JULI 2026

Barometer Digital Decade 2026

Digitale volwassenheid, wetgevingsgereedheid en de soevereiniteitsvraag

ICTRECHT

ICTRecht bv
020 663 1941
contact@ictrecht.nl

Jollemanhof 12
1019 GW Amsterdam
www.ictrecht.nl

KVK
72602651

BTW
NL859169820.B01

IBAN
NL64 RABO 0334 0962 94

Arnoud Engelfriet	Chief Knowledge Officer
Guido Grevink	Business Development Manager, Senior Legal Counsel
Saskia Brouwer	Legal Counsel (Tech)

Fotografie

Joep Hijwegen

ICTRecht bv

Inhoud

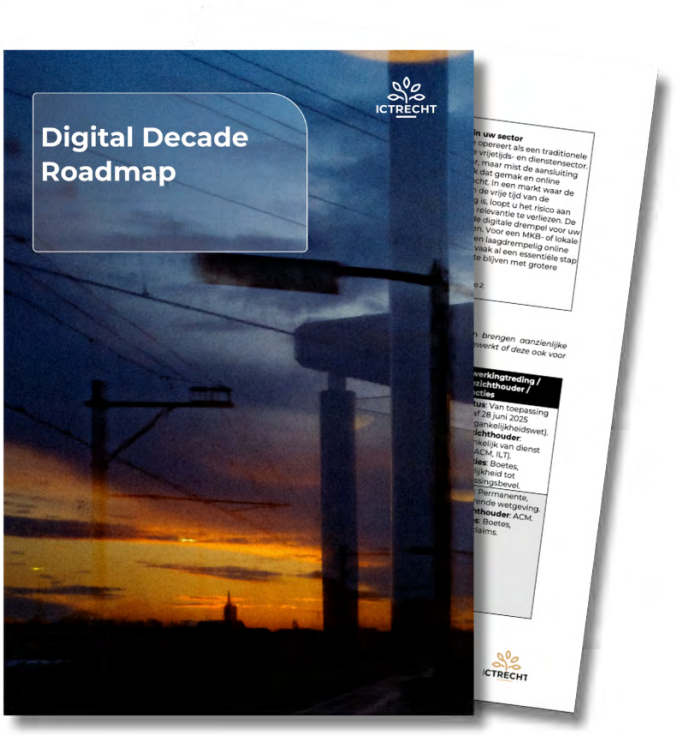
1. Inleiding

De Europese Unie heeft zichzelf een deadline gegeven. In 2030 moet Europa een digitaal volwassen continent zijn: 80% van de bevolking met digitale basisvaardigheden, 75% van de bedrijven op cloud of AI, alle overheidsdiensten online, elke burger met een digitale identiteit. Het programma heet de Digital Decade en het klinkt ambitieus. Dat is het ook. Maar tegelijkertijd is het een wetgevingsmachine.

Om die digitale transformatie in goede banen te leiden, heeft de EU in de afgelopen vijf jaar een ongekend pakket aan wet- en regelgeving uitgerold. De AI Act reguleert kunstmatige intelligentie. De Cyber Resilience Act stelt beveiligingseisen aan elk product met een digitaal element. DORA dwingt de financiële sector tot digitale weerbaarheid. NIS2 doet hetzelfde voor kritieke infrastructuur. De Data Act regelt wie toegang heeft tot productdata. De EHDS opent gezondheidsdata voor hergebruik. En de lijst gaat door. Wij monitoren meer dan honderd verordeningen en richtlijnen die samen het speelveld herdefiniëren.

Dit pakket aan wetten verwijst naar elkaar, bouwt op elkaar en werkt via de keten door. Een modern connected product kan aan vijf of zes wetten tegelijk moeten voldoen. Een clouddienstverlener in de financiële sector valt onder DORA, CSDDD, de Data Act én de aankomende Cloud and AI Development Act tegelijkertijd. Medische startups krijgen te maken met de MDR, de AI Act, de AVG en het medisch tuchtrecht van hun klanten. Het overzien van dit landschap is geen eenvoudige taak.

In juni 2025 publiceerden we de Monitor Digital Decade 2030: een eerste verkenning van hoe organisaties zich op dit alles voorbereiden. Het beeld was ontnuchterend. Slechts 22% had een concrete implementatiestrategie.



Cybersecurity was overal de hoogste prioriteit. En het grootste knelpunt was universeel: gebrek aan mensen, tijd en expertise. Dat rapport stelde de vraag: weet je wat er op je afkomt? De Barometer die je nu leest, gaat een stap verder. Wij ontwikkelden een interactieve tool, de Digital Decade Roadmap. Deze leidt organisaties langs een uitgebreide thematische vragenlijst om hun positie en readiness in de Digital Decade in kaart te brengen. Hiermee hebben we bij 516 organisaties in kaart gebracht hoe digitaal volwassen ze zijn en welke concrete wetgeving op basis van hun profiel op hen van toepassing is. De resultaten zijn duidelijk, en soms verrassend. In de productiesector bevat 85% van de producten software of IoT(Internet of Things)-connectiviteit, terwijl 42% van diezelfde sector digitaal nog op basisniveau opereert. In de zorg gebruikt 52% AI voor triage of diagnose. Dit zijn toepassingen die onder de AI Act als high-risk kwalificeren, maar de readiness is zeer wisselend. In de financiële sector is 84% DORA-plichtig, maar 29% van de ICT-bedrijven die aan hen leveren, wordt via de keten meegezogen in datzelfde regime. En de publieke sector wordt geraakt door meer wetgeving tegelijk dan welke andere sector ook.

Achter deze cijfers schuilt een patroon. De traditionele aanpak van “per wet een actielijst” is ontoereikend geworden. Wat nodig is, is een geïntegreerd beeld: waar sta ik, wat komt er op me af, en wat moet ik als eerste doen? Wij noemen dit holistische compliance en beschreven de methodiek in ons boek Wetwijs in de digital decade. En in dit rapport laten we zien wat voor inzichten en actiepunten je daarmee kunt verkrijgen.

We sluiten af met een essay over digitale soevereiniteit. Dit is het thema dat het debat domineert, maar in de dagelijkse praktijk van organisaties nog nauwelijks in concrete stappen is vertaald. Ons argument: soevereiniteit is een collectief probleem dat een collectief antwoord vereist.

Hoe lees je dit rapport?

De Barometer Digital Decade 2026 is opgebouwd in lagen, zodat je hem op meerdere manieren kunt gebruiken.

Wil je alleen de hoofdpunten?
Lees hoofdstuk 3, de samenvatting van de belangrijkste resultaten.

Wil je weten wat jouw sector raakt?
Spring naar hoofdstuk 4 voor de digitale volwassenheid per sector, of naar hoofdstuk 6 voor de concrete aanbevelingen per sector.

Wil je het wetgevingsperspectief?
Hoofdstuk 5 zet de belangrijkste Europese wetten op een rij en laat zien welke sectoren zij hoe hard raken.

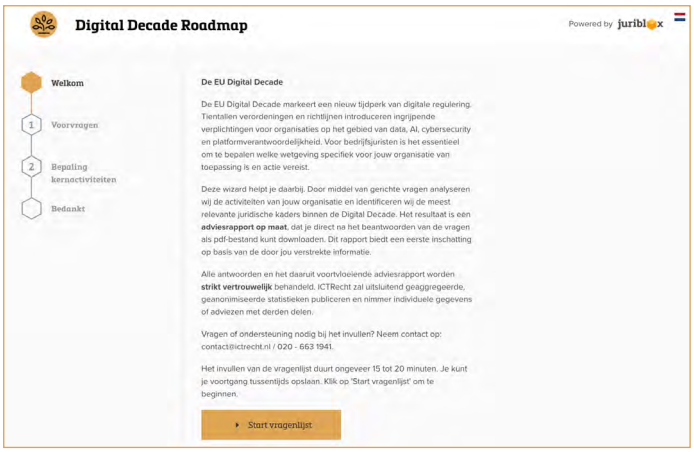
Wil je het grotere verhaal?
Lees het essay in hoofdstuk 7, waarin Arnoud Engelfriet de spanning tussen wetgevingsdruk en digitale soevereiniteit ontleedt.

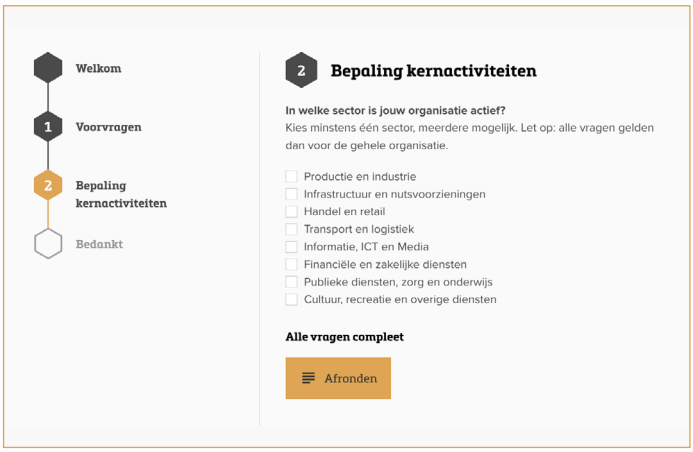
Wil je de balans opmaken?
Hoofdstuk 8 vat de belangrijkste conclusies samen en wijst de weg naar de vervolgstappen.

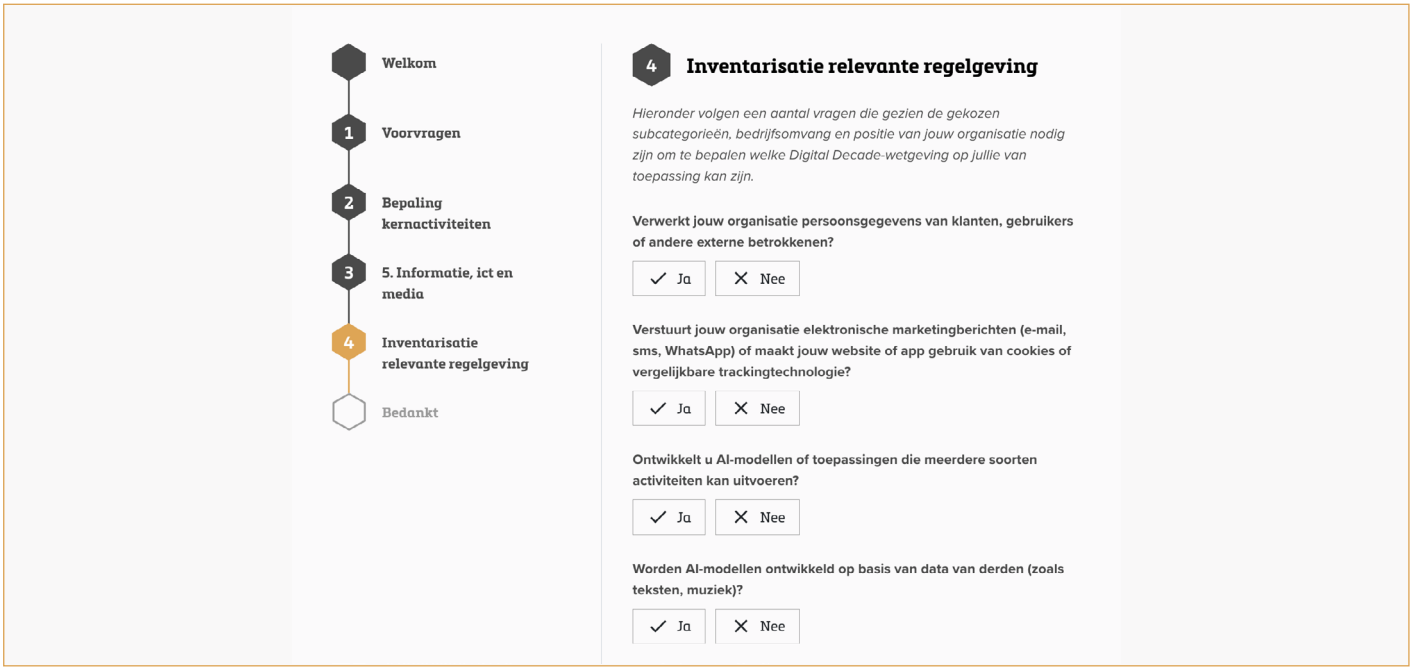
2. Onderzoeksopzet

De Roadmap stelt vragen over je sector, omvang, specifieke activiteiten en digitale volwassenheid. Op basis van de antwoorden wordt een profiel opgesteld dat bepaalt welke Europese wetgeving waarschijnlijk op je organisatie van toepassing is. De Roadmap is verspreid onder onze klanten en het netwerk van juridische en compliance professionals in brede zin. Deze organisaties zijn waarschijnlijk digitaal bewuster dan het gemiddelde bedrijf. Dat betekent dat de werkelijke stand van zaken eerder slechter is dan wat dit rapport laat zien.

In totaal hebben 516 organisaties de Roadmap volledig ingevuld. De grootste groep komt uit de publieke sector, zorg en het onderwijs (146 respondenten), gevolgd door ICT en media (127), de financiële en zakelijke dienstverlening (77), handel en retail (45), de productie-industrie (45), cultuur en recreatie (28), infrastructuur en nutsvoorzieningen (27) en transport en logistiek (21).

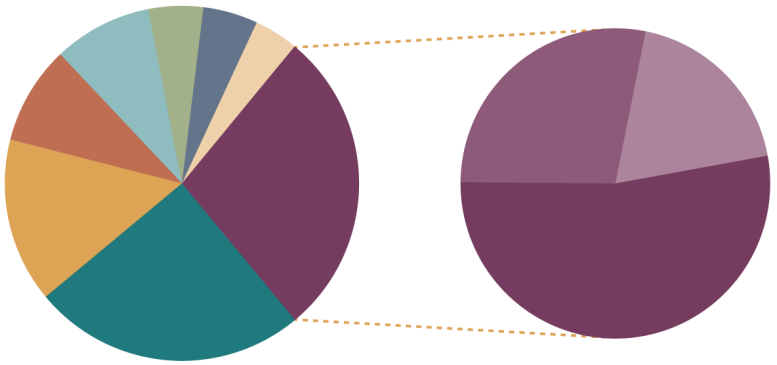






Respondentenverdeling per sector

Organisaties konden maximaal 3 antwoorden selecteren



Subsectoren op basis van de 28% (n=146) aandeel in het hoofdonderzoek.

Publiek, zorg & onderwijs	(n=146)	28%
Publiek		53%
Zorg		28%
Onderwijs		19%
ICT & Media	(n=127)	25%
Financieel & zakelijk	(n=77)	15%
Productie & industrie	(n=45)	9%
Handel & retail	(n=45)	9%
Cultuur & recreatie	(n=28)	5%
Infrastructuur & nuts	(n=27)	5%
Transport & logistiek	(n=21)	4%

De respondenten zijn overwegend middelgroot tot groot. Iets meer dan de helft (55%) heeft meer dan 250 medewerkers. De andere categorieën zijn gelijkelijk verdeeld – 15% valt in de categorie middelgroot (50 tot 249 medewerkers), 16% is klein (10-49) en 14% telt als micro-organisatie (0-9 medewerkers). Dat weerspiegelt waarschijnlijk dat grotere organisaties eerder aanleiding zien om hun wetgevingsexposure in kaart te brengen, en dat kleinere organisaties minder snel een uitgebreide scan invullen. Ook bereikt ons netwerk overwegend juridische professionals, die bij micro- en kleine organisaties minder vaak aanwezig zijn.

De Roadmap levert twee soorten data op. De eerste is een digitale volwassenheidsscore: per sector beantwoordt de respondent een volwassenheidsvraag op een schaal van 1 (traditioneel, handmatig) tot 5 (transformerend, platformmodel). De tweede zijn antwoorden op gerichte ja/nee-vragen die bepalen welke wetgeving van toepassing is: gebruik je AI in je product? Bevatten je producten IoT? Lever je diensten aan de financiële sector? Die combinatie maakt het mogelijk om niet alleen te meten waar organisaties staan, maar ook hoe groot de kloof is tussen die positie en wat er wettelijk op hen afkomt.

Een kanttekening bij de vergelijking met ons eerdere onderzoek. De Monitor Digital Decade 2030,

Micro (0-9)	14%
Klein (10-49)	16%
Middelgroot (50-249)	15%
Groot (250+)	55%

gepubliceerd in juni 2025, bevroeg 141 organisaties over hun prioriteiten, knelpunten en adviesbehoefte. De Barometer 2026 meet iets anders: feitelijke volwassenheid en feitelijke wetgevingsrelevantie op basis van activiteiten. De twee onderzoeken vullen elkaar aan maar zijn niet direct vergelijkbaar. Waar het kan, leggen we de verbinding.

Verantwoording

De Digital Decade Roadmap is in de periode maart tot juni 2026 opengesteld als online scan, toegankelijk via het netwerk van ICTRecht en via gerichte LinkedIn-campagnes. Medio juni leidde een extra oproep via de ICTRecht-nieuwsbrief tot een aanzienlijke tweede instroom. In totaal zijn 588 inzendingen ontvangen, verdeeld over twee instroomperiodes.

Deze zijn in drie stappen opgeschoond voordat ze in de analyse zijn betrokken. Eerst zijn 27 inzendingen als ongeldig uitgefilterd op basis van duidelijke fantasienamen of inhoudelijke inconsistenties die duiden op niet-serieuze invulling. Daarnaast zijn ook testinzendingen van medewerkers van ons kantoor verwijderd. Vervolgens zijn 43 inzendingen verwijderd als duplicaten: respondenten die de Roadmap meerdere malen hebben ingevuld, vaak met kleine variaties, om verschillende rapportversies op te vragen. In die gevallen is de meest recente volledige inzending behouden. Tot slot zijn 2 inzendingen uitgesloten wegens een technische storing in het formulier waardoor antwoorden op de wetgevingsvragen niet correct zijn opgeslagen.

De resterende 516 inzendingen zijn steekproefsgewijs gecontroleerd op interne consistentie en vormen de basis van de analyse in dit rapport. De verdeling over de twee instroomperiodes is gecontroleerd op systematische verschillen in antwoordpatronen; die zijn niet gevonden, wat het samenvoegen van beide cohorten rechtvaardigt.

De steekproef is zelfselecterend: deelnemers hebben zich vrijwillig aangemeld, wat betekent dat organisaties die bewust met digitale transformatie bezig zijn waarschijnlijk oververtegenwoordigd zijn. De bevindingen zijn daarmee indicatief voor het digitale speelveld maar niet statistisch representatief voor de Nederlandse economie als geheel.

3. Samenvatting van de belangrijkste resultaten

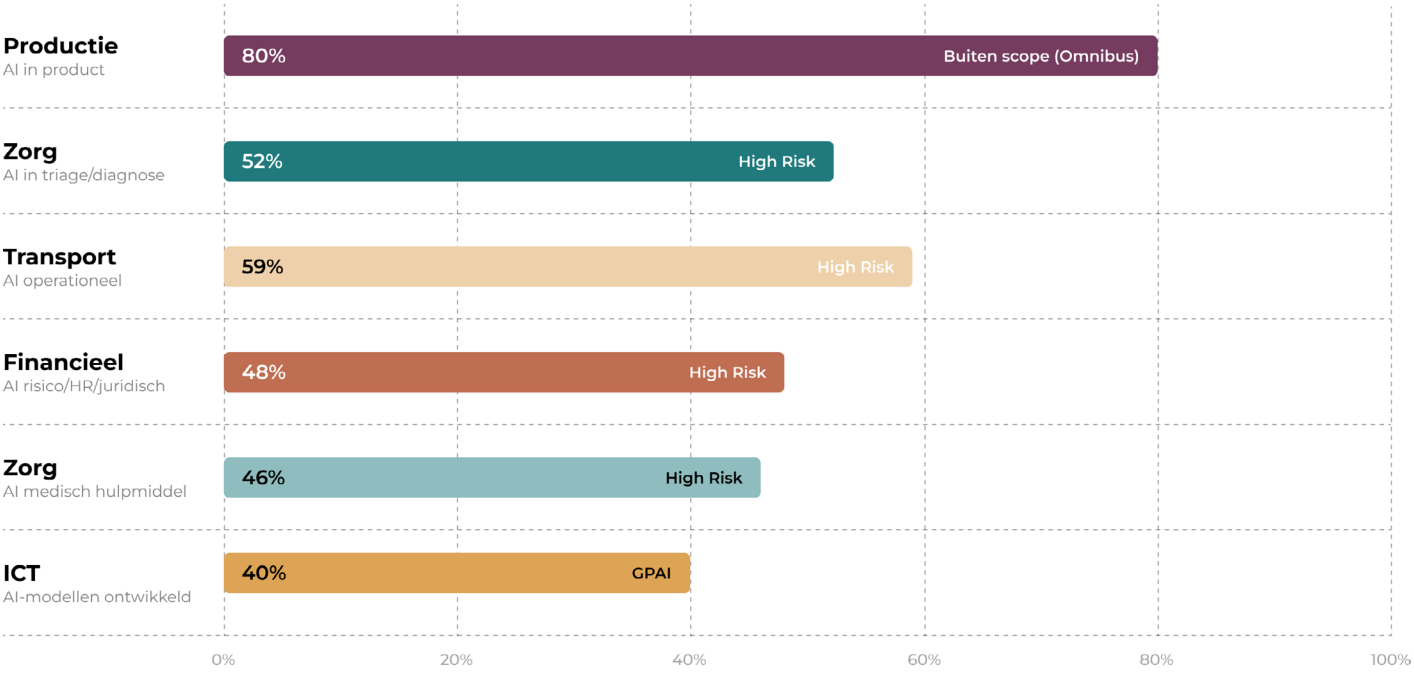
Wie de Digital Decade op afstand bekijkt, ziet een abstract beleidsprogramma met verre deadlines. Wie inzoomt op de data van 516 organisaties, ziet iets anders: een wetgevingsgolf die al is begonnen en die vrijwel elke sector raakt, vaak op plekken die je niet verwacht. Vier bevindingen springen eruit.

1. AI is overal, niet alleen in de techsector
2. Connected products en de beveiligingsplicht
3. De keten trekt de wet door
4. De publieke sector: geraakt op elke as

3.1 AI is overal, niet alleen in de techsector

Het debat over de AI Act wordt gedomineerd door de techsector: wie bouwt de grote taalmodellen, wie moet transparant zijn over trainingsdata, wie valt onder de GPAI-verplichtingen. Maar de data laten een breder beeld zien.

In de productiesector geeft 80% aan AI op te nemen in het product en gebruikt 75% AI in interne processen als kwaliteitscontrole en HR. In de zorgsector zet 52% AI in voor triage of diagnose en gebruikt 46% AI als medisch hulpmiddel. In de financiële sector past 48% AI toe voor kredietbeoordeling, risicomodellering, werving of juridische besluitvorming. In de transportsector gebruikt 59% AI voor operationele doelen als routeoptimalisatie en dynamische prijsstelling, en stuurt 47% personeel of zzp'ers aan met behulp van AI. Zelfs in de culturele sector gebruikt ruim een derde AI voor surveillance op evenementen of het aansturen van personeel.

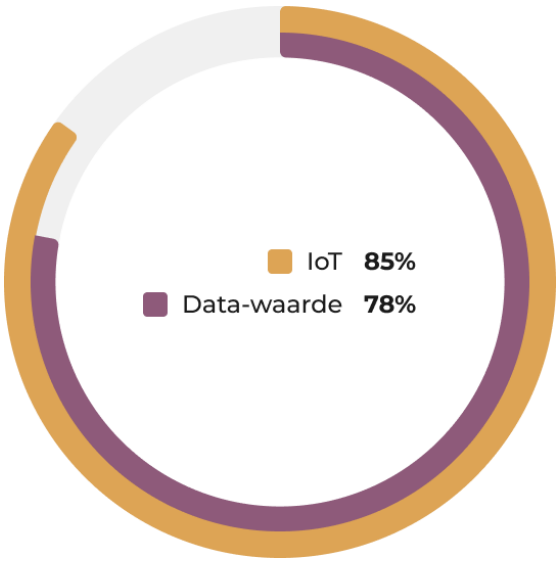


"De opmars van AI sectoraal bekeken (en haar AI Act impact)"

Veel van deze toepassingen vallen onder de AI Act als high-risk: AI in medische diagnostiek, in kredietbeoordeling, in toegang tot publieke diensten, in leerlingevaluatie. De Omnibus Act verschuift de deadline voor high-risk-toepassingen naar december 2027 en haalt industriële productietoepassingen grotendeels uit de directe verplichtingen. Maar de breedte van het AI-gebruik in de zorg, de financiële sector, het onderwijs en de publieke dienstverlening maakt dat de AI Act voor meer organisaties relevant is dan de meeste denken. De implementatie kost maanden. Wie nu nog niet begonnen is met ten minste de inventarisatie, heeft een probleem.

3.2 Connected products en de beveiligingsplicht

De Cyber Resilience Act stelt beveiligingseisen aan elk product met een digitaal element: van industriële machines tot consumentenelektronica, van IoT-sensoren tot embedded software. In de productiesector beantwoordde 85% van de respondenten bevestigend op de vraag of hun producten software of



internetconnectiviteit bevatten. Bij 78% genereert het product data die waarde heeft voor de eindgebruiker, wat ook de Data Act activeert.

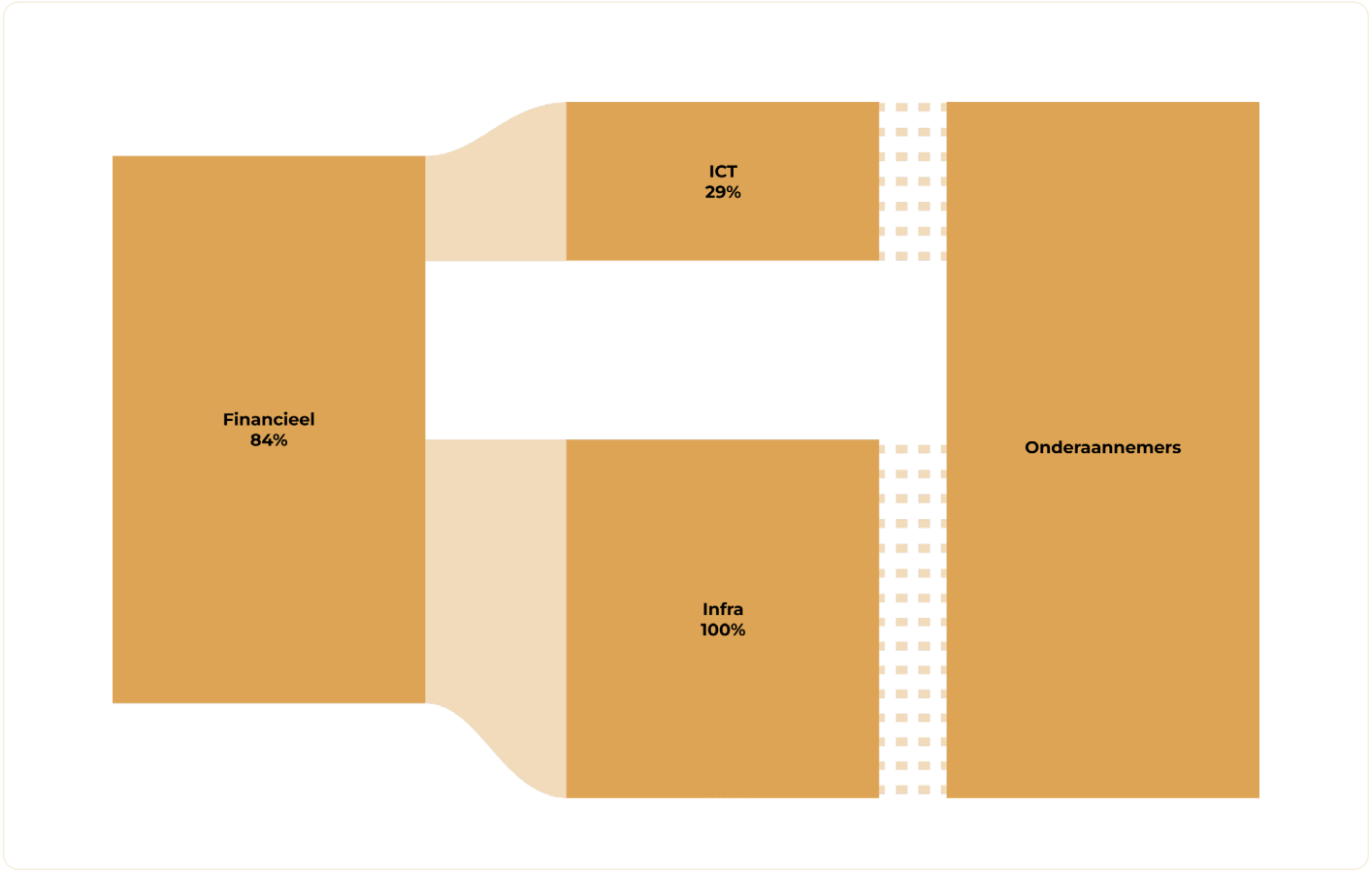
De CRA kent twee deadlines. Vanaf september 2026 geldt een meldplicht bij actief misbruikte kwetsbaarheden. Vanaf december 2027 gelden de volledige beveiligingseisen: secure-by-design, software-updatebeleid, een software bill of materials en een gecoördineerd vulnerability disclosure-proces.

Dat 85% van de productiebedrijven connected products maakt, is op zichzelf niet verrassend, de digitalisering van producten is al jaren gaande. Wat wél opvalt, is de combinatie met de volwassenheidsdata: 42% van diezelfde sector zit digitaal op niveau 1 of 2. Dat zijn bedrijven die kantoorautomatisering als het hoogste digitale ambitieniveau hebben of nog experimenteren met pilots, maar die wel producten op de markt brengen die straks aan CRA-beveiligingseisen moeten voldoen. De kloof tussen productcomplexiteit en organisatorische gereedheid is in deze sector het grootst.

3.3 De keten trekt de wet door

DORA, de Digital Operational Resilience Act, is in januari 2025 van kracht geworden en reguleert de digitale weerbaarheid van de financiële sector. Banken, verzekeraars en pensioenfondsen moeten hun ICT-risicobeheer op orde hebben, incidenten melden, en hun afhankelijkheid van externe ICT-dienstverleners beheersen. In onze steekproef geeft 84% van de financiële respondenten aan bank, verzekeraar of pensioenfonds te zijn, zij vallen direct onder DORA.

Maar de impact reikt veel verder dan de financiële sector zelf.



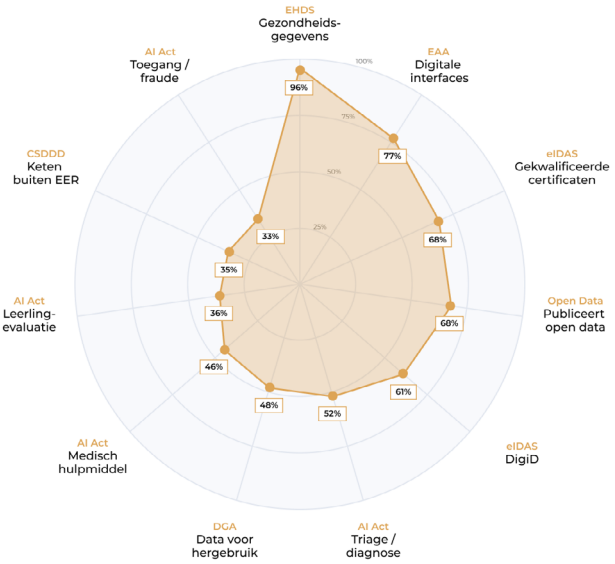
Van de ICT-respondenten levert 29% diensten aan financiële instellingen. Van de infrastructuur- en datacenter-respondenten die deze vraag beantwoordden, doet 100% dat. Die organisaties vallen daarmee als "kritieke derde ICT-dienstverlener" potentieel onder DORA's outsourcing-regime: contractuele eisen rond incidentrapportage, auditrechten, exit-strategieën en continuïteit. DORA stopt niet bij de sectorgrens. Het trekt door de hele keten.

Datzelfde mechanisme zien we bij NIS2, dat via supply chain security-eisen doorwerkt naar leveranciers van essentiële entiteiten. En we verwachten het bij de aankomende Cloud and AI Development Act (CADA), die soevereiniteitseisen gaat stellen aan clouddiensten voor de publieke sector, eisen die onvermijdelijk doorwerken naar de leveranciers van die diensten.

De implicatie voor organisaties is concreet: ken je keten. Niet alleen wie je leveranciers zijn, maar ook wie je klanten zijn en onder welk regime zij vallen. Als je levert aan een bank, een ziekenhuis of een overheidsinstantie, gelden er indirect eisen aan jou, ook als je zelf niet in een gereguleerde sector opereert.

3.4 De publieke sector: geraakt op elke as

De publieke sector, inclusief zorg en onderwijs, is de sector met de breedste wetgevingsexposure in ons onderzoek. Geen andere sector scoort op zoveel indicatoren tegelijk hoog.



Van de zorginstellingen verwerkt 96% elektronische gezondheidsgegevens, de European Health Data Space raakt vrijwel iedereen. Van alle publieke organisaties biedt 77% digitale interfaces aan burgers of patiënten, waarmee de European Accessibility Act van toepassing is. Bij 68% zijn gekwalificeerde digitale certificaten in gebruik en 61% verleent diensten via DigiD. eIDAS 2.0 en de Europese digitale identiteitsportemonnee worden voor hen operationele realiteit. In de zorg gebruikt 52% AI voor triage of diagnose en 46% als medisch hulpmiddel. Bij overheden en semi-publieke organisaties gebruikt 33% AI voor het beoordelen van toegang tot diensten en 33% voor fraudedetectie. In het onderwijs zet 36% AI in voor leerlingevaluatie. En 48% van de publieke sector stelt data beschikbaar voor hergebruik door derden.

Elke individuele wet is beheersbaar. De uitdaging zit in de stapeling. Een middelgroot ziekenhuis kan tegelijkertijd te maken krijgen met de EHDS, de AI Act (diagnostiek), de EAA (patiëntportaal), NIS2 (als essentiële entiteit), de AVG (persoonsgegevens) en eIDAS (digitale identiteit). Dat vereist geen zes afzonderlijke compliancetrajecten maar een geïntegreerde aanpak. En die is er bij de meeste organisaties nog niet.

Dat wordt versterkt door het volwassenheidsprobleem. In de publieke dienstverlening zit 41% op niveau 1 of 2: alleen een informatiewebsite of losstaande formulieren zonder systeemkoppeling. In het sociaal domein is dat zelfs 65%. De wetgeving veronderstelt een digitale basis, zoals verwerkingsregisters, gestructureerde data-uitwisseling, toegangsbeheersing, die bij een aanzienlijk deel van de sector simpelweg niet aanwezig is. De eerste stap is dan niet "compliance met wet X" maar "de digitale huishouding op orde brengen."

4. Digitale volwassenheid per sector

Elke sector in dit onderzoek beantwoordde een eigen volwassenheidsvraag, toegesneden op wat digitalisering in die sector concreet betekent. Voor de productiesector gaat het over smart factory en verbonden producten. Voor de zorg over het EPD en eHealth. Voor de overheid over digitale dienstverlening aan burgers. De schaal loopt steeds van 1 (traditioneel, handmatig) tot 5 (transformerend, platformmodel).

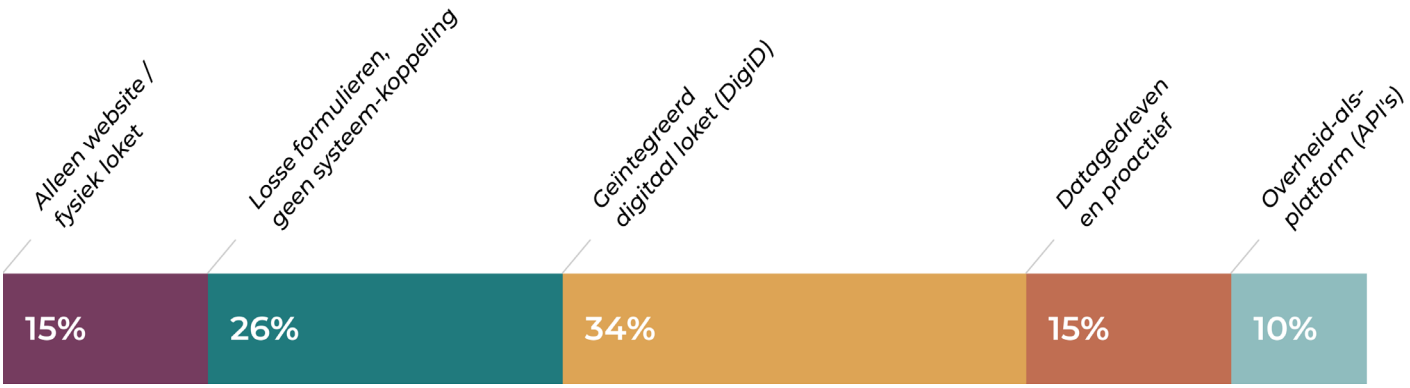
Dat maakt de scores binnen een sector goed vergelijkbaar, maar vergelijkingen tússen sectoren zijn indicatief. Een "3" bij de overheid (geïntegreerd digitaal loket) is iets wezenlijk anders dan een "3" bij een softwarebedrijf (telemetrie en roadmap-sturing). Wat wél vergelijkbaar is, is het patroon: hoeveel organisaties zitten nog op basisniveau, hoeveel lopen voorop, en hoe groot is de kloof binnen de sector?

4.1 Publiek, zorg & onderwijs

De publieke sector is met 146 respondenten de grootste groep in ons onderzoek, en de meest diverse. Overheid, zorg en onderwijs beantwoorden elk een eigen volwassenheidsvraag, waarbij de resultaten sterk uiteen lopen.

Digitale dienstverlening aan burgers

Voor overheden, het sociaal domein en semi-publieke organisaties gaat de volwassenheidsvraag over hoe je je diensten digitaal aanbiedt aan burgers of cliënten. Van "alleen een informatiewebsite" tot "overheid-als-platform met open API's."



Van de respondenten die deze vraag beantwoordden, biedt 15% online alleen informatie aan. Burgers moeten voor het echte werk nog naar het loket of per post. Ruim een kwart (26%) biedt wel digitale formulieren aan, maar die werken als losstaande processen: geen systeemkoppeling, geen dossieroverdracht tussen afdelingen. Samen is dat 41% op het laagste niveau.

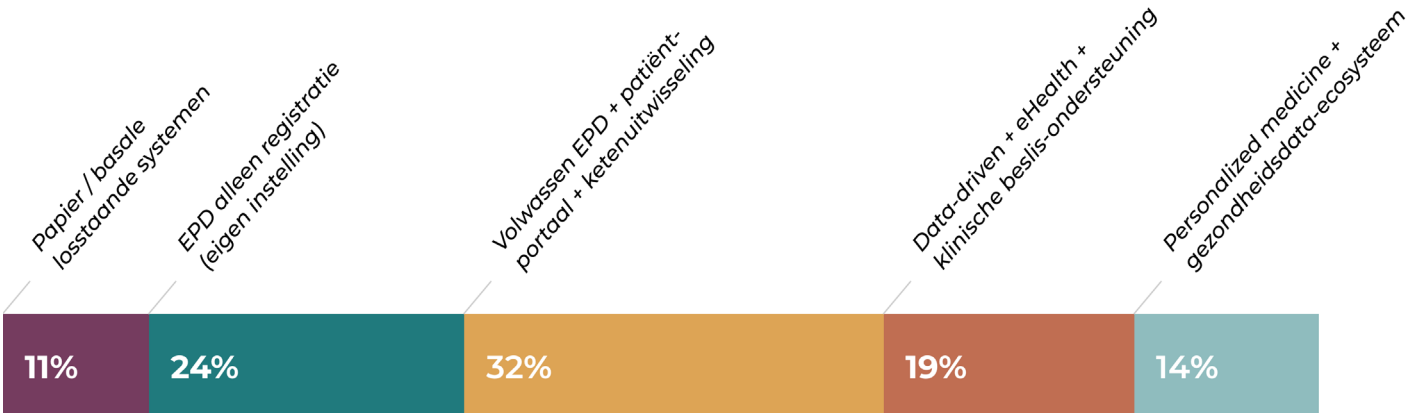
De grootste groep (34%) zit op niveau 3: een geïntegreerd digitaal loket waar burgers met één login (veelal DigiD) hun zaken kunnen regelen. Dat is functioneel en bruikbaar, maar nog geen proactieve dienstverlening. Slechts 15% werkt datagedreven en proactief, en 10% opereert als overheid-als-platform met open API's waarop externe partijen toepassingen kunnen bouwen.

Achter het gemiddelde zitten scherpe verschillen. In het sociaal domein (jeugdzorg, welzijnsorganisaties, sociale dienstverlening) zit naar schatting twee op de drie organisaties op niveau 1 of 2. Bij gemeenten en rijksoverheid is dat een kwart. De verklaring is structureel: het sociaal domein werkt met kwetsbare doelgroepen, complexe casuïstiek en gefragmenteerde IT-systemen die historisch niet op integratie zijn gebouwd. De digitale achterstand is niet het gevolg van onwil maar van systeemcomplexiteit.

Voor beleidsmakers is dit een relevant gegeven. De Digital Decade-doelstelling van 100% online overheidsdiensten in 2030 veronderstelt dat het fundament er ligt. Bij vier op de tien organisaties in ons onderzoek is dat niet het geval.

Digitalisering van het zorgproces

De volwassenheidsvraag voor zorginstellingen gaat over de rol van digitalisering in het zorgproces: van papieren dossiers tot personalized medicine.



De zorg laat een ander patroon zien dan de publieke dienstverlening. De basis is iets steviger: de grootste groep (32%) heeft een volwassen EPD-implementatie met patiëntportaal en gestructureerde gegevensuitwisseling met andere zorgverleners.

Daarnaast gebruikt 19% het EPD actief voor klinische beslisondersteuning en eHealth, en 14% opereert op het niveau van personalized medicine en bijdrage aan gezondheidsdata-ecosystemen.

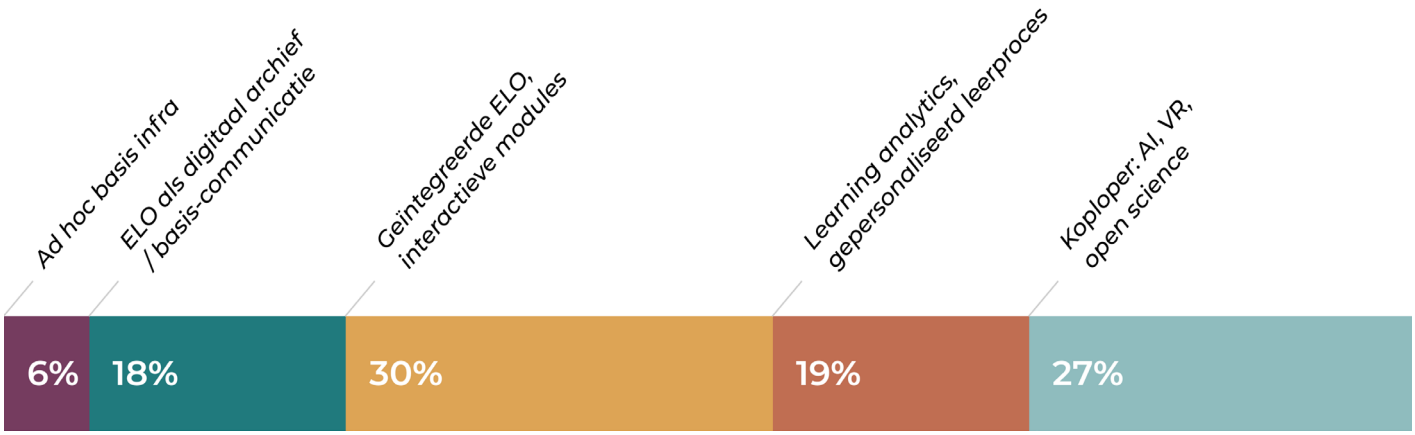
Maar er is een staart. 11% werkt nog grotendeels op papier of met basale losstaande systemen, en 24% gebruikt het EPD alleen voor registratie binnen de eigen instelling, zonder portal, zonder ketenuitwisseling. Samen is dat 35% met de digitale basis niet op orde.

Die 35% is relevant in het licht van de European Health Data Space, die interoperabiliteit en datatoegang als uitgangspunt neemt. Als een derde van de zorginstellingen het EPD nog primair als registratiesysteem gebruikt, is EHDS-compliance niet een kwestie van een technische koppeling maar van een fundamentele procesverandering.

Middelgrote zorginstellingen (50-249 medewerkers) zijn het kwetsbaarst. Ze zijn groot genoeg om complexe patiëntenpopulaties te bedienen maar te klein voor de transformatieprogramma's die grote ziekenhuizen kunnen opzetten.

Digitalisering van het onderwijs

Het onderwijs toont een opvallend ander patroon dan de overige publieke sectoren.



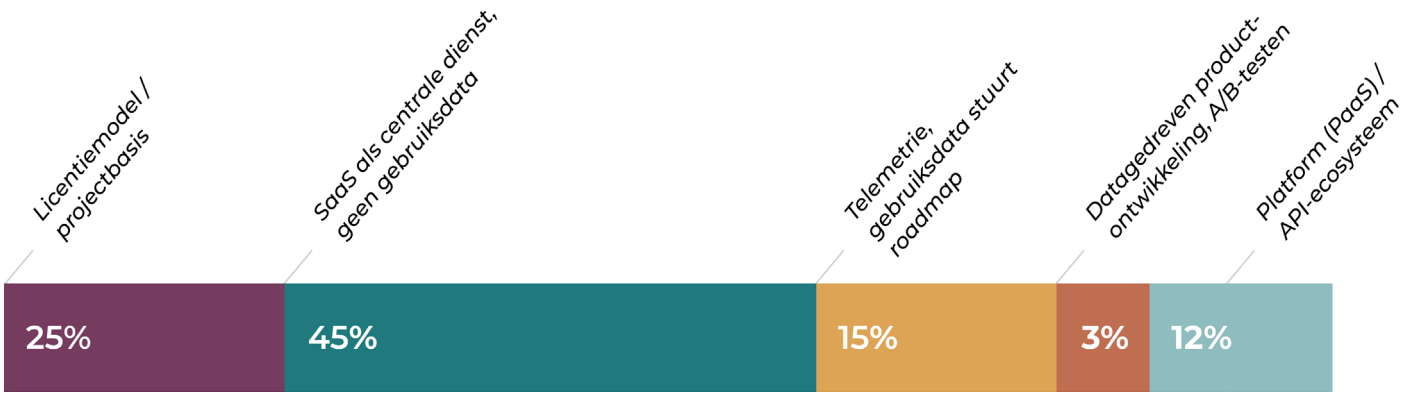
Slechts 6% zit op het allerlaagste niveau (alleen basisinfrastructuur, ad hoc-inzet van digitale tools). Maar 18% gebruikt de digitale leeromgeving voornamelijk als archief: een plek om documenten te delen, niet om het leerproces te ondersteunen. De grootste groep (30%) heeft een geïntegreerde digitale leer- of onderzoeksomgeving, en 19% zet learning analytics actief in om het leerproces te personaliseren.

Het opvallendste: 27% positioneert zich als koploper, met inzet van AI, VR en open science. Het onderwijs is gepolariseerd: een relatief dunne middenmoot, een substantiële staart die de ELO als digitaal archief gebruikt, en een voorhoede die volop experimenteert. De uitdaging zit niet in bewustzijn maar in het meenemen van de brede middenmoot.

4.2 ICT & Media

De ICT-sector is met 127 respondenten de op een na grootste groep, en intern de meest diverse. Softwareontwikkelaars, hosters, dataplatformen, contentproducenten, platformbeheerders en consultants beantwoorden elk een eigen volwassenheidsvraag. Dat levert een gelaagd beeld op.

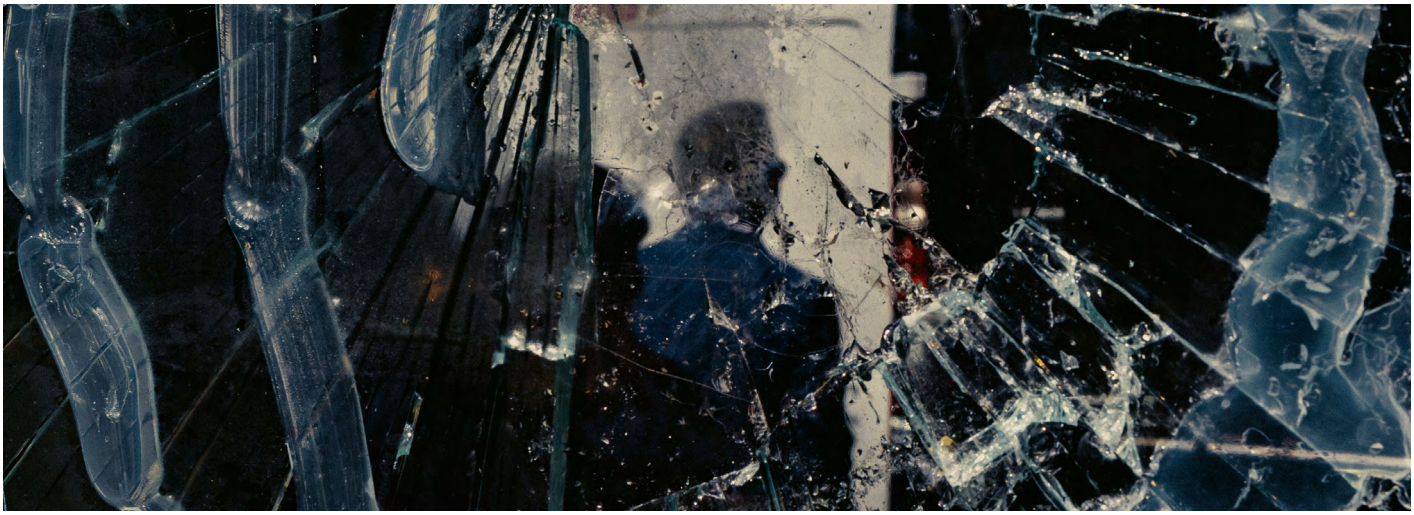
Software en Saas



Van de softwarebedrijven werkt 25% nog op een licentiemodel of op projectbasis. Dat impliceert geen continue dienstverlening, periodieke updates, geen structurele relatie met de gebruiker na oplevering. Bijna de helft (45%) biedt software primair aan als SaaS, maar verzamelt geen of nauwelijks data over het feitelijke gebruik. Samen is dat 70% dat blind vliegt: ze weten niet hoe hun product in de praktijk wordt gebruikt.

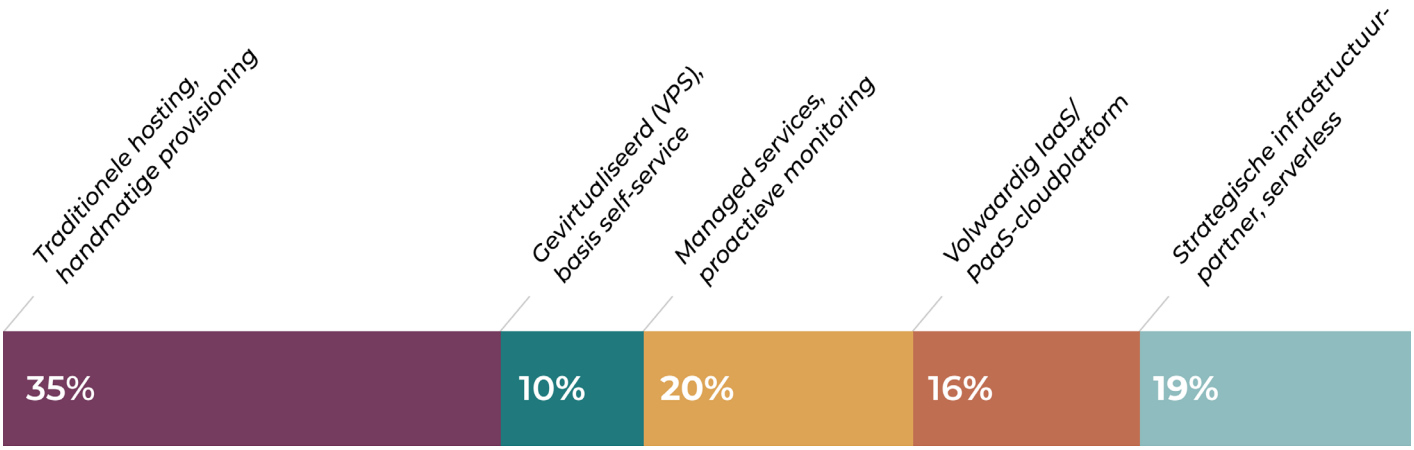
Slechts 15% verzamelt systematisch gebruiksdata (telemetrie) om de productontwikkeling te sturen. Een enkeling (3%) doet aan datagedreven productontwikkeling met A/B-testen, en 12% opereert als platform met een API-ecosysteem.

Dit is de sector die andere organisaties adviseert over datagedreven werken en die zelf de producten bouwt waarmee de rest digitaliseert. Dat 70% geen structureel inzicht heeft in het gebruik van het eigen product, is een opvallende blinde vlek. De Cyber Resilience Act verplicht softwareleveranciers om kwetsbaarheden actief te monitoren en te verhelpen. Dat veronderstelt dat je weet wat er met je product gebeurt na oplevering.



Hosting en cloud

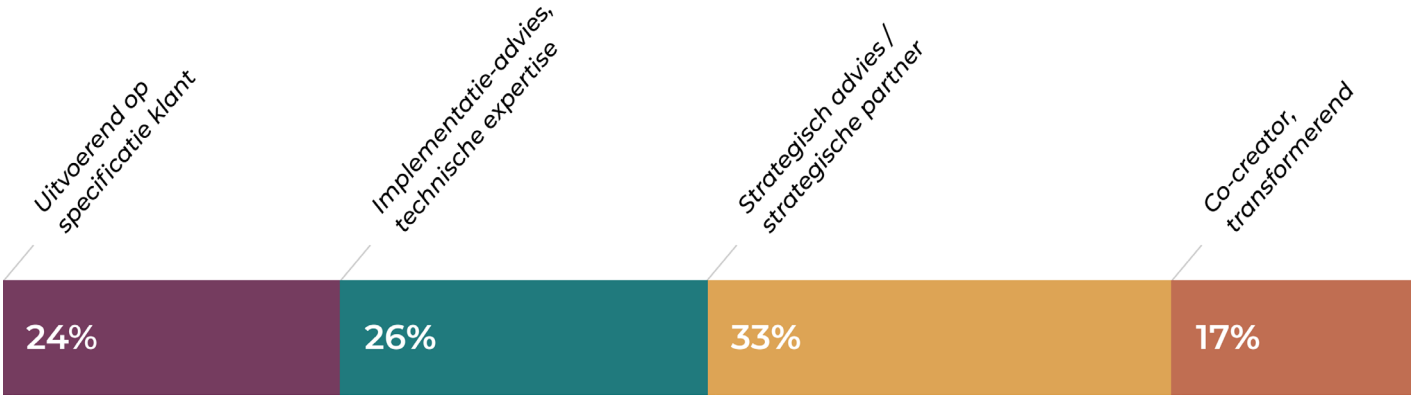
De hosting- en cloudproviders laten een vergelijkbare polarisatie zien. Ruim een derde (35%) biedt traditionele hostingdiensten aan met grotendeels handmatige provisioning. Aan de andere kant opereert 19% als strategische infrastructuurpartner met serverless computing en AI-tooling. De middengroep (managed services, geautomatiseerde platforms) is gevuld maar niet dominant.



ICT-consultancy

De ICT-consultants en maatwerkontwikkelaars laten een ander beeld zien. Hier gaat de volwassenheidsvraag niet over technologie maar over positionering: voer je uit wat de klant vraagt, of vorm je mee wat de klant nodig heeft?

Bijna een kwart (24%) is primair uitvoerend; ze werken op specificatie van de klant. Ruim een kwart (26%) adviseert over implementatie van specifieke oplossingen. Een derde (33%) opereert op strategisch niveau, en 17% treedt op als co-creator die samen met de klant nieuwe businessmodellen ontwikkelt.



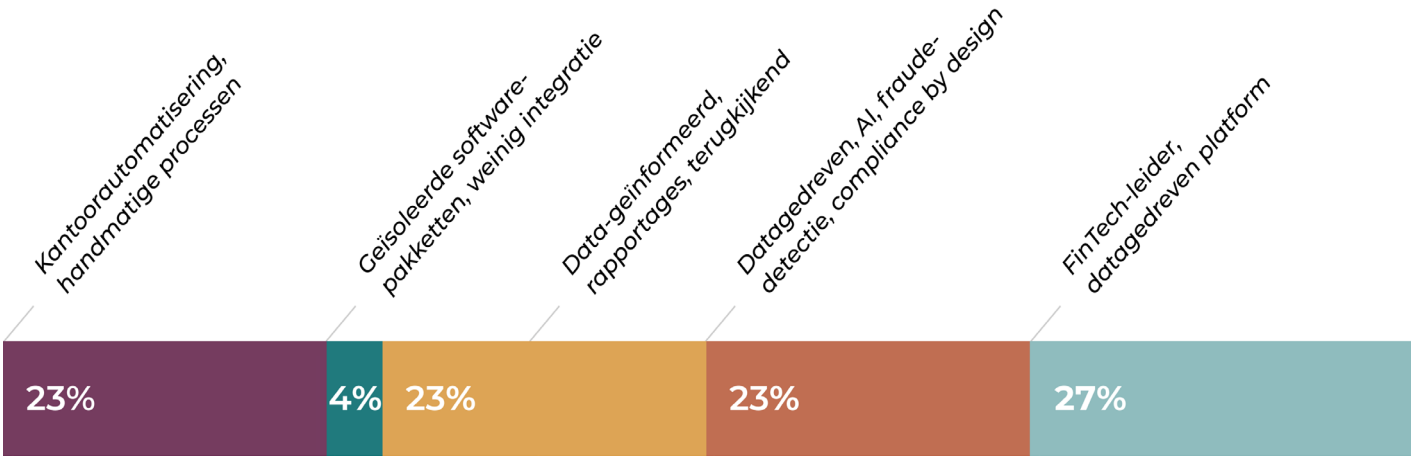
NB: de oorspronkelijke niveaus 3 en 4 (domeinspecifiek en holistisch strategisch advies) zijn samengevoegd tot "Strategisch advies / strategische partner", omdat het onderscheid voor respondenten onduidelijk bleek.

Het beeld is beter dan bij software: de helft (50%) positioneert zich als strategisch partner of co-creator. Maar het contrast met de softwarekant is schril: de adviseurs positioneren zich als strategisch, terwijl de producten die ze aanbevelen voor het merendeel zonder gebruiksdata worden doorontwikkeld.

4.3 Financieel & zakelijk

De financiële en zakelijke dienstverlening telt 77 respondenten, maar het is essentieel om deze sector niet als één geheel te behandelen. Banken en verzekeraars opereren in een fundamenteel ander landschap dan advocatenkantoren en accountants. De wetgevingsdruk verschilt, de digitale cultuur verschilt, en de volwassenheid verschilt.

Banken en verzekeraars

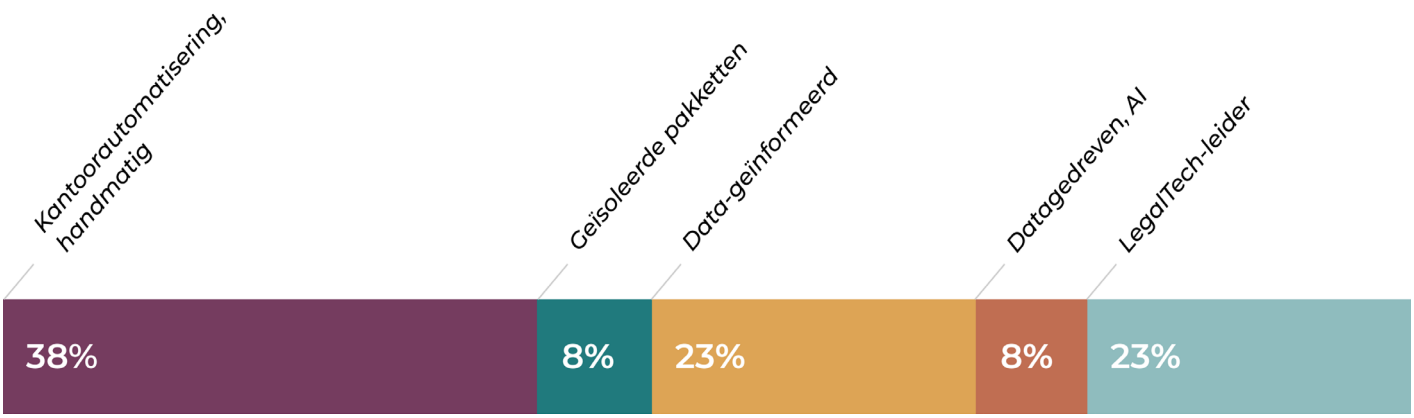


De financiële kernactiviteiten (banken, verzekeraars, pensioenfondsen) zijn sterk gepolariseerd. Aan de bovenkant opereert 27% als FinTech-leider: volledig datagedreven, geautomatiseerd platform, fundamenteel vernieuwde dienstverlening. Nog eens 23% zet AI actief in voor risicomodellering, fraudedetectie en geautomatiseerde compliance. Samen is dat 50% op het hoogste niveau.

Maar aan de onderkant leunt 23% nog op kantoorautomatisering en handmatige processen, met 4% op geïsoleerde softwarepakketten. Dat is 27% op het laagste niveau, en dat in een sector die sinds januari 2025 onder DORA valt en waar de toezichthouder actief toetst.

De middenmoot (23% data-geïnformeerd, terugkijkend) is opvallend dun. Je bent in de financiële sector óf vooruit, óf je staat stil. Er is nauwelijks tussenweg.

Advocatuur en accountancy



Bij de advocatuur, het notariaat en de accountancy ziet het beeld er wezenlijk anders uit. Hier werkt 38% nog puur op kantoorautomatisering en handmatige processen, met 8% op geïsoleerde pakketten. Samen 46% op het laagste niveau. Het gemiddelde (2.5 op 5) is het laagste van alle deelsectoren in ons onderzoek.

Dat is op zichzelf niet schokkend, de juridische sector heeft geen DORA-verplichtingen en de aard van het werk (persoonlijk advies, complexe casuïstiek) leent zich minder voor platformisering. Maar het wordt relevanter als je bedenkt dat deze kantoren hun klanten adviseren over digitale wetgeving: AVG-compliance, AI Act-readiness, DORA-implementatie. De geloofwaardigheid van dat advies wordt ondermijnd als de eigen digitale basis achterblijft.

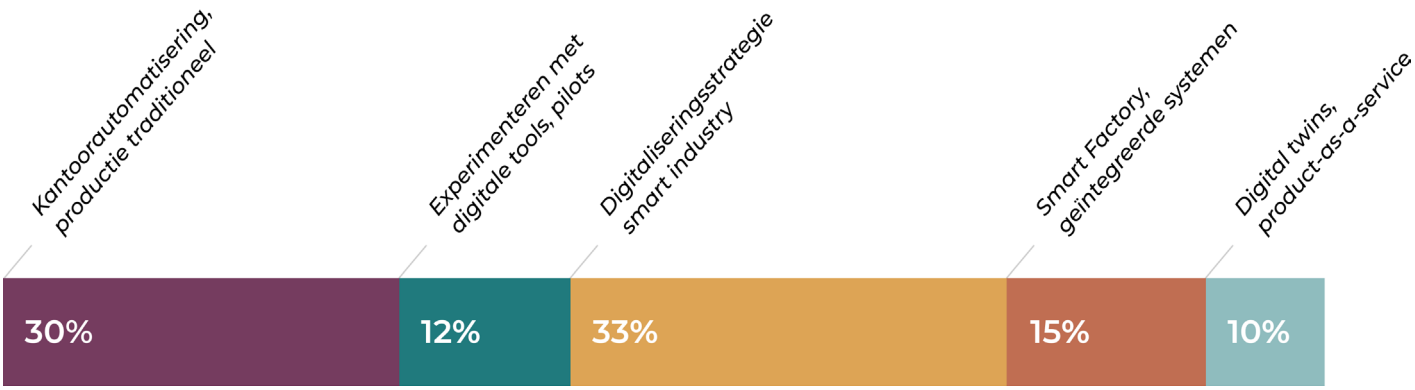
Kleine en middelgrote kantoren scoren het laagst (gemiddeld 2.2). Pas bij grote kantoren (250+) stijgt het gemiddelde naar 3.2. De schaaldrempel voor digitale transformatie in deze sector is hoog.

HR, detachering en ondersteunende diensten

De overige deelsectoren, HR en detachering, management- en strategieadvies, ondersteunende bedrijfsdiensten, beantwoorden eigen volwassenheidsvragen die gaan over positionering (uitvoerend vs. strategisch) en technologie-inzet (handmatig vs. geautomatiseerd). De helft van de HR-consultants positioneert zich als uitvoerend of op het niveau van bewezen oplossingen. Bij ondersteunende diensten is het beeld iets beter: 36% zet procesautomatisering in en 18% gebruikt AI om de dienstverlening te transformeren. Maar de aantallen per deelsector zijn te klein voor harde conclusies.

4.4 Productie & industrie

De productiesector (n=45) laat een patroon zien dat je elders niet terugvindt: de organisatie digitaliseert langzamer dan het product.



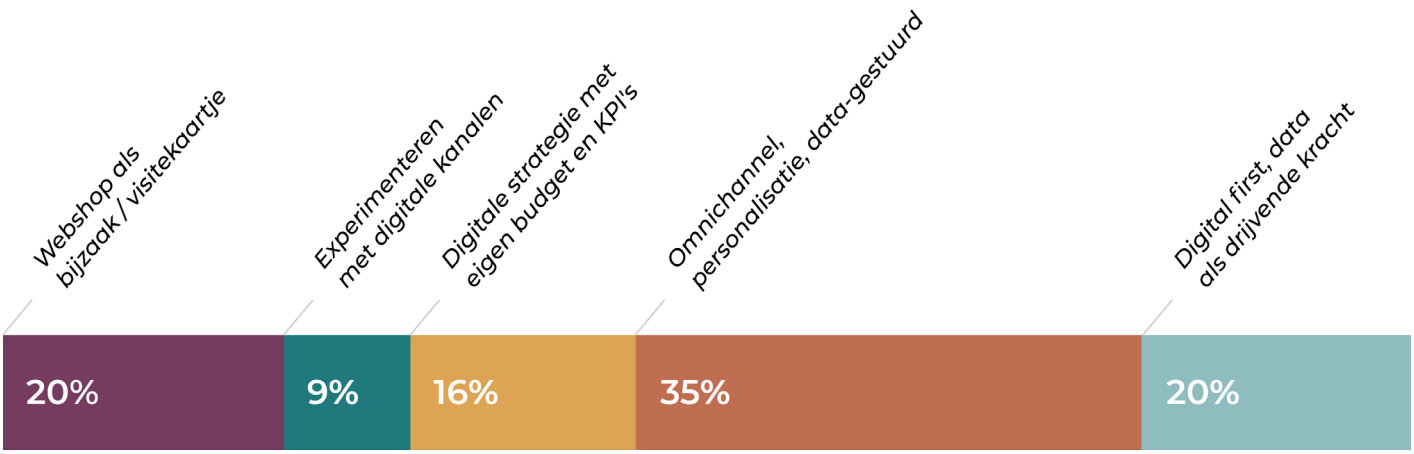
Bijna een derde (30%) heeft digitalisering beperkt tot kantoorautomatisering en basis bedrijfsprocessen. De productieomgeving is grotendeels traditioneel. Nog eens 12% experimenteert met digitale tools in de productie, sensoren op specifieke machines, een pilotproject, maar dat leidt nog niet tot strategische aanpassingen. Samen is dat 42% op het laagste niveau.
De grootste groep (33%) heeft een duidelijke digitaliseringsstrategie voor de productieprocessen: smart industry, gericht investeren in het verbinden van machines en systematisch data verzamelen. 15% opereert als Smart Factory met geïntegreerde business-systemen en voorspellend onderhoud. En 10% zet digitalisering in als kern van het businessmodel met digital twins en product-as-a-service.

Het contrast met de productdata is scherp. Van de respondenten die de vraag beantwoordden, bevat 85% software of IoT-connectiviteit in het product. Die producten zijn dus digitaler dan de organisaties die ze maken. Het bedrijf opereert op Excel en e-mail, maar het product stuurt data naar de cloud. Die kloof is een compliancepROBLEEM. De CRA verplicht fabrikanten tot security-by-design, vulnerability handling en updatebeleid. Dat veronderstelt een organisatie die weet wat er met haar producten gebeurt na levering. Bij 42% op niveau 1-2 is dat niet vanzelfsprekend.

Een lichtpunt: de Omnibus Act heeft industriële AI-toepassingen in het productieproces grotendeels uit de directe AI Act-verplichtingen gehaald (verplaatsing naar Bijlage B). Dat vermindert de reguleringsdruk op de 80% die AI inzet in het product. Maar voor producenten van medische hulpmiddelen (13% van de respondenten) en veiligheidscomponenten blijft de AI Act onverkort gelden, en de CRA geldt voor iedereen met een connected product.

4.5 Handel & retail

De handel is de best gedigitaliseerde sector in ons onderzoek.



Ruim de helft (55%) opereert op niveau 4 of 5: omnichannel-strategie met gepersonaliseerde klantervaring, of volledig digital first. De volwassenheidsvraag ging hier over de rol van digitalisering in de brede bedrijfsvoering: van "webshop als bijzaak" tot "data en technologie als drijvende kracht."

Dat de handel vooroploopt, is niet verrassend: de sector digitaliseert al twee decennia en de concurrentiedruk (e-commerce, platforms, consumentenverwachtingen) dwingt tot voortdurende investering.

Wat wél opvalt, is het contrast met de productiesector. De voorkant van de keten, handel, retail, klantinteractie, is bij 55% op het hoogste niveau. De achterkant, productie, fabrieksautomatisering, supply chain, zit voor 42% nog op basisniveau. Die

asymmetrie schept een knelpunt: de winkel is digitaal, maar de fabriek die levert is dat niet. In het kader van de Data Act en de CRA, die eisen stellen aan de hele keten van product tot eindgebruiker, is dat een relevant gegeven.

De sector is relatief licht gereguleerd vergeleken met financieel of publiek. De EAA (toegankelijkheid van webshops), de CRA (voor importeurs en distributeurs van digitale producten) en het consumentenrecht zijn de voornaamste wettelijke raakpunten. Voor marktplaatsen komt daar de DSA bij.

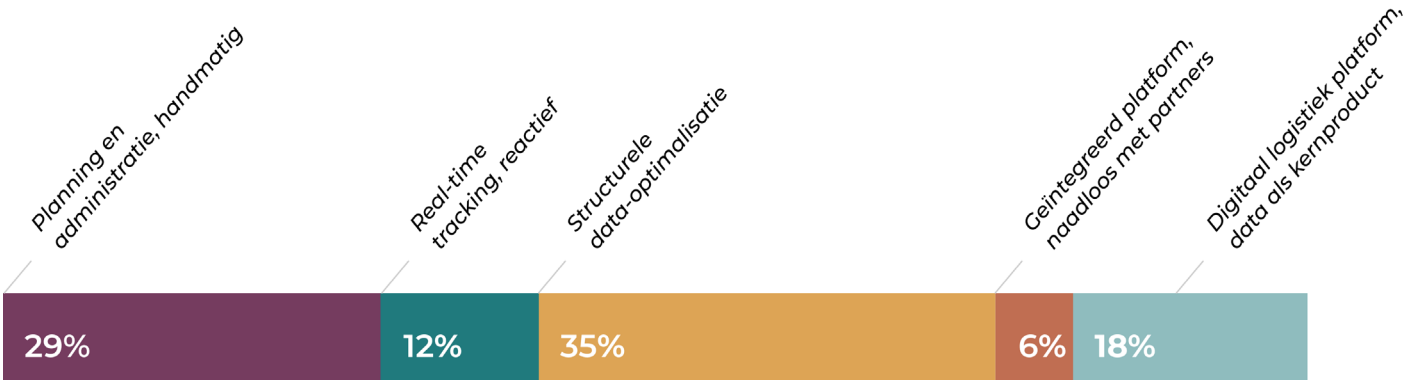
4.6 Overige sectoren

Transport en logistiek, infrastructuur en nuts-voorzieningen, en cultuur en recreatie zijn elk met minder dan 50 respondenten vertegenwoordigd. De bevindingen zijn daarom alleen richtinggevend, maar de aantallen zijn te klein voor harde uitspraken.

Transport & logistiek

De transportsector is verdeeld. Bijna een derde (29%) gebruikt digitale tools alleen voor planning en administratie. Dat maakt inzicht in de actuele status van transporten beperkt en vereist veel handmatige communicatie. De grootste groep (35%) gebruikt vloot- en managementsystemen structureel voor optimalisatie. Maar aan de bovenkant opereert 18% als volledig digitaal logistiek platform dat de hele keten bedient.

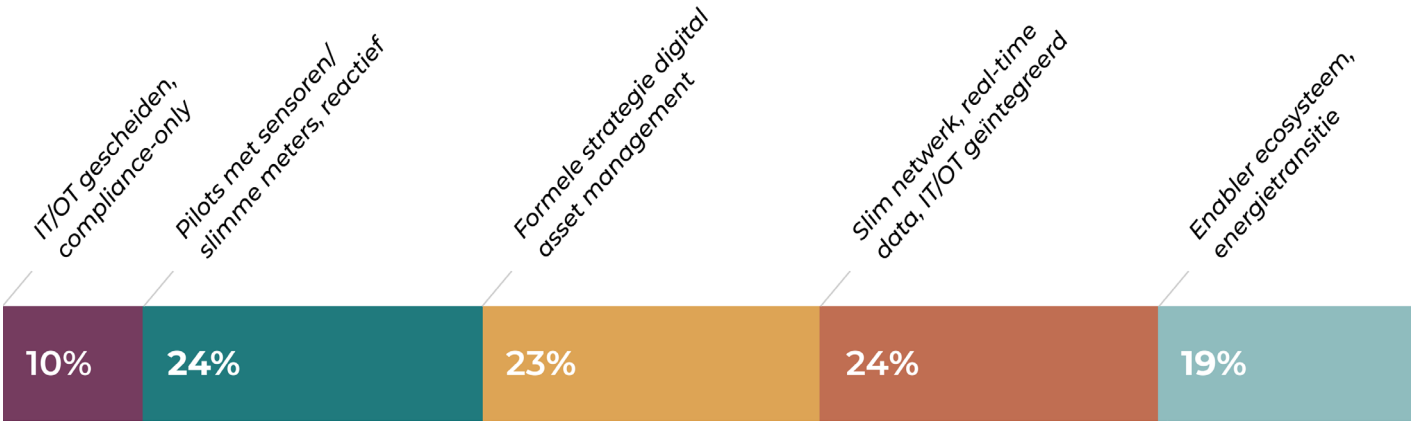
Opvallend is het hoge AI-gebruik in deze relatief kleine steekproef: 59% zet AI in voor operationele doelen en 47% stuurt personeel of zzp'ers aan met behulp van AI. Gecombineerd met het feit dat 44% zzp'ers aanstuurt via algoritmische systemen, is de transportsector een sector waar de AI Act en de Platform Work Directive tegelijkertijd ingrijpen.



Infrastructuur & nuts

De infrasector laat het meest extreme patroon zien van alle sectoren: er is vrijwel geen middenmoot. Ruim een derde (34%) zit op niveau 1-2, oftewel gescheiden IT- en OT-systemen, pilots en reactief databeheer. Maar bijna de helft (43%) opereert op niveau 4-5: slim netwerk met real-time data, of een platform dat de energietransitie faciliteert.

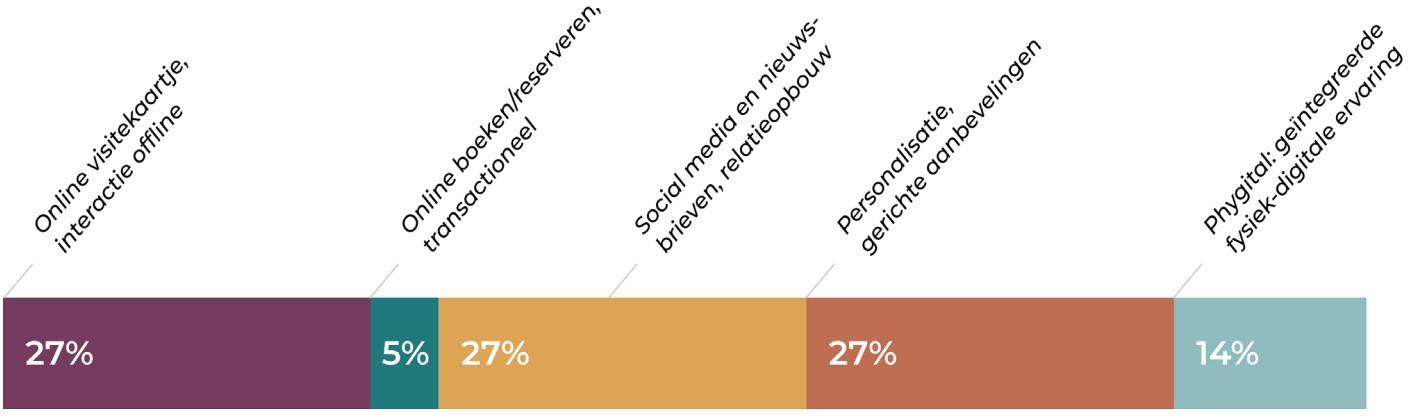
Die polarisatie weerspiegelt een sectorstructuur waarin grote nutsbedrijven en netwerkbeheerders zwaar investeren in digitalisering, terwijl kleinere spelers in water, afval of regionale infrastructuur achterblijven. Voor NIS2, dat de hele sector als essentieel classificeert, is die achterblijvende groep een zorg.



Cultuur, recreatie & overige diensten

De culturele sector is de meest diverse in ons onderzoek: van musea tot sportclubs, van hotels tot stichtingen. Ruim een kwart (27%) gebruikt digitalisering als visitekaartje: de website toont basisinformatie, de echte interactie is offline. Maar aan de andere kant personaliseert eveneens 27% actief de bezoekerservaring met data, en 14% biedt een geïntegreerde fysiek-digitale ervaring.

De wetgevingsdruk is beperkter dan in andere sectoren, maar niet afwezig. De EAA stelt sinds juni 2025 toegankelijkheidseisen aan online kaartverkoop en self-service terminals: en 55% van deze sector biedt dat aan. Wie digitaal op visitekaartje-niveau opereert maar wel online tickets verkoopt, heeft een probleem dat niet met een nieuw logo op de website is opgelost.



5. Van volwassenheid naar wetgeving: wat komt er op je af?

De vorige hoofdstukken lieten zien waar organisaties staan. Dit hoofdstuk laat zien wat er op hen afkomt, en hoe groot de kloof is tussen die twee.

De Digital Decade Roadmap stelt niet alleen een volwassenheidsvraag. Per sector worden ook gerichte vragen gesteld over activiteiten die bepalen welke wetgeving van toepassing is: gebruik je AI in je product? Bevatten je producten IoT? Lever je aan de financiële sector? Verwerk je gezondheidsgegevens? De antwoorden op die vragen maken het mogelijk om per sector te bepalen welke wetten raken en hoeveel organisaties dat betreft.

Drie wetten springen er sectoroverstijgend uit. We behandelen ze eerst als dwarsdoorsnede, en geven daarna per sector het bredere wetgevingslandschap.

5.1 AI Act is overal, niet alleen in de techsector

De AI Act is de meest besproken wet van de Digital Decade, maar het debat concentreert zich op de verkeerde plek. De aandacht gaat naar GPAI-modellen en de techsector: wie bouwt de grote taalmodellen, wie moet transparant zijn over trainingsdata. De data uit ons onderzoek laten zien dat de werkelijke impact veel breder is.

In de zorgsector zet 52% AI in voor triage of diagnose. 46% gebruikt AI als medisch hulpmiddel. Dat zijn toepassingen die onder Annex I en III van de AI Act als high-risk kwalificeren. Ze vereisen een conformiteitsbeoordeling, een risicobeheersysteem, eisen aan trainingsdata, menselijk toezicht, transparantie en technische documentatie, en dat alles voordat ze op de markt mogen worden gebracht of in gebruik genomen.

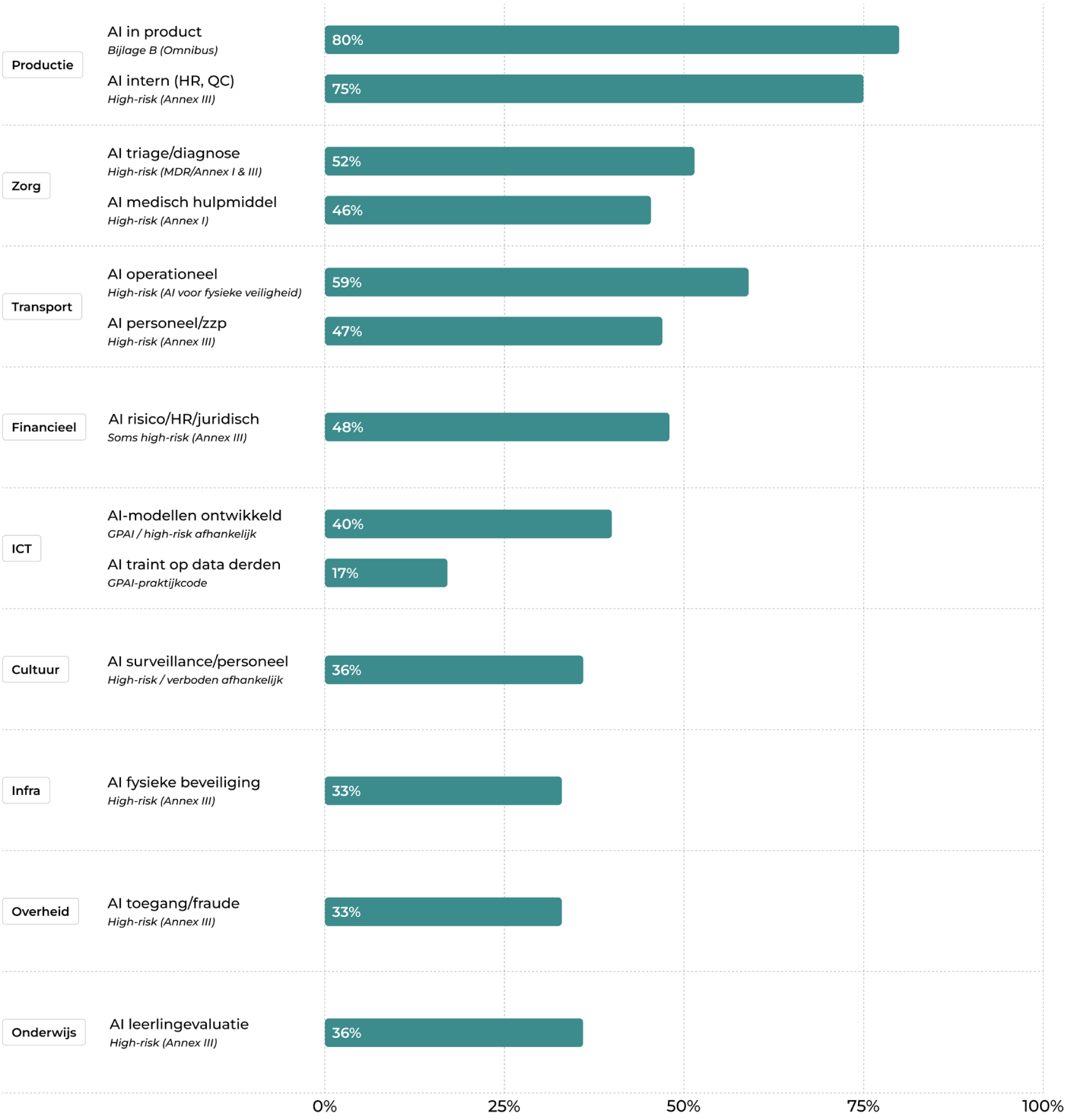
In de financiële sector past 48% AI toe voor kredietbeoordeling, risicomodellering, werving of juridische besluitvorming. Kredietbeoordeling en biometrische identificatie zijn expliciet high-risk. AI in werving en selectie eveneens.

In de transportsector gebruikt 59% AI voor operationele doelen, zoals routeoptimalisatie, dynamische prijsstelling, autonome voertuigfuncties. Verder stuurt 47% personeel of zzp'ers aan met behulp van AI. Die laatste categorie raakt niet alleen de AI Act (werknemersmanagement is high-risk) maar ook de Platform Work Directive.

Bij de overheid gebruikt 33% AI voor het beoordelen van toegang tot publieke diensten of voor fraudedetectie. In het onderwijs zet 36% AI in voor leerlingevaluatie. Zelfs in de culturele sector gebruikt 36% AI voor surveillance op evenementen of het aansturen van personeel. Biometrische identificatie in real-time op openbaar toegankelijke plaatsen, is onder de AI Act in beginsel verboden, met beperkte uitzonderingen voor rechtshandhaving.

De productiesector verdient een aparte vermelding. Met 80% AI-gebruik in het product en 75% intern, scoort deze sector het hoogst. Maar de Omnibus Act heeft industriële productietoepassingen grotendeels verplaatst naar Bijlage B, waarmee de directe AI Act-verplichtingen wegvallen. Dat is een substantiële verlichting. Het geldt echter niet voor AI in medische hulpmiddelen of veiligheidscomponenten daarvan. Daar blijft de AI Act onverkort van toepassing.

AI gebruik per sector



In de ICT-sector ontwikkelt 40% AI-modellen of -toepassingen en traint 17% modellen op data van derden. Die laatste groep valt mogelijk onder de GPAI-verplichtingen: een samenvatting van trainingsdata publiceren, een auteursrechtbeleid voeren, en aan transparantie-eisen voldoen. Die verplichtingen gelden vanaf 2 augustus 2026.

De herziene AI Act tijdlijn.

De Omnibus Act heeft de deadlines verschoven. GPAI-transparantieverplichtingen gelden vanaf 2 augustus 2026. Maar high-risk-verplichtingen voor Annex III-toepassingen gelden pas vanaf 2 december 2027. Annex I-toepassingen (productveiligheid) vanaf 2 augustus 2028.

Achttien maanden klinkt als ruimte. Maar de implementatie van een AI-managementsysteem (inventarisatie, classificatie, risicobeoordeling per toepassing, documentatie, governance, menselijk toezicht, monitoring) is voor de meeste organisaties een project van maanden. Wie nu nog niet begonnen is met ten minste de inventarisatie, loopt het risico de deadline niet te halen.

5.2 Beveiligingsplicht voor slimme apparaten

De Cyber Resilience Act stelt beveiligingseisen aan elk product met een digitaal element dat op de Europese markt wordt gebracht. Dat is breder dan het klinkt: niet alleen consumentenelektronica en IoT-apparaten, maar ook industriële machines met embedded software, SaaS-producten en standalone software.

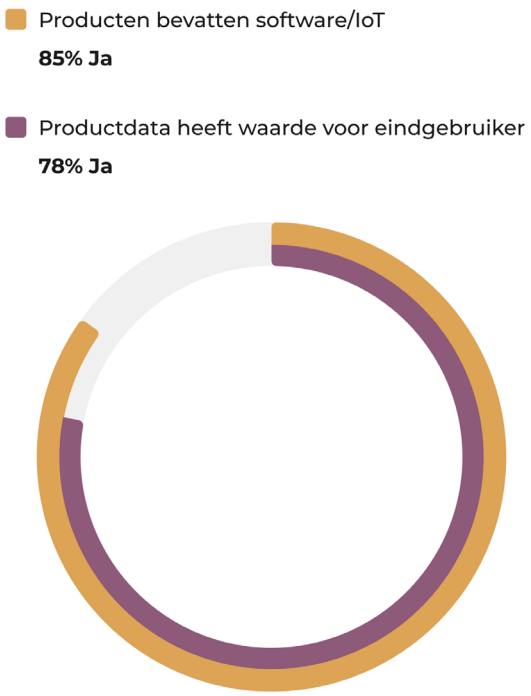
De impact concentreert zich in twee sectoren.

Productie. Van de productiebedrijven die de vraag beantwoordden, geeft 85% aan dat hun producten software of internetconnectiviteit bevatten. Bij 78% genereert het product data die waarde heeft voor de eindgebruiker, wat naast de CRA ook de Data Act activeert.

De CRA stelt twee soorten eisen. Fabrikanten moeten producten secure-by-design ontwikkelen, een software bill of materials bijhouden, kwetsbaarheden actief monitoren en beveiligingsupdates leveren gedurende de verwachte levensduur van het product. Daarnaast geldt een meldplicht: actief misbruikte kwetsbaarheden moeten binnen 24 uur worden gemeld aan het nationale CSIRT (in Nederland het NCSC) en aan ENISA.

De meldplicht geldt vanaf september 2026. De volledige beveiligingseisen gelden vanaf 11 december 2027.

Dat 85% van de productiebedrijven connected products maakt, is op zichzelf niet verrassend. Wat wél opvalt, is de combinatie met de volwassenheidsdata. 42% van deze sector opereert op digitaal niveau 1 of 2: kantoorautomatisering of experimentele pilots. Die bedrijven maken producten die straks aan CRA-beveiligingseisen moeten voldoen, maar hebben de interne organisatie (security-expertise, vulnerability management, gestructureerde softwareontwikkeling) er nog niet voor staan.



ICT. Alle software met digitale elementen valt onder de CRA. Dat raakt de hele softwaresector: 67% biedt SaaS-diensten aan. Open source met commercieel karakter valt er ook onder. De CRA maakt geen onderscheid tussen een industrieel besturingssysteem en een boekhoudpakket, als het software is met netwerkmogelijkheden, gelden de eisen.

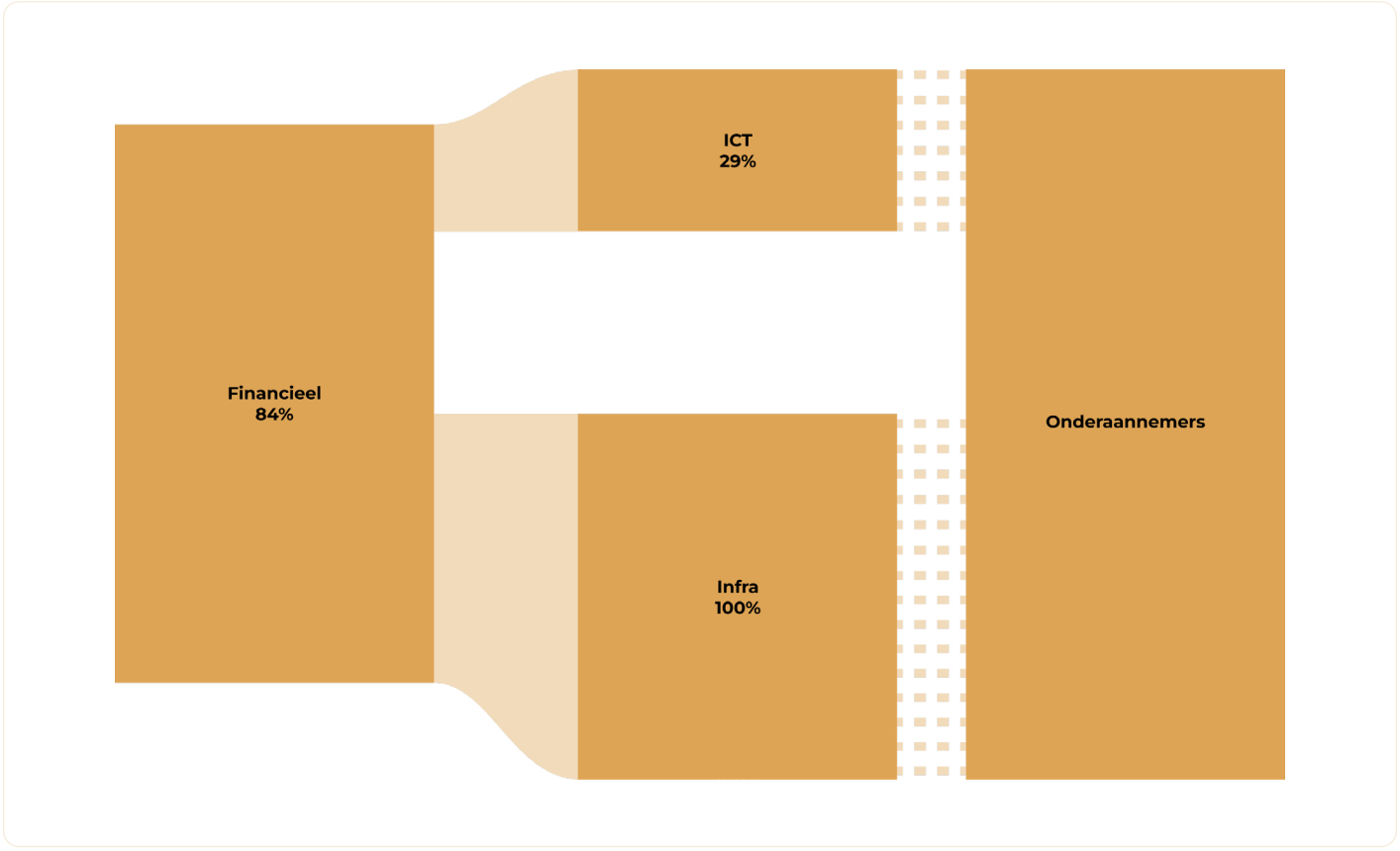
Voor softwarebedrijven die hun product als SaaS aanbieden en geen gebruiksdata verzamelen (45% van de softwarerespondenten), is de CRA een bijzondere uitdaging. De verplichte vulnerability monitoring veronderstelt dat je weet wat er met je product gebeurt in het veld. Als je niet meet hoe je software wordt gebruikt, kun je ook niet meten of er iets misgaat. Voor deze organisaties kan de migratieplicht en gebruiksrechten rondom data uit de Data Act ook een forse kluif zijn.

5.3 DORA door de keten

De Digital Operational Resilience Act (DORA) is van kracht sinds 17 januari 2025. De wet stelt eisen aan het ICT-risicobeheer van financiële instellingen: banken, verzekeraars, pensioenfondsen, beleggingsondernemingen en betaaldienstverleners. Maar de werkelijke impact reikt veel verder dan de financiële sector zelf.

In ons onderzoek geeft 84% van de financiële respondenten aan bank, verzekeraar of pensioenfonds te zijn. Zij vallen direct onder DORA's verplichtingen: ICT-risicobeheer, incidentrapportage, resilience testing en beheer van derdepartij-ICT-risico's. Dat laatste betekent dat financiële instellingen contractuele eisen moeten stellen aan hun ICT-dienstverleners: incidentmelding, auditrechten, exit-strategieën, continuïteit.

Die contractuele eisen werken door naar de keten. Van de ICT-respondenten in ons onderzoek levert 29% diensten aan financiële instellingen. Van de infrastructuur- en datacenter-respondenten die deze vraag beantwoordden, doet 100% dat. Die organisaties vallen daarmee potentieel onder DORA's regime voor "kritieke derde ICT-dienstverleners", met directe toezichteisen vanuit de Europese toezichthoudende autoriteiten.



Het keteneffect stopt niet bij de eerste ring. ICT-dienstverleners die aan banken leveren, stellen op hun beurt eisen aan hún leveranciers. Een hostingpartij die aan een MSP (Managed Service Provider) levert die aan een bank levert, zit drie schakels verwijderd van de financiële sector maar voelt de druk van DORA net zo goed.

In ons onderzoek onder de financiële sector heeft 44% een toeleveringsketen buiten de (EER) Europese Economische Ruimte. Dat voegt een extra dimensie toe: DORA's eisen aan derdepartijbeheer veronderstellen dat je grip hebt op de gehele keten, inclusief onderaannemers in derde landen. Als je clouddienstverlener in de VS zit en je subcontractor in India, moet je kunnen aantonen dat de hele keten aan DORA-normen voldoet.

De praktische implicatie: als je levert aan een bank, een verzekeraar of een pensioenfonds, gelden er indirect eisen aan jou. Bereid je voor op contractuele aanpassingen, auditverzoeken en incidentrapportageverplichtingen, ook als je zelf niet in de financiële sector opereert.

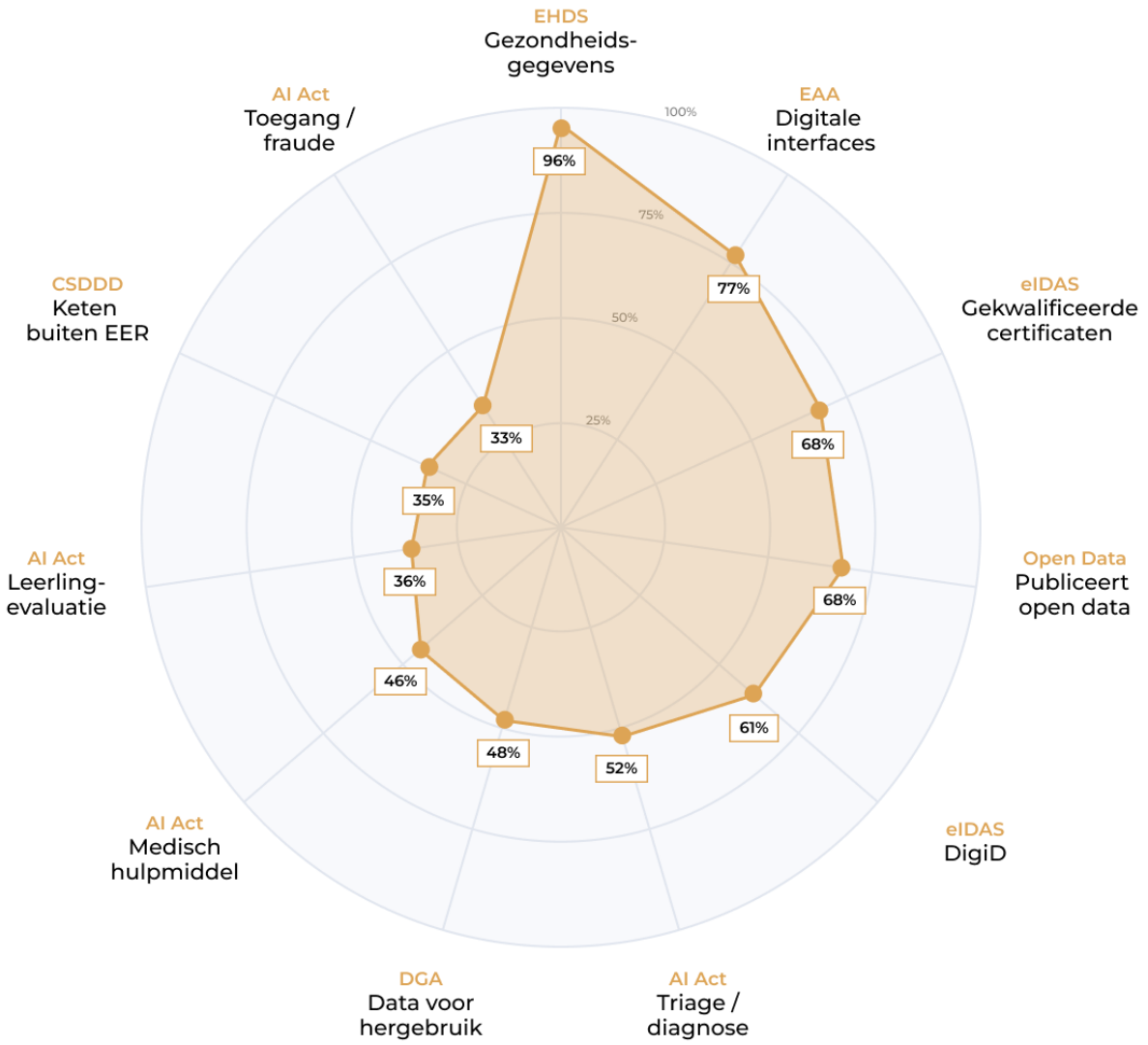
5.4 Het bredere wetgevingslandschap per sector

Naast de drie sectoroverstijgende wetten hierboven raakt elke sector een eigen combinatie van wetgeving. De tabellen hieronder geven per sector aan welke wetten op basis van onze data relevant zijn, voor welk percentage van de respondenten, en met welke deadline.

De percentages zijn gebaseerd op de antwoorden van respondenten die de betreffende vraag beantwoordden. Niet iedereen kreeg elke vraag, de Roadmap gebruikt branching op basis van eerdere antwoorden.

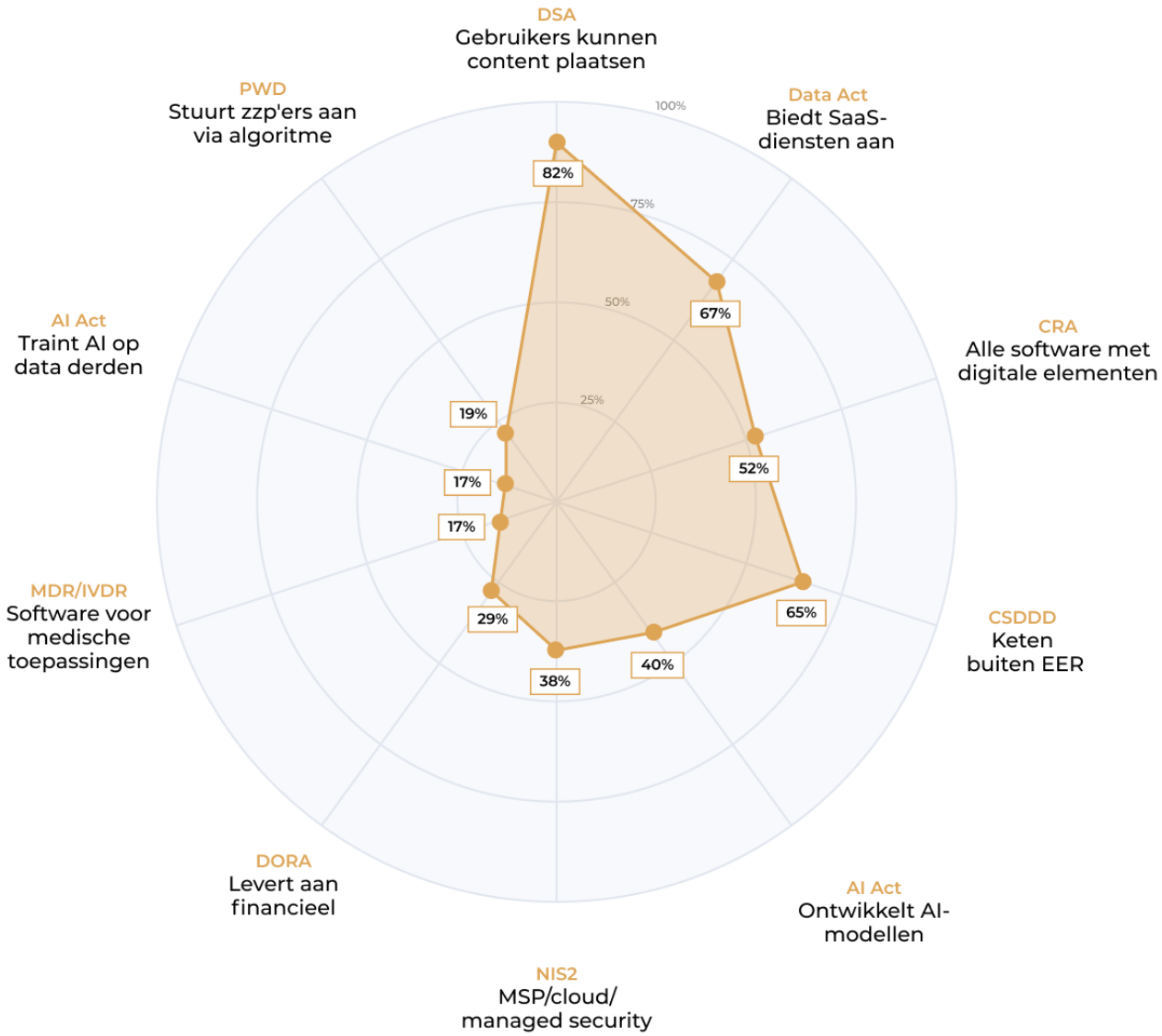
Publiek, zorg & onderwijs

De publieke sector is de sector met de breedste wetgevingsexposure. Geen andere sector scoort op zoveel indicatoren tegelijk hoog. Een middelgroot ziekenhuis kan tegelijkertijd te maken krijgen met de EHDS, de AI Act, de EAA, NIS2, de AVG en eIDAS. Dat vereist geen zes afzonderlijke compliancetrajecten maar een geïntegreerde aanpak.



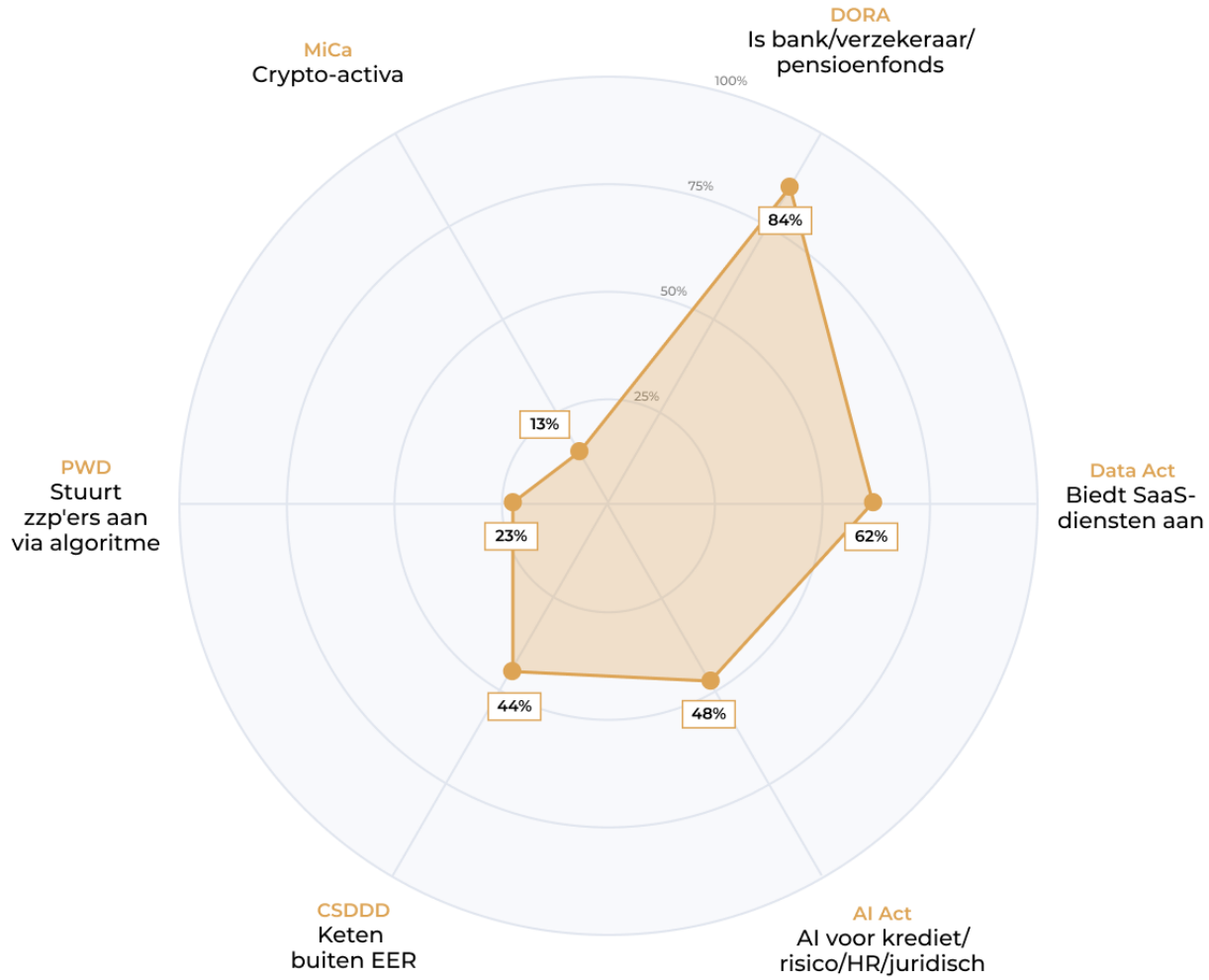
ICT & Media

De ICT-sector wordt minder breed geraakt dan de publieke sector, maar dieper per wet. De combinatie CRA + DORA + NIS2 treft organisaties die software leveren aan gereguleerde sectoren bijzonder hard. En de 17% die AI traint op data van derden, valt onder GPAI-verplichtingen die al over zes weken gelden.



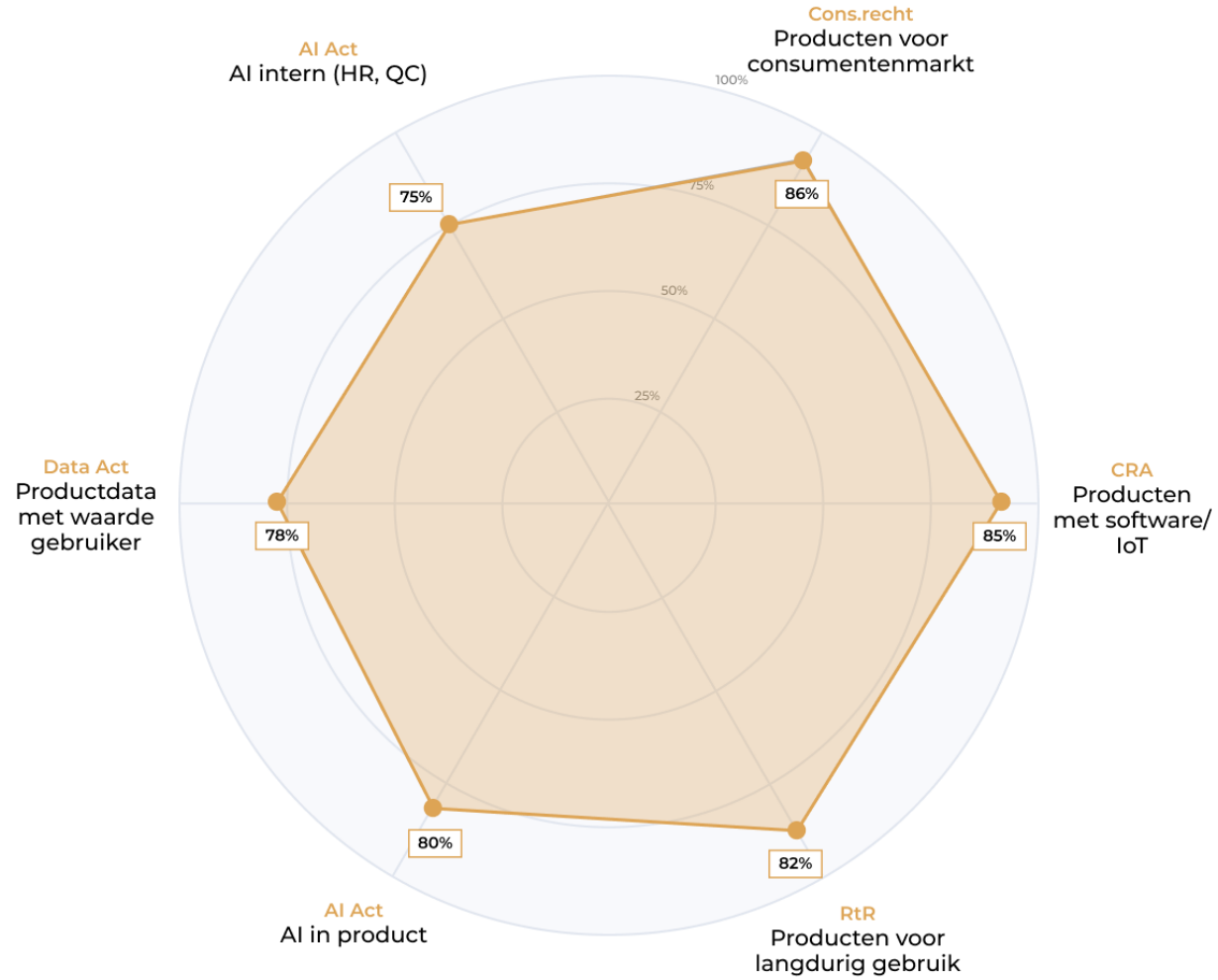
Financieel & zakelijk

De financiële en zakelijke sector laat een ander patroon zien dan de overige sectoren. Hier is niet de breedte van de wetgevingsexposure het verhaal, maar de diepte van één wet. 84% van de financiële instellingen is direct DORA-plichtig, en die wet is al van kracht. Dat maakt deze sector de enige waarin de zwaarste regulering niet toekomstig is maar actueel. Tegelijk wordt het beeld vertekend doordat de tabel banken en advocatenkantoren samenvoegt. Voor banken is DORA het zwaartepunt, aangevuld met AI Act-verplichtingen voor de 48% die AI inzet in kredietbeoordeling of risicomodellering. Voor de juridische en zakelijke dienstverlening is DORA niet aan de orde, maar speelt de Platform Work Directive (23% stuurt zzp'ers algoritmisch aan). De 13% met crypto-activiteiten valt onder MiCA — een nichewet maar met zware verplichtingen voor wie eronder valt.



Productie & industrie

De productiesector heeft het interessantste profiel: de percentages zijn overal hoog. Vrijwel iedereen maakt iets dat onder minstens twee wetten valt. De CRA en de Data Act zijn de meest acute, de CRA vanwege de naderende meldplicht in september 2026, de Data Act omdat die al geldt.

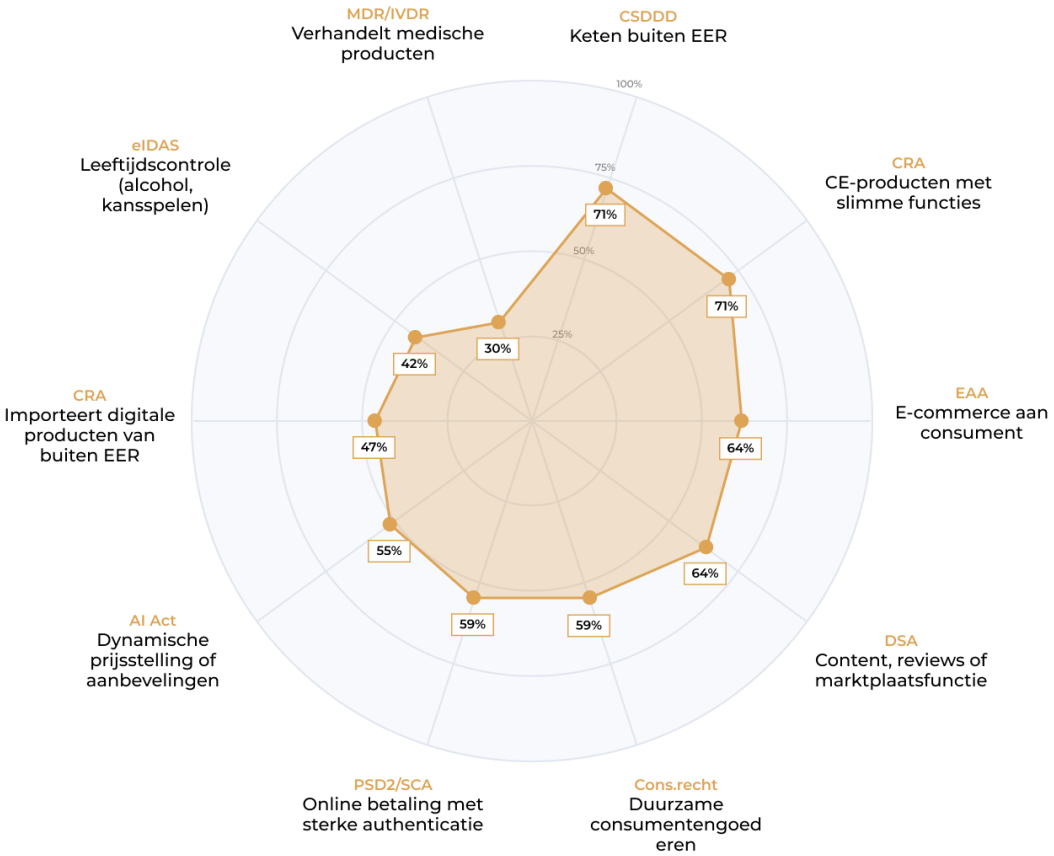


Handel & retail

De handel laat een ander patroon zien dan de overige sectoren, vanwege de zeer hoge ketenexposure. Met 71% die een toeleveringsketen buiten de EER heeft, deelt de handel de eerste plaats met de infrasector. De CSDDD raakt hier niet een handvol multinationals maar de meerderheid van de sector: importeurs, groothandels en retailers die inkopen in Azië of elders buiten Europa.

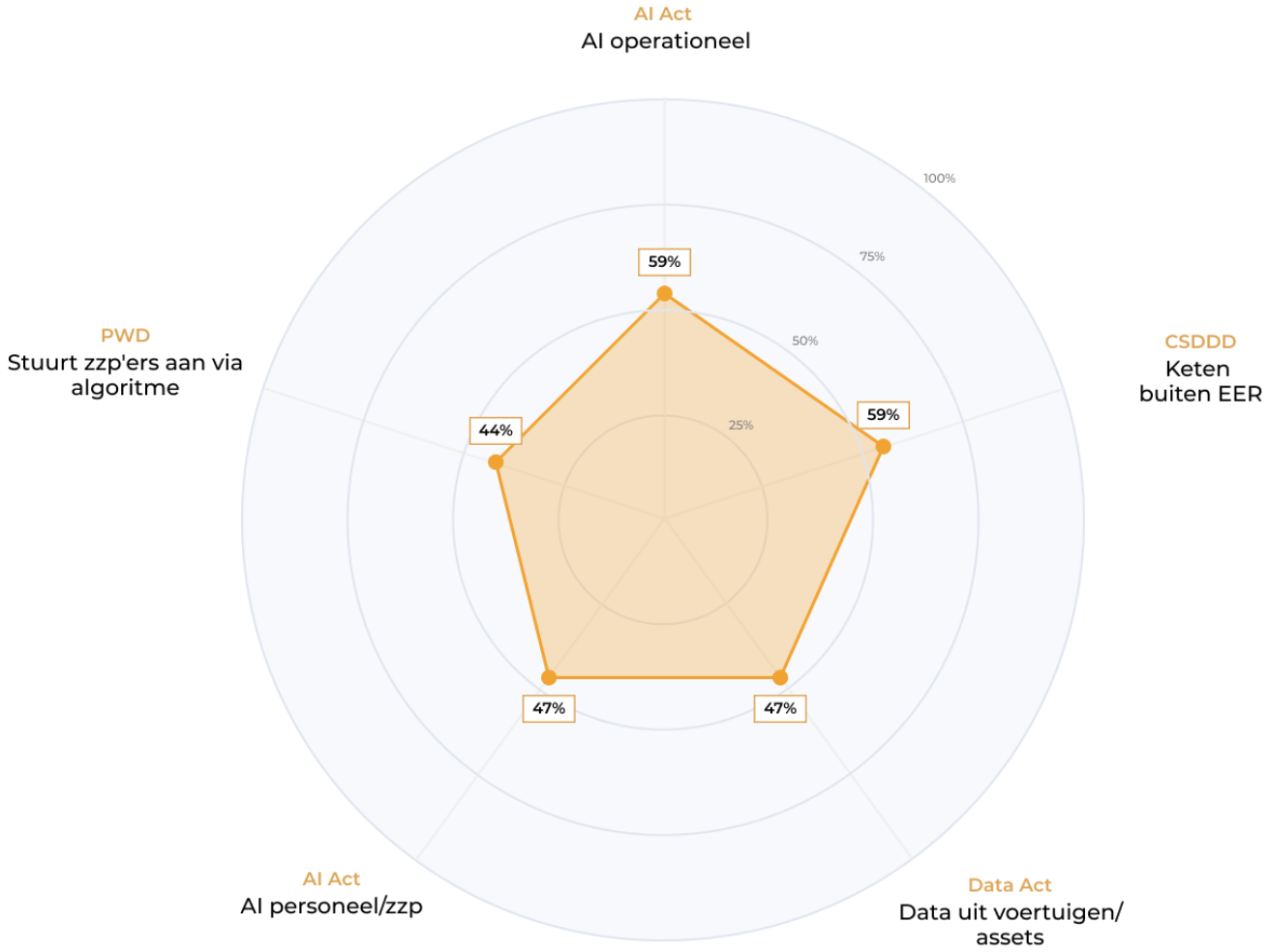
Opvallend is ook de dubbele CRA-blootstelling. 71% verkoopt producten met CE-keurmerk en slimme functies. Als distributeur of retailer ben je medeverantwoordelijk voor de conformiteit van die producten. Daarnaast importeert 47% digitale producten van buiten de EER, wat je onder de CRA tot importeur maakt met eigen verplichtingen: je moet controleren of de fabrikant aan de beveiligingseisen voldoet, en als dat niet het geval is, mag je het product niet op de markt brengen. Dat is een andere rol dan de handel gewend is: niet alleen verkopen, maar ook toetsen.

De 55% die AI inzet voor dynamische prijsstelling of aanbevelingssystemen verdient aandacht. De AI Act classificeert bepaalde vormen van prijsbeïnvloeding als risicovol, met name waar kwetsbare consumenten worden gemanipuleerd. En de DSA stelt transparantie-eisen aan aanbevelingssystemen op platforms: 64% van de marktplaatsen en platformrespondenten biedt gebruikers de mogelijkheid om content of producten te plaatsen, wat hen onder de DSA-verplichtingen voor online tussenhandeldiensten brengt.



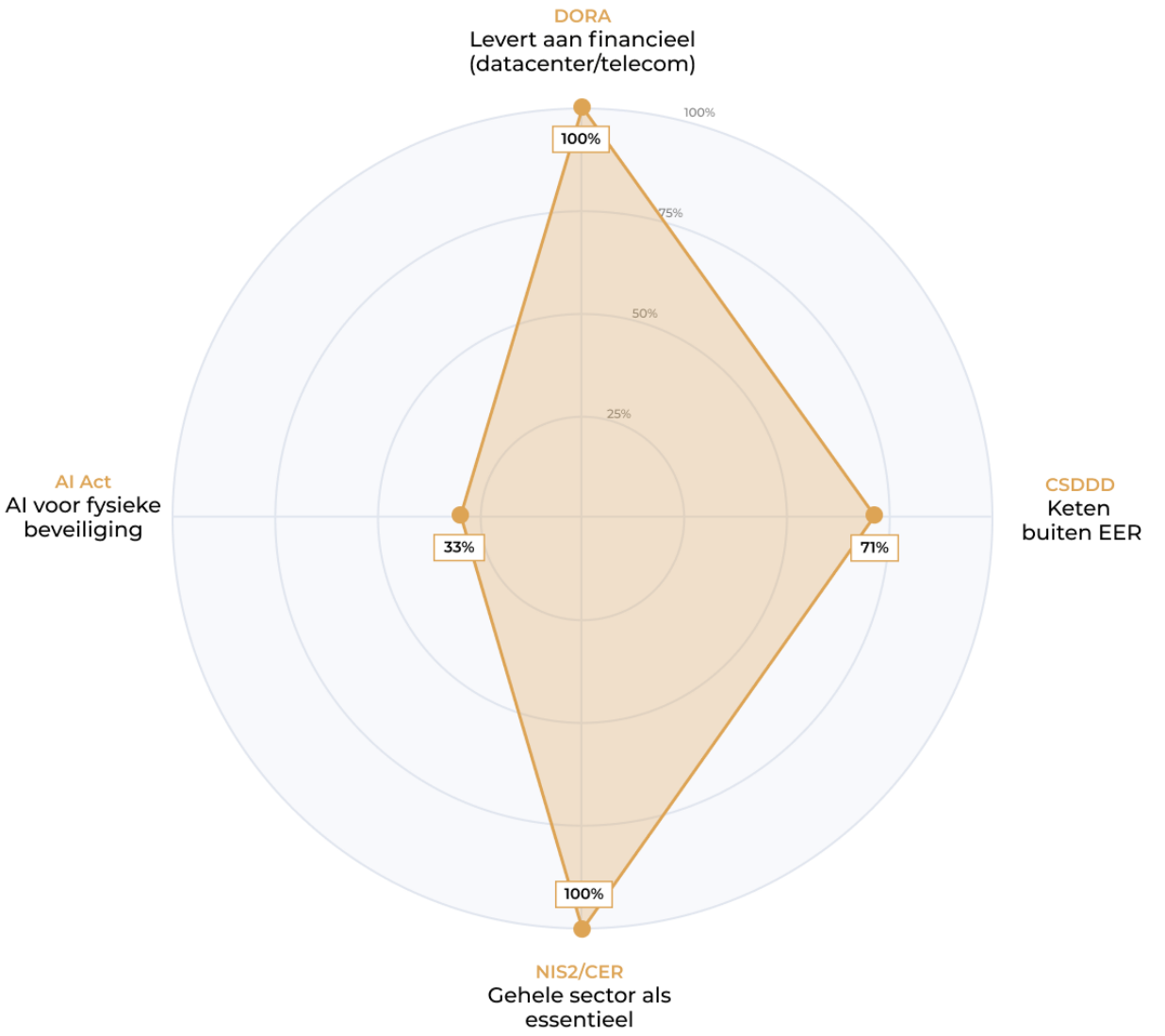
Transport & logistiek

De transportsector is klein in onze steekproef maar opvallend in profiel: op alle indicatoren scoort men meer dan 44%. De combinatie van hoog AI-gebruik (59% operationeel, 47% personeel) en algoritmisch aansturen van zzp'ers (44%) maakt dit de sector waar de AI Act en de Platform Work Directive het sterkst tegelijkertijd ingrijpen. Dat onderscheidt transport van alle andere sectoren: elders is het één van de twee, hier zijn het allebei. Voeg daar de 59% met een toeleveringsketen buiten de EER bij, en je hebt een sector die met drie zware regimes tegelijk te maken krijgt terwijl ruim een derde digitaal nog op basisniveau opereert. biedt gebruikers de mogelijkheid om content of producten te plaatsen, wat hen onder de DSA-verplichtingen voor online tussenhandeldiensten brengt.



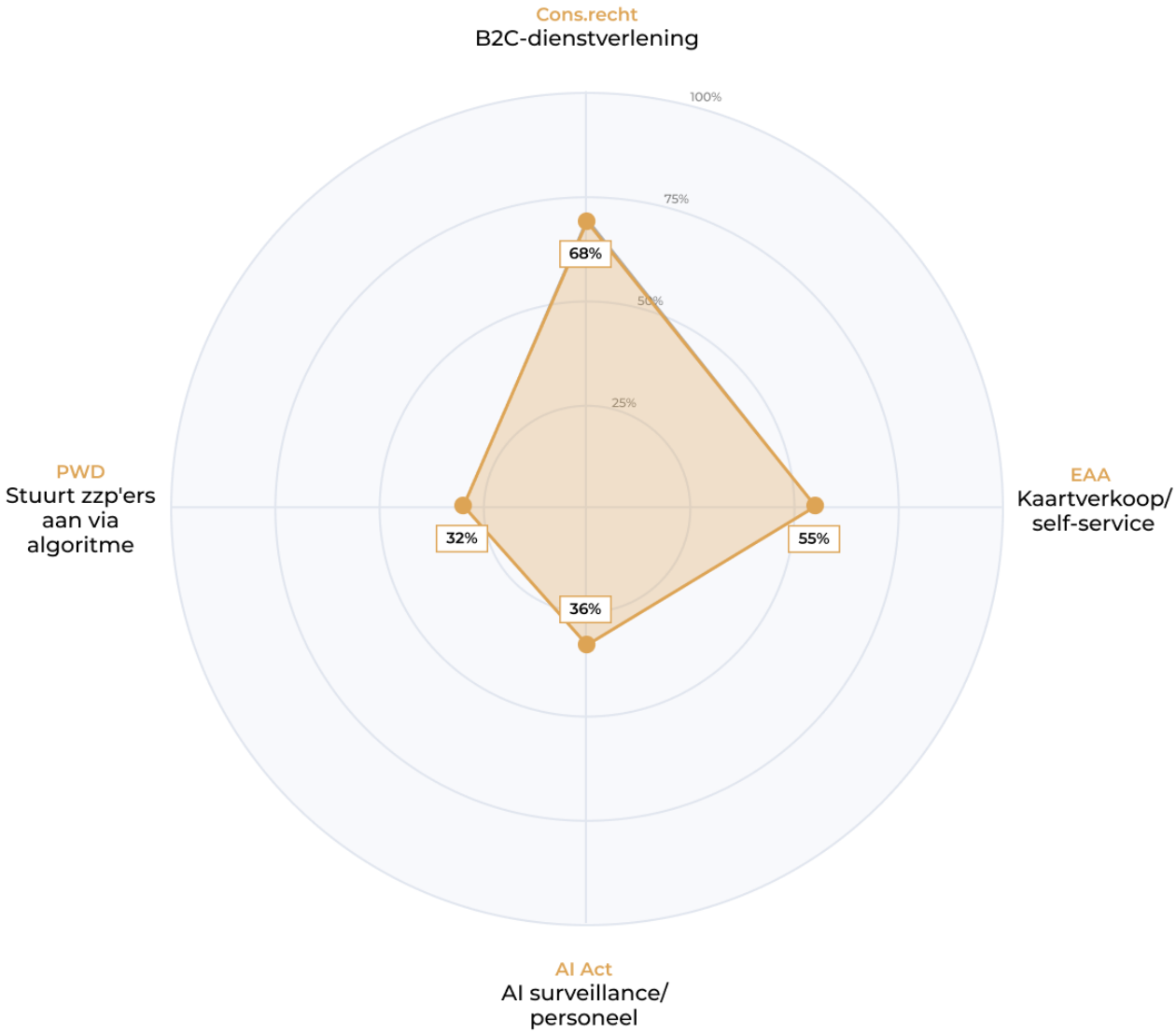
Infrastructuur & nuts

De infrasector heeft het eenvoudigste maar hardste wetgevingsprofiel: NIS2 en CER gelden voor de gehele sector als essentiële entiteiten. Dat is geen percentage maar een feit. Wie levert aan de financiële sector, krijgt daar DORA's ketenregime bovenop. En 71% heeft een toeleveringsketen buiten de EER, wat CSDDD-exposure geeft op het niveau van de handel. Dat de sector tegelijk het meest gepolariseerd is in volwassenheid (34% op niveau 1-2, 43% op niveau 4-5) maakt de combinatie kwetsbaar: de achterblijvers moeten aan dezelfde wettelijke eisen voldoen als de koplopers, maar missen de digitale basis om dat waar te maken.



Cultuur, recreatie & overige diensten

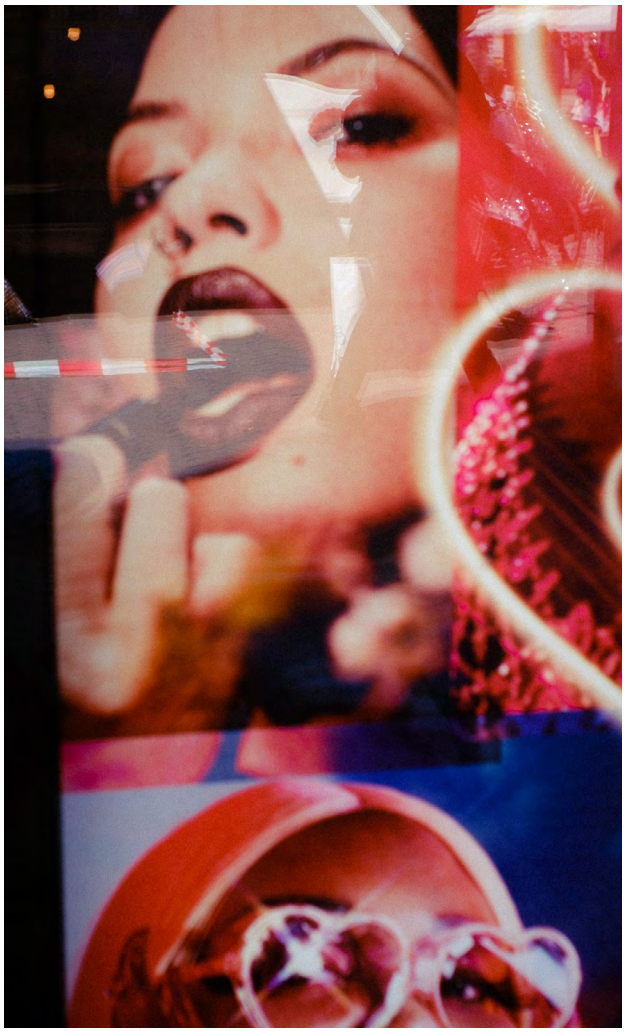
De culturele sector wordt lichter geraakt dan de andere sectoren, maar niet zo licht als veel organisaties denken. De EAA is het meest acute raakpunt: 55% biedt online kaartverkoop of self-service aan, en de toegankelijkheidseisen gelden al sinds juni 2025. Dat 27% van de sector digitaal nog op visitekaartje-niveau opereert maar wel online tickets verkoopt, schept een concreet compliancerisico. De 36% die AI inzet voor surveillance of personeelsaansturing raakt aan de zwaarste categorie van de AI Act, en de 32% die zzp'ers algoritmisch aanstuurt valt mogelijk onder de Platform Work Directive. Het zijn geen grote aantallen, maar het zijn organisaties die zich doorgaans niet als gereguleerd beschouwen, en dat juist daardoor risico lopen.



5.5 De tijdlijn: wat geldt wanneer?

Het wetgevingslandschap is niet alleen breed, het is ook gelaagd in de tijd. Sommige wetten zijn al van kracht en worden actief gehandhaafd. Andere hebben een concrete deadline in de komende achttien maanden. En weer andere zijn nog in onderhandeling. Het overzicht hiernaast ordent de belangrijkste mijlpalen chronologisch.

De tijdlijn maakt twee dingen zichtbaar. Ten eerste: er is al veel van kracht. Organisaties die denken dat ze nog tijd hebben, onderschatten hoeveel wetten al gelden. DORA, de Data Act, de EAA en de DSA zijn geen toekomstige verplichtingen maar huidige. Ten tweede: de piek van nieuwe verplichtingen valt in het vierde kwartaal van 2027, wanneer de AI Act high-risk en de CRA volledige toepassing tegelijkertijd ingaan. Dat is anderhalf jaar weg. Wie dan pas begint, is te laat.



2025

Q1 2025	DORA 17 januari 2025
Q2 2025	EAA 28 juni 2025
Q3 2025	Data Act September 2025
Doorlopend	DSA Gefaseerd volledig van kracht
Doorlopend	AVG, MDR/IVDR, consumentenrecht Doorlopend

2026

Q3 2026	AI Act: CPAI-transparantie 2 augustus 2026
Q3 2026	CRA: meldplicht kwetsbaarheden September 2026
Loopt	NIS2: nationale implementatie Loopt
Q4 2026	Platform Work Directive December 2026

2027

Q4 2027	AI Act: high-risk Annex III 2 december 2027
	CRA: volledige toepassing 11 december 2027
	CSDDD: grote ondernemingen 2027
	CADA: onderhandelingen Q4 2027

2028 / 2029

Q3 2028	AI Act: Annex I (Productveiligheid) 2 augustus 2028
2028 - 2029	CSDDD: Middelgroot Geleidelijke uitbreiding
2029	CADA: eerste effecten (schatting) 2029

6. Aanbevelingen: wat nu te doen

De vorige hoofdstukken lieten zien waar je staat en wat er op je afkomt. Dit hoofdstuk vertelt je wat je nu moet doen. Niet alles is even urgent. Sommige wetten gelden al. Andere hebben een deadline in 2027. En weer andere zijn nog in onderhandeling. De kunst is om te beginnen waar het het hardst nodig is.

6.1 Productie & industrie

Je maakt producten die digitaler zijn dan je organisatie. 85% van de productiebedrijven in ons onderzoek maakt connected products, terwijl 42% digitaal op basisniveau opereert. De CRA en de Data Act zijn je meest acute verplichtingen. De AI Act raakt je minder dan je denkt: de Omnibus Act heeft industriële AI-toepassingen grotendeels naar Bijlage B verplaatst, al blijft de wet gelden voor AI in medische hulpmiddelen en veiligheidscomponenten.

Nu: De CRA-meldplicht voor actief misbruikte kwetsbaarheden geldt vanaf september 2026. Als je producten met software of IoT-connectiviteit op de markt brengt, en dat doet 85%, moet je een proces inrichten om kwetsbaarheden te monitoren, te beoordelen en binnen 24 uur te melden aan het NCSC en ENISA. Begin vandaag met het opzetten van een vulnerability disclosure-beleid en een intern meldproces.

De Data Act is al van kracht. Bij 78% van de productiebedrijven genereert het product data met waarde voor de eindgebruiker. Die eindgebruiker heeft recht op toegang tot die data, en wel eenvoudig, veilig en kosteloos. Controleer of je producten dat ondersteunen. Als het antwoord nee is, heb je een probleem dat er al is.

Komend jaar: De volledige CRA-beveiligingseisen gelden vanaf 11 december 2027. Dat omvat secure-by-design, een software bill of materials (SBOM), een gecoördineerd vulnerability disclosure-proces en beveiligingsupdates gedurende de verwachte levensduur van het product. Dat vereist aanpassingen in je productontwikkelingsproces.

Start met CSDDD-ketenanalyse als je een grote of middelgrote onderneming bent met toeleveranciers buiten de EER. De eerste verplichtingen voor grote ondernemingen gelden vanaf 2027.

Structureel: Bouw cybersecurity in je product-ontwikkelingsproces in. De CRA maakt security-by-design een wettelijke eis, niet een best practice. En bouw data-toegangsrechten in je productarchitectuur in. De Data Act maakt dat een recht van de gebruiker.

6.2 ICT & Media

Je bouwt de producten waarmee de rest digitaliseert, maar 70% van de softwarebedrijven in ons onderzoek meet niet hoe het eigen product wordt gebruikt. Tegelijk lever je aan steeds meer gereguleerde sectoren: 29% aan financieel, 38% biedt MSP- of clouddiensten aan. De wetten van je klanten worden jouw wetten.

Nu: Als je diensten levert aan financiële instellingen (29%) en je contracten zijn nog niet aangepast aan DORA's outsourcing-eisen: dit is urgent. DORA is van kracht. Je klanten zijn verplicht om van jou incidentrapportage, auditrechten en exit-strategieën te eisen. Wacht niet tot ze bellen, maar neem het initiatief.

Als je MSP- of clouddiensten levert (38%): controleer je NIS2-status. De meldplicht voor incidenten (24 uur) geldt zodra de nationale implementatiewet van kracht is. Richt je meldproces nu in.

Als je SaaS aanbiedt (67%): de Data Act switchingrechten gelden al. Kunnen je klanten hun data exporteren in een gestandaardiseerd formaat? Zo niet, los dat op voordat een klant het als probleem ervaart.

Als je AI traint op data van derden (17%): de GPAI-transparantieverplichtingen gelden vanaf 2 augustus 2026. Dat is over zes weken. Je moet een samenvatting van je trainingsdata publiceren en een auteursrechtbeleid voeren.

Bij alle software: De CRA-meldplicht voor actief misbruikte kwetsbaarheden geldt vanaf september 2026.

Komend jaar: Start met AI Act-compliance als je AI-modellen of -toepassingen ontwikkelt (40%). GPAI-verplichtingen gelden al. High-risk-toepassingen hebben een deadline van 2 december 2027. Concreet: technische documentatie, risicobeoordeling, transparantie naar je afnemers.

Bereid de volledige CRA-compliance voor: secure development lifecycle, SBOM, vulnerability handling en incident reporting. Volledige toepassing: 11 december 2027.

Structureel: Bouw telemetrie en gebruiksmonitoring in je producten. Als je niet meet hoe je product wordt gebruikt, kun je het niet verbeteren, niet beveiligen, en niet compliant maken. De CRA en AI Act veronderstellen allebei dat je weet hoe je product in de praktijk functioneert. Bij 70% is dat nu niet het geval. Dat is een productrisico én een compliancerisico. Hetzelfde geldt voor je herstel- en verbeterproces van fouten in je software of diensten.

Richt gestructureerd leveranciersmanagement in als je levert aan gereguleerde sectoren. De eisen vanuit DORA, NIS2 en straks de CADA stromen via je klanten naar jou door. Ken je klantenportfolio, en weet welke regimes je indirect binden.

6.3 Financieel & zakelijk

Deze sector valt uiteen in twee werelden die je apart moet aanpakken.

Banken & verzekeraars

Je sector is gepolariseerd: 50% opereert op het hoogste niveau, maar 27% leunt nog op handmatige processen of geïsoleerde pakketten. DORA is van kracht en de toezichthouder toetst actief. AI-gebruik is breed (48% voor krediet, risico, HR of juridisch) en valt grotendeels onder de AI Act high-risk-categorieën.

Nu: DORA is je eerste prioriteit. Als je ICT-uitbestedingscontracten nog niet zijn aangepast aan DORA's eisen (incidentmelding, auditrechten, exit-strategie, continuïteit): dit is niet een volgend-kwartaal-probleem. De wet geldt, het toezicht loopt.

Inventariseer je AI-toepassingen in kredietbeoordeling, risicomodellering en fraudedetectie. Classificeer ze onder de AI Act. De Omnibus Act geeft uitstel tot 2 december 2027, maar de inventarisatie en classificatie kosten maanden. Begin dus nu.

Komend jaar: Implementeer AI Act-compliance voor high-risk-toepassingen: risicobeoordeling, bias-monitoring, menselijk toezicht, transparantie naar betrokkenen. Integreer dit in je bestaande DORA-complianceframework, want de overlap op ICT-risicobeheer is groot.

Structureel: Start met CSDDD-ketenanalyse als je een toeleveringsketen buiten de EER hebt (44%).

Advocatuur, accountancy & overige zakelijke dienstverlening

46% van de advocaten- en accountantskantoren in ons onderzoek opereert op het laagste digitale niveau. Het gemiddelde is 2.5 op 5. Kleine en middelgrote kantoren scoren het laagst (gemiddeld 2.2).

Nu: Begin bij de basis. Niet bij de AI Act of de CADA, bij je AVG-verwerkingsregister, je toegangsbeheer, je back-upbeleid. Als 46% van je sector nog op kantoorautomatisering draait, is de eerste stap niet compliance met de nieuwste wet maar je digitale huishouding op orde brengen.

Komend jaar: Als je zzp'ers aanstuurt via digitale tools (23% in de bredere zakelijke sector): beoordeel of de

Platform Work Directive van toepassing wordt bij nationale implementatie in december 2026.

Structureel: Je adviseert klanten over digitale compliance. Investeer in je eigen digitale volwassenheid. Niet alleen om compliance-redenen, maar omdat de geloofwaardigheid van je advies ervan afhangt.

6.4 Publiek, zorg & onderwijs

Je sector wordt geraakt door meer wetgeving tegelijk dan welke andere. Van EHDS tot EAA tot eIDAS tot AI Act, op vrijwel elke as scoort meer dan de helft van de organisaties "ja." De uitdaging is niet één wet, maar de stapeling. En 41% van de publieke dienstverlening opereert digitaal nog op basisniveau.

Nu: De EAA geldt sinds juni 2025. 77% van de publieke organisaties biedt digitale interfaces aan burgers. Controleer of je websites, apps en terminals voldoen aan WCAG 2.1 niveau AA. Werk toe naar EN 301 549 compliance.

Inventariseer je AI-gebruik. Met 52% AI in triage en diagnose, 46% AI als medisch hulpmiddel, 33% in toegangsbeoordeling en 36% in leerlingevaluatie zit de publieke sector vol high-risk-toepassingen. De deadline (2 december 2027) biedt ruimte, maar de omvang van het werk, en meerdere high-risk-categorieën per organisatie, maakt vroeg beginnen noodzakelijk.

Als je DigiD aanbiedt (64%): volg de ontwikkelingen rondom eIDAS 2.0 en de Europese digitale identiteitsportemonnee. Er hoeven nu nog geen technische wijzigingen worden doorgevoerd, maar de strategische planning moet starten.

Komend jaar: EHDS-implementatie voorbereiden. 96% van de zorginstellingen verwerkt elektronische gezondheidsgegevens. De verordening raakt vrijwel iedereen. Concreet: interoperabiliteit van EPD-systemen, dataportabiliteit voor patiënten, governance voor secundair gebruik van gezondheidsdata. Bij 32% van de zorg die het EPD nog primair als registratiesysteem gebruikt, is dit een fundamentele procesverandering.

AI Act-compliance implementeren. De publieke sector is uniek in het aantal overlappende high-risk-categorieën. Een middelgroot ziekenhuis kan tegelijkertijd AI in diagnostiek, in patiënttriage en in personeelsplanning gebruiken. Coördineer dit centraal.

NIS2-implementatie voor overheden en zorginstellingen die als essentiële entiteiten kwalificeren: incidentmeldprocedures, risicobeheer, supply chain security.

Structureel: Werk toe naar een geïntegreerd digitaal loket. 41% zit nog op niveau 1-2: alleen een website of losstaande formulieren. De Digital Decade-doelstelling is 100% online overheidsdiensten in 2030. Dat vereist systeemkoppelingen, niet alleen losse formulieren.

Lever je aan overheden, of koop je in als overheidsorgaan, bereid je voor op CADA. Hoewel deze wet nog ver weg lijkt, zijn dergelijke contracten lange termijn. Houd er rekening mee dat je bij de eerstvolgende contractverlenging zal worden gevraagd naar jouw niveau, en dat gunningen afhankelijk gemaakt kunnen worden van het voldoen aan CADA wanneer die Europese wet er door komt.

6.5 Handel & retail

De handel is de best gedigitaliseerde sector in ons onderzoek (55% op niveau 4-5), maar tegelijk de sector met de hoogste ketenblootstelling: 71% heeft een toeleveringsketen buiten de EER en 47% importeert digitale producten van buiten Europa. Digitale volwassenheid beschermt niet automatisch tegen wetgevingsrisico's. Ook de handel krijgt een rol toebedeeld die nieuw is: niet alleen verkopen, maar ook toetsen.

Nu: De CRA-meldplicht geldt vanaf september 2026. Als je producten met CE-keurmerk en slimme functies verkoopt, ben je als distributeur medeverantwoordelijk. Importeer je die producten van buiten de EER (47%), dan is je rol nog zwaarder: als importeur moet je controleren of de fabrikant de conformiteitsbeoordeling heeft uitgevoerd, of de technische documentatie beschikbaar is, en of het product een CE-markering draagt. Begin

dus nu met het inventariseren van je assortiment: welke producten bevatten software of IoT, en wat weet je over de compliance van de fabrikant?

De EAA geldt al. Wie handel drijft met consumenten (64%) moet zorgen dat zijn digitale kanalen voldoen aan de relevante standaarden. Eén daarvan is transparantie over AI: als je een AI-chatbot inzet, moet deze duidelijk en transparant zijn over diens status. En als je een marktplaatsfunctie biedt, gelden ook DSA-verplichtingen rond transparantie van aanbevelingssystemen en moderatie van content en reviews.

Komend jaar: Diverse vormen van dynamic pricing en productpresentatie vallen onder de AI Act als verboden manipulatieve AI-algoritmen. Classificeer je AI-toepassingen en beoordeel of ze onder de transparantie- of conformiteitseisen vallen.

Met 71% die een toeleveringsketen buiten de EER heeft, is de handel samen met de infrasector de meest blootgestelde sector aan ketenverantwoordelijkheid. De eerste verplichtingen voor grote ondernemingen gelden vanaf 2027. Begin met het in kaart brengen van je keten. Dat omvat niet alleen je directe leveranciers maar ook de productie daarachter.

Structureel: Omarm je nieuwe rol en verantwoordelijkheid. Waar je vroeger kon volstaan met inkopen en verkopen, maakt de CRA je medeverantwoordelijk voor de beveiliging van de producten die je op de markt brengt. De CSDDD maakt je medeverantwoordelijk voor de keten erachter. En de DSA maakt je medeverantwoordelijk voor wat er op je platform gebeurt. Dat geeft nieuwe taken: leveranciersbeoordeling op compliance, producttesting op digitale veiligheid, en platformgovernance op content en algoritmes.

6.6 Transport, infra & cultuur

Transport & logistiek

De transportsector combineert hoog AI-gebruik (59% operationeel, 47% personeel) met hoog platformgebruik (44% stuurt zzp'ers algoritmisch aan). Dat maakt je de sector waar de AI Act en de Platform Work Directive het sterkst tegelijkertijd ingrijpen.

Nu: Beoordeel of je algoritmisch aansturen van zzp'ers onder de Platform Work Directive valt. Nationale implementatie komt eind 2026 en kan de arbeidsrelatie fundamenteel veranderen. Controleer daarnaast of je Data Act-verplichtingen nakomt: als je voertuigen of trackingsystemen data genereren (47%), hebben gebruikers recht op toegang.

Komend jaar: AI Act-classificatie voor operationele AI (59%). Met name bij autonoom transport en dynamische prijsstelling.

Infrastructuur & nuts

Je sector is volledig NIS2-plichtig en 34% opereert op het laagste digitale niveau. Die combinatie is zorgelijk: NIS2 veronderstelt continue monitoring, incidentrespons en supply chain security. Dat vereist een digitale basis die er bij een derde van de sector niet is.

Nu: NIS2 en CER zijn van kracht. Als je nog geen incidentmeldprocedure, risicobeheerplan en supply chain security-beleid hebt: dit is de meest urgente actie in dit hele rapport. Daarnaast: als je datacenter- of telecomdiensten levert aan financiële instellingen (100% van die respondenten): bereid je voor op DORA-audits en contracteisen.

Komend jaar: CSDDD-ketenanalyse. Met 71% die een toeleveringsketen buiten de EER heeft, is dit het hoogste percentage van alle sectoren.

Cultuur & recreatie

De wetgevingsdruk is beperkter maar niet afwezig. 55% biedt online kaartverkoop of self-service. De EAA geldt daar al voor. 36% gebruikt AI voor surveillance of personeel. Classificeer die toepassingen onder de AI Act.

Nu: EAA-compliance als je online kaartverkoop of self-service aanbiedt. Controleer of je digitale kanalen WCAG 2.1 AA-compliant zijn. Dit geldt nu.

Komend jaar: AI Act-classificatie. Biometrische identificatie in real-time op evenementen is in beginsel verboden.

Van Roadmap naar actieplan: de Praktijkdag Digital Decade

De aanbevelingen in dit hoofdstuk zijn sectoraal en algemeen. De vertaling naar jouw organisatie, welke prioriteit als eerste, welke afdeling pakt het op, hoe krijg je je bestuur mee, vraagt om verdieping.

Tijdens onze Praktijkdag Digital Decade werk je in één dag met je eigen Roadmap aan een concreet 100-dagen actieplan, samen met onze juristen en met hands-on inzet van AI-assistenten uit het AI Pro Pack. Je gaat naar huis met heldere prioriteiten, eigenaarschap en antwoord op de vraag: waar begin ik?

Bekijk de Praktijkdag Digital Decade

6.7 Cross-sectoraal: drie universele actiepunten

Drie aanbevelingen gelden voor elke organisatie, ongeacht sector of omvang.

1. Inventariseer je AI-toepassingen dit kwartaal.
In elke sector in ons onderzoek gebruikt een substantieel deel AI, vaak in contexten die als high-risk kwalificeren. De Omnibus Act biedt uitstel tot december 2027, maar de implementatie van een AI-managementsysteem kost maanden. Begin met de inventarisatie: welke AI-toepassingen draaien er, waar komen de data vandaan, wie houdt er toezicht op, en in welke risicocategorie vallen ze?

2. Ken je keten.
DORA werkt door naar ICT-leveranciers. NIS2 naar de supply chain. De CADA straks naar cloudleveranciers van de overheid. Als je levert aan gereguleerde sectoren, gelden de eisen indirect ook voor jou. Controleer je klantenportfolio en weet welke regimes je indirect binden. En omgekeerd: als je diensten afneemt van partijen buiten de EER, breng de risico's in kaart.

3. Breng je digitale basis op orde.
In de productiesector zit 42% op basisniveau. In de publieke dienstverlening 41%. In de advocatuur 46%. Veel van de wetgeving die op deze organisaties afkomt veronderstelt registers, systeemkoppelingen, datagovernance en beveiligingsbeleid. Als die basis er niet is, is elke specifieke compliance-exercitie bouwen op drijfzand. De eerste stap is vaak niet "compliance met wet X" maar "je digitale huishouding op orde."

AI Act-readiness bij koplopers

De Barometer laat zien dat AI breed wordt ingezet: 52% van de zorg, 48% van de financiële sector, 33% van de overheid in high-risk-contexten. Maar hoe ver zijn organisaties met de voorbereiding?

Cijfers uit ons netwerk van CAICO®-professionals laten zien dat driekwart (74%) van organisaties met een dergelijke dedicated professional al goede slagen maakt met het inventariseren van AI-toepassingen, maar dat slechts 5% die inventarisatie volledig heeft afgerond. Wie begonnen ís, pakt door: 61% heeft voor alle geïdentificeerde toepassingen al een risicoclassificatie uitgevoerd. Het knelpunt is starten, niet classificeren.

7. Digitale soevereiniteit begint niet bij de tandarts

"Waarom individuele actie tekortschiet en Europa een collectief antwoord nodig heeft"

Arnoud Engelfriet
Chief Knowledge Officer

Laatst moest ik naar de tandarts. De afspraakbevestiging kwam via een Outlook-uitnodiging. Mijn gebit zit dus in de Amerikaanse cloud. Op LinkedIn zou deze tandarts worden afgefakkeld. Gezondheidsgegevens bij Big Tech! Weet ze wel dat Microsoft onder de CLOUD Act valt? Heeft ze een DPIA gedaan? Iemand zou een screenshot maken, er een post van maken met het woord "schandalig" erin, en drieduizend likes verder weet heel Nederland dat tandartsen het probleem zijn.

Maar mijn tandarts is niet het probleem. Mijn tandarts doet wat wij allemaal doen.

Iedereen zit in de cloud

In mei 2025 onderzocht de NOS 1.722 websites van Nederlandse overheidsorganisaties en cruciale bedrijven. Het resultaat: op precies één na gebruikten ze allemaal minstens één Amerikaanse clouddienst. Die ene uitzondering was de gemeente Hardinxveld-Giessendam, en die bleek bij navraag ook gewoon via de Drechtsteden op Amerikaanse cloud te draaien. De teller staat op nul.

Negen van de vijftien ministeries vergaderen via Microsoft Teams of Webex. De Autoriteit Financiële Markten, het Veiligheidsberaad, De Nederlandsche Bank, de politie; allemaal op Amerikaanse infrastructuur. De VS zou, aldus datzelfde NOS-onderzoek, met één druk op de knop ruim 650 Nederlandse overheidssites kunnen blokkeren of manipuleren. Inclusief Crisis.nl, de site waar burgers naartoe worden gestuurd bij rampen.

En ondertussen escaleert de geopolitieke context. De Verenigde Staten legden sancties op aan de aanklager van het Internationaal Strafhof in Den Haag, wat later werd uitgebreid naar rechters en aanklagers. Visumrestricties volgden voor voormalig Eurocommissaris Thierry Breton en vier anderen wegens hun rol bij de Digital Services Act. Microsoft verstrekte namen van Nederlandse ambtenaren die werken aan de uitvoering van de DSA aan het Amerikaans Congres. En toen het Amerikaanse Kyndryl het Nederlandse Solvinity wilde overnemen — hoster van DigiD — brak een publieke storm los. Er werden kort gedingen aangespannen om het DigiD-contract te beëindigen. De Tweede Kamer nam een motie aan met 141 stemmen tegen verlenging. De opluchting was voelbaar toen het kabinet de overname uiteindelijk blokkeerde via de Wet ongewenste zeggenschap telecommunicatie.

Maar diezelfde Tweede Kamer vergadert via Microsoft. Diezelfde overheid draait op Azure. En datzelfde Kyndryl bouwt op dit moment de complete IT-infrastructuur van het ministerie van Defensie om.

En het gaat niet alleen om infrastructuur. Medio juni plaatste de VS de meest geavanceerde AI-modellen Mythos en Fable van Anthropic op de Amerikaanse exportcontrolelijst. Niet-Amerikanen hebben er geen toegang meer toe. Geen sanctie, geen rechtszaak, geen politiek conflict: één exportregeling, en een technologie die gisteren beschikbaar was, is vandaag verboden terrein. Als dat kan met een AI-model, kan het met elke dienst die op Amerikaans grondgebied wordt beheerd.

Iedereen voelt dat dit wringt. Maar bijna niemand beweegt. Niet uit onwil, niet uit onwetendheid, maar omdat digitale soevereiniteit een collectief probleem is dat je niet individueel kunt oplossen.

Het juridische kader zegt: het mag

Laten we beginnen bij wat in het publieke debat steeds wordt overgeslagen: het juridische fundament.

Europa doet al dertig jaar alsof de Verenigde Staten een veilige bestemming zijn voor persoonsgegevens. Dat begon in 2000 met het Safe Harbor-verdrag, dat in 2015 door het Hof van Justitie werd vernietigd in Schrems I. De opvolger, het Privacy Shield, sneuvelde in 2020 in Schrems II. In 2023 nam de Europese Commissie voor de derde keer een adequaatheidsbesluit: het EU-US Data Privacy Framework. Driemaal is scheepsrecht, kennelijk.

Zolang dat besluit staat, mogen persoonsgegevens naar de VS worden doorgegeven zonder aanvullende waarborgen, mits de ontvangende partij gecertificeerd is onder het Framework. Microsoft, Google en Amazon zijn dat. Mijn tandarts met haar Outlook-agenda is niet in overtreding van de AVG. Een ziekenhuis op Azure evenmin. Een gemeente die via Teams vergadert al helemaal niet.

Dat dit derde adequaatheidsbesluit net zo kwetsbaar is als zijn voorgangers, weten we. Het Franse Kamerlid Philippe Latombe vocht het aan bij het Gerecht van de EU, maar werd in september 2025 niet-ontvankelijk verklaard. Hij heeft hoger beroep aangetekend bij het Hof van Justitie. En Max Schrems heeft te kennen

gegeven een derde zaak niet uit te sluiten. Maar tot het Hof spreekt, is het kader geldig. Je kunt individuele organisaties niet verwijten dat ze het kader volgen dat Europa zelf heeft neergezet.

Wat we wél kunnen vaststellen is dat de verontwaardiging niet alleen over privacy gaat. Ze gaat over blootstelling. De sancties tegen ICC-functionarissen, de dreigementen richting DSA-ambtenaren, de namenlijsten bij het Congres. Dat zijn geen abstracte risico's meer. Het zijn demonstraties van een machtspositie die we zelf hebben gecreëerd door onze complete digitale infrastructuur te bouwen op Amerikaanse fundamenten. De boosheid gaat niet echt over die specifieke ambtenaren of over Breton die niet meer naar de VS kan vliegen. De boosheid gaat over de plotselinge, oncomfortabele confrontatie met hoe afhankelijk we zijn. Het is, als we eerlijk zijn, deels schaamte die naar buiten wordt gericht.

En die schaamte leidt tot incidentgedreven reacties. Solvinity moest geblokkeerd worden. De structurele afhankelijkheid die het probleem veroorzaakt, blijft intact. Ik schreef elders uitgebreid over de juridische houdbaarheid van dat overnameverbod. De kern: als de CLOUD Act en de Amerikaanse sanctiebevoegdheid de reden zijn om Kyndryl te blokkeren als eigenaar van Solvinity, dan geldt dat argument voor élke Amerikaanse dienstverlener aan de Nederlandse overheid. Maar datzelfde Kyndryl legt de IT-infrastructuur voor Defensie aan. Dat kan niet daar een beheersbaar compliance-issue zijn en bij DigiD een onaanvaardbare schending van de Nederlandse soevereiniteit. De inconsistentie is het bewijs dat we geen kader hebben, maar alleen reflexen.

Het helpt ook niet dat niemand hetzelfde bedoelt met "soevereiniteit." Voor de een is het een contract met een Europees bedrijf. Voor de ander betekent het dat de supportmedewerker in India niet bij je mailbox kan. Weer een ander accepteert niets minder dan dat de NAND-chips in de server in Dresden zijn geëtst. Die niveaus schelen onderling een factor tien in kosten en een factor honderd in complexiteit, maar in het debat worden ze vrolijk door elkaar gebruikt. Het resultaat is dat de maximalist elke pragmatische stap afdoet als schijnoplossing, terwijl de pragmatist het jurisdictierisico wegwuift als theoretisch. Beiden hebben ongelijk. Het is precies deze begripsverwarring die maakt dat niemand beweegt: zelfs als je wílt, weet je niet waarheen.

Waarom niemand beweegt

Als het probleem zo breed wordt erkend, waarom handelt dan bijna niemand? Het antwoord is niet laksheid of onwetendheid. Het is een klassiek collectief-actieprobleem met drie versterkende mechanismen.

1. De netwerkval

Microsoft 365 is geen product, het is het weefsel van professionele samenwerking in Europa. Je kunt niet overstappen zonder dat je hele keten meekomt: klanten, leveranciers, samenwerkingspartners, brancheorganisaties. Ons eigen kantoor, een kantoor dat organisaties adviseert over digitale wetgeving, draait op Microsoft. Niet omdat we het risico niet kennen, maar omdat overstappen in isolatie ons afsnijdt van het ecosysteem waarin we opereren. Zoals Claude zou zeggen: dat is geen zwakte, dat is een marktstructuur. En voor één keer heeft de taalcomputer gelijk.

2. De kostenasymmetrie

De kosten van overstappen zijn direct, meetbaar en zeker: licenties, migratie, productiviteitsverlies, omscholing, compatibiliteitsproblemen. De baten — minder afhankelijkheid, minder extraterritoriaal risico — zijn diffuus, onzeker en langetermijn. Geen bestuurder, geen CFO, geen gemeenteraad tekent voor: "we worden dit kwartaal 20% minder productief zodat we over vijf jaar misschien minder kwetsbaar zijn voor een risico dat zich misschien niet materialiseert." Dat is geen kortzichtigheid. Dat is rationeel handelen onder onzekerheid.

3. De first-mover-straf

Wie als eerste overstapt, draagt alle kosten en oogst geen baten. Het Europese alternatief wordt pas levensvatbaar als genoeg partijen overstappen om het ecosysteem te dragen. Maar niemand wil de eerste zijn, want de eerste betaalt het meest en profiteert het minst. Dit is het prisoner's dilemma op continentale schaal, en de conclusie is bekend: zonder coördinatiemechanisme beweegt niemand.

De parallel met klimaat is verhelderend. We hebben het klimaatprobleem niet opgelost door burgers te vertellen dat ze minder moeten vliegen. We hebben het (deels, moeizaam) geadresseerd met emissiehandel, subsidies voor hernieuwbare energie, bouwvoorschriften en industriebeleid. Niemand verwachtte dat individuele huishoudens uit eigen beweging van gas zouden stappen zolang er geen warmtenet lag. Bij digitale soevereiniteit verwachten we precies dat: dat individuele organisaties eigenhandig migreren naar alternatieven die nauwelijks bestaan, in een ecosysteem dat niet op hen wacht, tegen kosten die ze alleen dragen.

Dat is geen realistisch beleid. Dat is de illusie van actie.

Wat er al gebeurt, en waarom het niet genoeg is

> *"Een Amerikaans bedrijf dat onder de CLOUD Act valt, kan volgens de CADA niet meedoen aan Europese of Nederlandse aanbestedingen."*

Het zou oneerlijk zijn om te zeggen dat er niets beweegt. Op 3 juni 2026 publiceerde de Europese Commissie het voorstel voor de Cloud and AI Development Act (CADA), als onderdeel van het bredere Tech Sovereignty Package. De CADA introduceert een vier-lagen classificatiesysteem voor cloud- en AI-diensten. Kritieke dienstverlening (denk aan overheidsinfrastructuur, gezondheidsdata, justitiële systemen) mag alleen worden ingekocht op de twee hoogste niveaus. Daar geldt een certificeringsplicht, en soevereiniteit is een harde eis: juridische en operationele onafhankelijkheid van derdelandsjurisdicties. Een Amerikaans bedrijf dat onder de CLOUD Act valt, kan daar naar de letter van het voorstel niet aan voldoen.

Dat is een serieuze stap. Het is voor het eerst dat de EU een horizontaal kader voorstelt dat soevereiniteitseisen codificeert in plaats van ze per sector of per incident te improviseren. En het is een aanbestedingsplicht, niet slechts een raamwerk: bij de eerstvolgende verlenging van een contract moet de toets worden doorlopen.

Maar er zijn beperkingen die eerlijke benoeming verdienen.

Allereerst dekt de CADA alleen public procurement. De private sector, waar het overgrote deel van de digitale economie draait, valt erbuiten. Mijn tandarts, elk MKB-bedrijf, elke private zorginstelling: voor hen verandert er niets.

Ten tweede gaat dit nog wel even duren. Parlement en Raad moeten er wat van vinden, en dit is me een partij politiek gevoelig. Trilogue-onderhandelingen hoeven we niet te verwachten eerder dan het vierde kwartaal van 2027. Na goedkeuring volgt een implementatieperiode. De eerste effecten zijn dus op zijn vroegst in 2029 voelbaar, krap een jaar voordat het Digital Decade-programma zijn einddatum bereikt.

En het is een voorstel. Big Tech heeft al het geld van de wereld, en de eerste legioenen aan lobbyisten lopen zich al warm. Wat er uiteindelijk uit de trilogue komt, hoeft niet te lijken op wat er in juni 2026 is ingediend.

Naast de CADA zijn er sectorale initiatieven. DORA stelt in de financiële sector eisen aan outsourcing naar clouddienstverleners, inclusief exit-strategieën. NIS2, heel positief gelezen, biedt voor de kritieke sector aanknopingspunten om soevereiniteitseisen te stellen. De Data Act bevat bepalingen over overstapbaarheid van clouddiensten. Maar DORA geldt alleen voor financieel, NIS2 is primair een cybersecuritywet, en de Data Act-bepalingen over cloudswitching missen tanden zolang er geen concurrerende Europese alternatieven zijn.

Wat er nog moet gebeuren

Het kernprobleem is helder: Europa heeft wél het besef dat digitale afhankelijkheid een strategisch risico is, maar nog niet het instrumentarium om dat risico structureel te adresseren voor de volle breedte van de economie.

Soevereiniteitseisen horizontaal, niet sectoraal

DORA doet het voor financieel. De CADA straks voor publieke aanbestedingen. NIS2, met goede wil, voor de kritieke sector. Maar waarom zou een ziekenhuis dat buiten NIS2 valt, een school, of een logistiek bedrijf niet dezelfde exit-strategie-eis verdienen? Het risico van een Amerikaans sanctiebevel dat een clouddienst stilzet, discrimineert niet naar sector. De eis om dat risico te beheersen zou dat ook niet moeten doen.

Interoperabiliteitsplichten die overstappen reëel maken

Je kunt pas verwachten dat organisaties bewegen als er iets is om naartoe te bewegen. Dat vereist Europese cloudstandaarden die lock-in doorbreken, zodat migreren van Azure naar een Europees alternatief niet een tweejarig project is maar een operationele keuze. De Data Act zet hier een eerste stap met switchingrechten, maar die blijven tandeloos zonder volwassen alternatieven en zonder afdwingbare standaarden.

Investering als industriebeleid

Europa heeft geen concurrerend cloud-ecosysteem, niet omdat Europese ingenieurs minder capabel zijn, maar omdat er nooit serieus in is geïnvesteerd. De hyperscalers hebben twee decennia en honderden miljarden voorsprong. Die kloof dicht je niet met regelgeving alleen. Dat vereist industriebeleid van het kaliber Airbus.

Handhaving richting de juiste partij

En hier wordt het oncomfortabel. Als we het echt menen met soevereiniteit, moeten we niet de tandarts aanpakken maar Microsoft, Apple en Google. Waarom gaat er telemetrie van Europese overheidsapparatuur naar servers in de VS? Waarom hebben servicemedewerkers vanuit India toegang tot Europese mailboxen? Dat zijn de vragen die gesteld moeten worden, niet aan mijn tandarts, maar aan de partijen die deze diensten leveren en aan de toezichthouders die erop moeten toezien.

Maar ook dát is ingewikkelder dan het klinkt. Boetes kunnen de hyperscalers dragen, het zijn afrondingsfouten op hun kwartaalcijfers. En verboden raken vooral de gebruiker: als Apple drie maanden niet mag opereren in Europa, ligt de creatieve sector drie maanden plat. Handhaving tegen Big Tech vereist instrumenten die pijn doen bij het bedrijf zonder de afnemer te verlammen. Dat is geen onmogelijke opgave, maar het is ook geen eenvoudige.

De eerlijke boodschap: soevereiniteit kost geld

Dit is het punt dat in het publieke debat consequent wordt vermeden. Digitale soevereiniteit is geen gratis bijproduct van goede regelgeving. Het is een investering in strategische autonomie, vergelijkbaar met defensie

of waterbeheer.

Nederland geeft jaarlijks miljarden uit aan waterkeringen. Niet omdat de zee morgen binnenkomt, maar omdat de kosten van niet-handelen exponentieel hoger zijn dan de kosten van preventie. Diezelfde calculus geldt voor digitale infrastructuur. Het verschil is dat de zee zichtbaar is en de digitale afhankelijkheid niet, tot het moment dat een Amerikaans sanctiebevel 650 overheidswebsites op zwart zet.

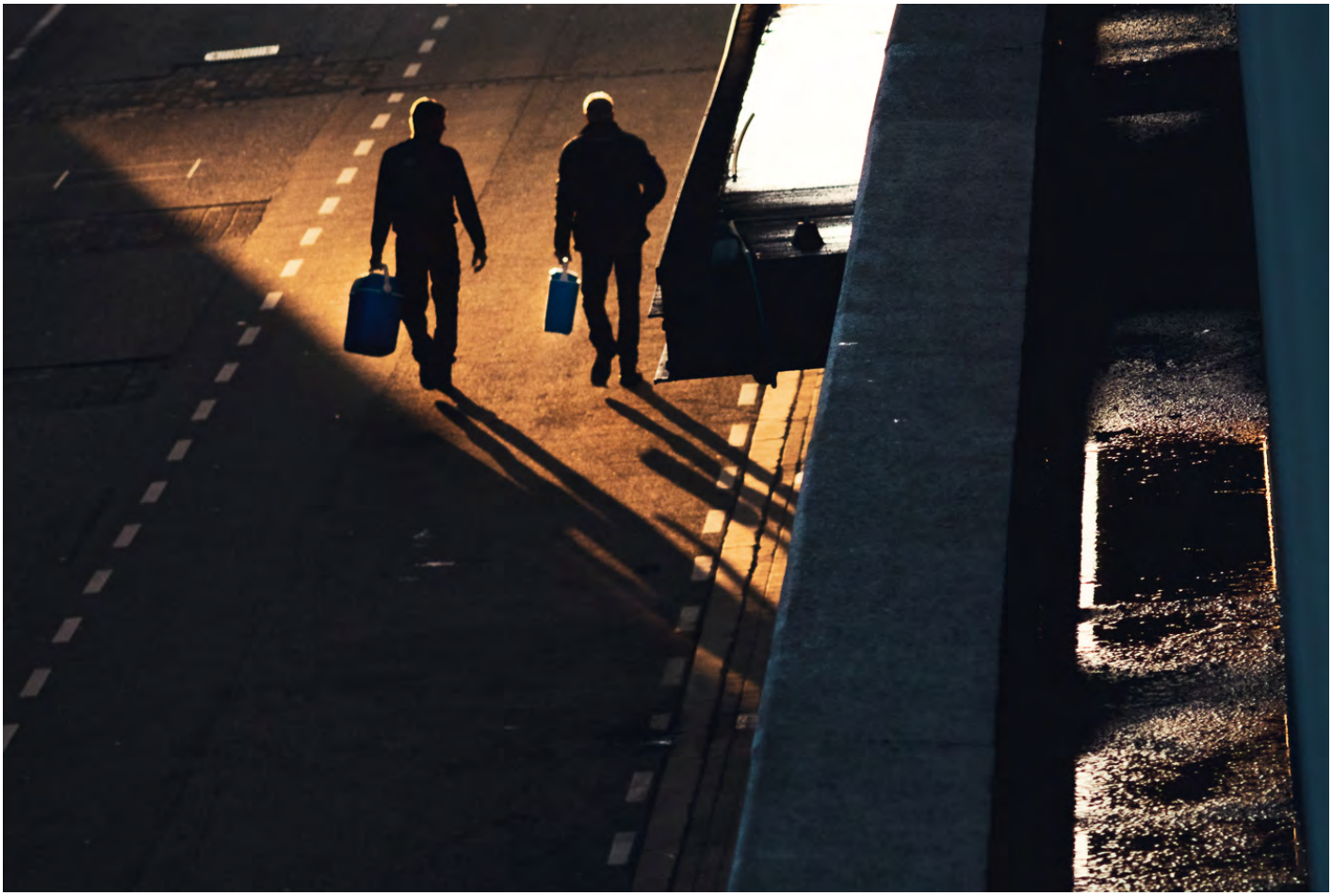
De tandarts met rust laten

Mijn tandarts boort gaatjes, plaatst kronen, en doet dat uitstekend. Ze is niet opgeleid om geopolitieke risico's van cloudinfrastructuur te beoordelen, en ze heeft geen alternatief dat dezelfde functionaliteit biedt als haar huidige praktijksoftware. Als we van haar verwachten dat ze eigenhandig Europese digitale soevereiniteit realiseert door over te stappen op een e-mailprovider waar haar patiënten, haar beroepsvereniging en haar leveranciers niet op zitten, dan verwachten we iets onredelijks.

Het probleem is niet dat individuele organisaties verkeerde keuzes maken. Het probleem is dat Europa geen kader heeft gebouwd waarin de juiste keuze ook de makkelijke keuze is.

De CADA is een eerste stap. Er moeten er meer komen. Voor de private sector, voor het MKB, voor iedereen die niet groot genoeg is om dit zelf op te lossen. Het doel is niet een digitaal IJzeren Gordijn. Zulke Europese marktafscherming zou innovatie schaden en kosten verhogen. Het doel is een marktstructuur waarin Europese alternatieven levensvatbaar zijn, overstappen reëel is, en strategische afhankelijkheden beheerst in plaats van genegeerd worden.

Stop met het uitpakken van tandartsen. Stop met incidentgedreven verontwaardiging bij elke volgende overname. Begin met het bouwen van een digitale dijk.



8. Conclusie

In 2025 constateerden we in de Monitor Digital Decade 2030 dat 22% van de organisaties een concrete strategie had voor de digitale transformatie. Cybersecurity was de hoogste prioriteit. Gebrek aan mensen en expertise het grootste knelpunt. Het beeld was breed maar onscherp: organisaties wisten dát er iets op hen afkwam, maar niet precies wát.

Een jaar later is dat beeld scherper. En minder geruststellend.

De Barometer 2026 laat zien dat de wetgevingsexposure van organisaties groter is dan de meeste denken. Niet omdat er meer wetten zijn dan verwacht, maar omdat de wetten breder raken dan het publieke debat doet vermoeden. AI wordt niet alleen in de techsector ingezet maar in de zorg, de financiële sector, het onderwijs, het openbaar bestuur en de transportsector. Vaak in contexten die als high-risk kwalificeren. Connected products zijn niet het domein van een handvol IoT-startups maar van 85% van de productiesector. En DORA is geen financiële-sectorwet maar een keten die via contractuele eisen doortrekt tot in de serverruimte van elke hoster die aan een bank levert.

Tegelijk laat de Barometer zien dat de digitale basis bij veel organisaties niet op het niveau is dat die wetgeving veronderstelt. In de publieke dienstverlening zit 41% op het laagste niveau. In de productiesector 42%. In de advocatuur 46%. De wetten vragen om verwerkingsregisters, om gestructureerde data-uitwisseling, om security-by-design, om AI-governance, en die vragen veronderstellen een digitale organisatie. Bij een substantieel deel van de respondenten is die er niet.

De kloof tussen wetgevingsdruk en digitale gereedheid is het kernverhaal van dit rapport. Het is geen abstract probleem. Het vertaalt zich in concrete risico's: organisaties die producten op de markt brengen zonder te weten of ze aan de CRA voldoen, zorginstellingen die AI inzetten voor diagnose zonder conformiteitsbeoordeling, ICT-leveranciers die aan banken leveren zonder zich bewust te zijn van DORA's keteneisen.

Drie lessen uit dit onderzoek verdienen het om mee te nemen.

De eerste les is: begin met de inventarisatie
Niet met compliance, niet met implementatie, met overzicht. Welke AI-toepassingen draaien er in je organisatie? Welke producten bevatten software? Aan welke gereguleerde sectoren lever je? De antwoorden op die vragen bepalen welke wetten je raken, en in welke volgorde je ze moet adresseren. De Digital Decade Roadmap is gebouwd om die eerste stap te ondersteunen.

De tweede les is: ken je keten
De Digital Decade-wetgeving werkt niet in sectorale silo's. DORA trekt door naar ICT-leveranciers. NIS2 naar de supply chain. De CADA straks naar cloudleveranciers van de overheid. Als je niet weet wie je klanten zijn en onder welk regime zij vallen, kun je verrast worden door eisen waarvan je niet wist dat ze op jou van toepassing zijn. Daarnaast kunnen Amerikaanse acties ook jouw infrastructuur raken, zoals wanneer een AI-model ineens staatsgeheim wordt verklaard.

De derde les is: de basis gaat voor
Veel organisaties die dit rapport lezen, zullen geneigd zijn om te beginnen bij de nieuwste en meest besproken wet: de AI Act, de CRA, de CADA. Maar als je verwerkingsregister niet op orde is, je systemen niet gekoppeld zijn en je geen zicht hebt op je datastromen, is elke specifieke compliance-exercitie dweilen met de kraan open. De eerste stap is vaak de minst spectaculaire: je digitale huishouding op orde brengen.

Vooruitblik: Barometer 2027

Dit rapport is een eerste editie. De Digital Decade loopt tot 2030, en het wetgevingslandschap verandert elk kwartaal. We willen de Barometer jaarlijks herhalen, met zicht op de voortgang die organisaties boeken.

Wat nu? Vier wegen verder

Dit rapport geeft het overzicht. Een paar manieren waarop wij je verder kunnen helpen:

Wil je weten waar jouw organisatie staat?

Vul de Digital Decade Roadmap in. In een kwartier krijg je een persoonlijk profiel met de wetgeving die op jou van toepassing is, je volwassenheidsscore en concrete eerste stappen.

→ Vraag jouw Roadmap aan

Wil je je Roadmap vertalen naar actie?

Tijdens onze Praktijkdag Digital Decade werk je in één dag met je eigen Roadmap aan een concreet 100-dagen actieplan, samen met onze juristen.

→ Bekijk de Praktijkdag

Wil je doorlopend op de hoogte blijven?

De Digital Decade-wetgeving verandert elk kwartaal. Met ons PE-portaal heb je het hele jaar door toegang tot webinars en kennismodules, inclusief het webinar van Arnoud Engelfriet dat we tijdelijk gratis aanbieden.

→ Bekijk het PE-portaal

Wil je sparren over jouw situatie?

Onze juristen denken graag mee. Plan een vrijblijvend gesprek met een van onze experts.

→ Plan een gesprek

Barometer 2027: wat we volgen

In de volgende editie kijken we niet alleen naar de stand van zaken, maar ook naar de voortgang. Welke sectoren hebben de basis op orde gebracht? Welke wetten zijn gehandhaafd? En, in het verlengde van Arnoud Engelfriets essay: heeft Europa stappen gezet om de soevereiniteitsparadox te doorbreken? Wil je bijdragen aan de volgende editie? De Roadmap blijft open.

De digitale transformatie kan niet zonder recht. Maar recht kan ook niet zonder een organisatie die er klaar voor is. Dit rapport laat zien waar de kloof zit. De volgende stap is aan jou.

Chief Knowledge Officer
Arnoud Engelfriet
- a.engelfriet@ictrecht.nl

Business Development Manager
Guido Grevink
- g.grevink@ictrecht.nl

Legal Counsel (Tech)
Saskia Brouwer
- s.brouwer@ictrecht.nl