global Trade Review, 2022). De sancties waren gericht op de Russische eigenaren van de bank, maar los van wat je van dat doelwit vindt, raakte het mechanisme Nederlandse curatoren en toezichthouders die hun wettelijke taak niet konden uitvoeren.

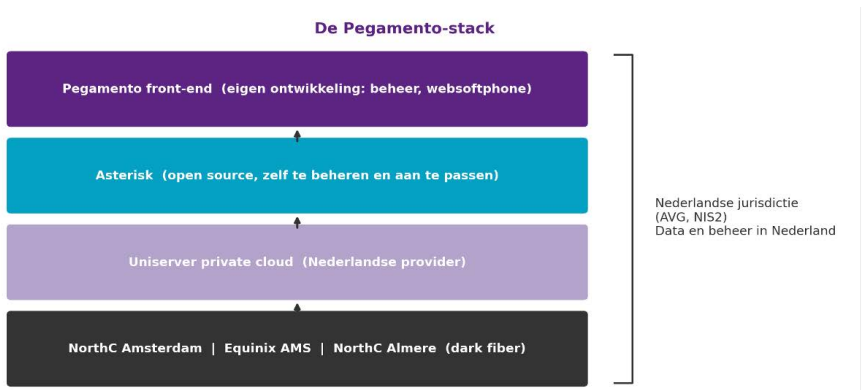
Dat het ook organisaties kan treffen die niets misdaan hebben, liet het Internationaal Strafhof in Den Haag zien. Nadat de Amerikaanse president in februari 2025 per decreet sancties oplegde aan hoofdaanklager Karim Khan, als reactie op arrestatiebevelen van het hof, verloor Khan de toegang tot zijn Microsoft-account en week hij uit naar een Zwitserse e-maildienst. Over de precieze toedracht lopen de lezingen uiteen en Microsoft ontkent diensten aan het hof te hebben stopgezet, maar de les is dezelfde. Een beleidsconflict met Washington volstond om een in Nederland gevestigde internationale instelling in de kern van haar bedrijfsvoering te raken. Het hof stapte daarna over op openDesk, een Europees open-sourcealternatief (Computer Weekly, 2025; Justice Info, 2025).

Hoe actueel dit mechanisme is, bleek in juni 2026 opnieuw, dit keer bij AI. Enkele dagen na de lancering van zijn nieuwste modellen, Claude Fable 5 en Mythos 5, ontving Anthropic van het Amerikaanse ministerie van Handel een exportrichtlijn. Omdat het bedrijf de nationaliteit van gebruikers niet betrouwbaar kon vaststellen, schakelde het de modellen wereldwijd uit. Europese organisaties die op deze modellen hadden gebouwd, stonden van de ene op de andere dag zonder. Begin juli werden de beperkingen weer opgeheven, maar ook dat besluit viel in Washington. Wie AI-modellen van Amerikaanse aanbieders diep in zijn processen verwerkt, doet er dus goed aan om ook daarvoor een alternatief of exitpad klaar te hebben (VRT NWS, 2026; Techzine, 2026).

Onze eigen software, waaronder ons telefonieplatform en AI-toepassingen zoals beeldherkenning en transcriptie, moet in een cloudomgeving draaien en hoog beschikbaar zijn. Bij de inrichting daarvan hebben we een aantal keuzes gemaakt. Sommige daarvan waren destijds misschien eerder intuïtief dan bewust, maar terugkijkend zijn we er blij mee.

De eerste keuze is open source als fundament. Ons Phone System is gebouwd op Asterisk. De volledige front-end, van de beheerapplicatie tot en met de websoftphone, hebben we zelf ontwikkeld bovenop die open architectuur. Asterisk komt oorspronkelijk van een Amerikaans bedrijf, maar doordat de broncode open is, kunnen we de software zelf beheren, aanpassen en desnoods zonder de oorspronkelijke leverancier voortzetten. Open source geeft daarmee een vorm van controle die bij gesloten software ontbreekt.

De tweede keuze is Nederlandse hosting. Voor de hosting van onze oplossingen kozen we voor Uniserver, een Nederlandse cloudprovider waarvan alle datacenters op Nederlands grondgebied staan. De omgeving draait op locaties van NorthC Amsterdam, Equinix AMS en NorthC Almere, onderling verbonden via dedicated dark fiber. Data blijft in Nederland, valt onder de AVG en NIS2 en wordt beheerd door mensen in Nederland. De juridische en de operationele controle liggen daardoor lokaal. Daarnaast wilden we een partner die naast hosting ook ondersteuning en expertise levert op gebieden waarvoor we zelf niet alle kennis of capaciteit in huis hebben.



Figuur 3. De opbouw van de Pegamento-omgeving, van datacenter tot applicatie.

We zijn hierin niet de enige. In april 2026 presenteerden zeven Nederlandse IT-bedrijven, te weten Centric, Info Support, Intermix, KPN, Nebul, Previder en Uniserver, als Open Cloud Alliantie een manifest voor een soevereine overheidscloud, ondersteund door Stichting DINL en TNO. Samen vertegenwoordigen zij twintig datacenters, 13.500 medewerkers en circa 6,5 miljard euro omzet (Open Cloud Alliantie, 2026). Dit zijn geen kleine spelers en het is geen eenmalige marketingactie, maar een oproep aan de overheid om het inkoopbeleid te laten aansluiten op soevereiniteitseisen. Veelzeggend is ook dat Atomic, het moederbedrijf van Uniserver, in diezelfde maand zijn publieke clouddochter CloudNation verkocht aan IG&H om zich volgens CEO Ronald Bezuur volledig te richten op soevereine cloud-, data- en AI-infrastructuur voor Nederland (IG&H, 2026).

Deze aanpak vraagt op architectuurniveau om bewuste keuzes, en die keuzes vragen om opleiding en ontwikkeling van het eigen team. Het is begrijpelijk dat organisaties liever een dienst afnemen dan zelf verantwoordelijkheid dragen voor beheer, beveiliging en doorontwikkeling van de onderliggende infrastructuur. Maar het kan dus wel. Het begint met inzicht in de eigen behoeften, de eigen infrastructuur en de diensten die je vandaag gebruikt. Op basis daarvan bepaal je welke software, data of dienst je als eerste aanpakt, en wordt soevereiniteit een vast afwegingsmoment in het inkoopbeleid en in de samenwerking met partners.

7. Waar begin je?

De vraag is niet hoe ver een organisatie moet gaan in het nastreven van digitale soevereiniteit, maar voor welke onderdelen afhankelijkheid van externe partijen onacceptabele risico's oplevert. Niet iedere toepassing hoeft soeverein te zijn. Een publieke website kan allicht zonder grote bezwaren bij een hyperscaler draaien. Voor bedrijfskritische data, e-mail en eigen software ligt die afweging anders.

Begin met onderzoek en stel per systeem de vraag wat er gebeurt als deze data of dit systeem er morgen niet meer is. Wie merkt dat en welke schade ontstaat er? Een contactcenter as a service kan misschien prima bij een Amerikaanse partij draaien. Maar wie een wettelijke plicht heeft om bereikbaar te zijn, moet weten welk alternatief er klaarstaat op het moment dat een sanctielijst de dienst onbereikbaar maakt, en welk verlies aan functionaliteit daarbij acceptabel is.

Composable architecturen maken het relatief eenvoudig om diensten en services uit te wisselen. Bij werkplekapplicaties zoals Word en Excel lijkt de afweging overzichtelijk. Valt Word weg, dan stap je over op een alternatief. Deze applicaties zijn echter onderdeel van een ecosysteem, en wie het ecosysteem verliest, verliest ook de toegang tot identiteiten, rechten en samenwerkingsomgevingen. De gemeente Groningen onderzoekt samen met de VNG of de werkplek kan overstappen op Linux en andere open-source software (Security.NL, 2026). De grootste uitdaging zit daar waarschijnlijk niet in de technische haalbaarheid, maar in de adoptie binnen de organisatie. Een overstap is dus niet onmogelijk, maar vraagt tijd, voorbereiding en een zorgvuldig implementatietraject.

Ook voor de documenten zelf geldt zo'n afweging. Bestanden met cruciale informatie wil je misschien als eerste op een andere locatie opslaan. Gaat een mkb-bedrijf daarvoor zelf een opslagoplossing inrichten, of kiest het voor het gemak en de integratie van de bestaande applicatiestack? Beide keuzes zijn verdedigbaar, zolang ze maar bewust worden gemaakt en terugkomen in het inkoopbeleid en in de afspraken met partners.



8. Conclusie

De centrale vraag van deze paper was in hoeverre organisaties bereid zijn het gemak en de brede technologische adoptie van big tech in te leveren voor een echt soevereine oplossing. Het eerlijke antwoord is dat de meeste organisaties daar op dit moment nog niet toe bereid zijn, zolang gemak, ontwikkelsnelheid en beschikbaarheid de norm blijven. Die bereidheid groeit pas wanneer de risico's concreet worden, zoals bij de Amsterdam Trade Bank, het Internationaal Strafhof of wanneer wetgeving en inkoopbeleid erom gaan vragen.

Tegelijk laat deze paper zien dat de tegenstelling minder absoluut is dan ze lijkt. Soevereiniteit is geen alles-of-niets keuze maar een spectrum, en op dat spectrum valt wat te kiezen. Een soevereine cloud van een hyperscaler verlegt de grens een stukje, maar laat de fundamentele afhankelijkheid intact. Open source, Nederlandse hosting en een groeiend ecosysteem van serieuze Nederlandse aanbieders maken het mogelijk om voor de systemen die er echt toe doen wel lokale controle te organiseren, zonder al het gemak op te geven.

Keuzes voor een Europees of Nederlands alternatief zullen op de korte termijn soms moeilijke keuzes zijn. Op de lange termijn leveren ze iets op. Kennis blijft behouden, de eigen industrie kan groeien en de organisatie weet van haar kritieke systemen wie erbij kan en wie de stekker eruit kan trekken. Er zijn mogelijkheden genoeg, van groot tot klein. De vraag aan iedere organisatie is welke zij als eerste oppakt.



Auteurs van dit whitepaper: Tobias Hoegen, Business Consultant, en Shannon Breuer, Chief Information & Security Officer (CISO), beiden werkzaam bij Pegamento.

9. Bronnen

Computable (2022). Rechter dwingt Microsoft om data ATB vrij te geven. computable.nl, 4 mei 2022.

Computer Weekly (2025). Microsoft's ICC email block reignites European data sovereignty concerns. computerweekly.com.

Europees Parlement, EPRS (2020). Digital sovereignty for Europe. Briefing PE 651.992.

Genesys (2026). Genesys to Offer Experience Orchestration Services on AWS European Sovereign Cloud. Persbericht, 18 februari 2026.

Global Trade Review (2022). Solvent but bankrupt: how sanctions felled Amsterdam Trade Bank. gtreview.com.

IG&H (2026). IG&H neemt CloudNation over van Atomic Group. Persbericht, 28 april 2026.

Justice Info (2025). How sanctions can weaponize US tech against the ICC. justiceinfo.net.

No Jitter (2026). Genesys to launch sovereign EU cloud. nojitter.com.

Open Cloud Alliantie (2026). Manifest: een Open Cloud voor Nederland. 1 april 2026. opencloudalliantie.nl.

Security.NL (2026). Gemeente Groningen onderzoekt vervangen van Windows door Linux. security.nl, juni 2026.

Strop & Verlaan (FTM Februari 2026). Van het ministerie mag big tech de gesprekken over digitale autonomie zelf leiden.

Techzine (2026). VS blokkeert AI-model Anthropic Fable, wat betekent dit voor Europa? techzine.nl, juni 2026.

VRT NWS (2026). VS dwingt Anthropic beste AI-modellen uit te schakelen. vrt.be, 13 juni 2026.

VRT NWS (2026). Waarom Amerikaanse regering plots krachtigste AI-modellen van Anthropic weer vrijgeeft. vrt.be, 1 juli 2026.

ZipTone (2025). Marktverkenning 'CCaaS made in Europe'





Bij Pegamento geloven we in de kracht van technologie om menselijke connecties te versterken. Onze innovatieve oplossingen voor klantcontact helpen bedrijven optimaal contact te maken met klanten en medewerkers.

We zien technologie niet als vervanging van menselijk contact, maar als versterking ervan. Onze 'Human Lead'-visie combineert geavanceerde technologie met uniek menselijke vaardigheden zoals intuïtie en empathie.

Wij bieden expertise in vier kerngebieden:

1. AI-gedreven intelligentie
2. Omnichannel & Bedrijfstelefonie
3. CX Solutions
4. Computer Vision

Onze belofte is om technologie menselijker te maken met oplossingen die niet alleen efficiëntie verhogen, maar ook de kwaliteit van interacties verbeteren.

Ontdek hoe Pegamento jouw organisatie kan helpen excelleren in een wereld waar technologie en menselijkheid hand in hand gaan.

Neem vandaag nog contact met ons op, dan laten wij zien hoe we samen kunnen bouwen aan betekenisvolle connecties en duurzaam succes.

Ga voor meer informatie naar www.pegamento.nl of bel ons via 088-0067180.