

DE PERFECT STORM

Nederlandse & Europese Compliance 2024–2027

Hoe meer dan twintig wetten tegelijkertijd uw organisatie raken, en waarom afwachten geen optie meer is

€20M

max. AVG-boete

8 wetten

tegelijk van kracht

72 uur

om incidenten te melden

Opgesteld door: HES Consultancy International | Datum: April 2026 | hes-consultancy.nl/perfectstorm

Mike Hes

Oprichter — HES Consultancy International

Arnhem, april 2026

mbhes@hes-consultancy-international.com

Van de auteur — Mike Hes

In meer dan 30 jaar in de Europese ICT-sector heb ik veel zien komen en gaan. De verschuiving van mainframe naar client-server. Van on-premise naar cloud. Van perimeter security naar zero trust, ook al heette het twintig jaar geleden anders. Centralisatie maakte plaats voor decentralisatie, totdat de beweging zich weer omkeerde. Secure by Design is terug, als antwoord op de kwetsbaarheden die ontstonden in een tijdperk van 'first ship, then fix'. De IT-wereld heeft een eigen cyclus. Wie lang genoeg meedraait, herkent het bekende in het nieuwe.

Maar soms, echt zelden, komen meerdere krachten tegelijk samen op een schaal die fundamenteel anders is dan gewone verandering. Dat is nu het geval.

"Het is goud wat blinkt — maar wie goed kijkt, ziet dat 80 procent lood bevat. Technologie die werkelijk waarde levert, begint niet bij het product. Het begint bij het probleem van de klant."

Iets wat ik in mijn loopbaan steeds weer tegenkwam: technologiebedrijven die goed presteren in één sector, nemen diezelfde aanpak mee naar een volgende markt. Zonder zich echt te verdiepen in hoe die sector werkt, hoe beslissingen worden genomen of hoe inkoop verloopt. Grote softwarespelers die vanuit de financiële sector de zorg willen bedienen. ERP-platformen die niet hun systeem aanpassen aan de klant, maar de klant vragen zijn processen aan te passen aan het systeem. Ik heb dit van dichtbij meegemaakt bij de verkoop van elektronische patiëntendossiers, in trajecten met tientallen stakeholders die allemaal begrijpelijke, maar onderling tegenstrijdige wensen hadden.

De compliance-golf die dit whitepaper beschrijft, dwingt organisaties een heilzame omgekeerde volgorde te hanteren: processen en risicobeheersing vóór platformkeuze, governance vóór features. Dat is, ondanks de last die nieuwe regelgeving meebrengt, ook een structurele kans voor organisaties die die volgorde al hanteren.

Waarom doet de EU dit eigenlijk? Die vraag krijg ik regelmatig van bestuurders. Deels om EU-burgers te beschermen: de privacyrechten van de AVG, de digitale veiligheid van NIS2, de eerlijkheid van algoritmen onder de AI Act. Maar er zit meer achter. Wetenschappers noemen dit het Brussels Effect: Europese regelgeving wordt wereldstandaard, simpelweg omdat iedere partij die op de EU-markt wil opereren eraan moet voldoen. De AVG is nu het privacyreferentiekader op zes continenten. De AI Act zal dat worden voor kunstmatige intelligentie. In een wereld die gedomineerd wordt door Amerikaanse softwareplatformen en Chinese hardwareproductie, gebruikt de EU regelgeving ook als geopolitiek instrument. Dat gaat verder dan burgerbescherming. Het is ook een bewuste strategische keuze.

Dit whitepaper beschrijft vier krachten die nu gelijktijdig spelen. Ten eerste een golf van nieuwe wetgeving: meer dan twintig actieve kaders, elk met eigen deadlines, boetes en toezichthouders. Ten tweede geopolitieke instabiliteit: twee lopende gewapende conflicten, een wankel Atlantische alliantie en een technologische ontkoppeling tussen het Westen en China. Ten derde een nijpend tekort aan IT- en cybersecurityspecialisten: alleen in Nederland staan 18.700 ICT-vacatures open (CBS, Q4 2024), terwijl Europa structureel 500.000 cybersecurityprofessionals tekortkomt (ENISA). Ten vierde economische onzekerheid: een eurozone in laagconjunctuur, met oplopende financieringskosten, terwijl compliance-investeringen niet uitgesteld kunnen worden.

Dit document geeft geen stappenplan en beveelt geen leveranciers aan. Het biedt een overzicht van wat er speelt, onderbouwd met 45 geverifieerde bronnen uit het EU Official Journal, CBS, ENISA, KPMG en IBM. Het doel is dat bestuurders, CISOs, CIOs en compliance-verantwoordelijken beter geïnformeerd de gesprekken voeren die ze toch al moeten voeren. Feedback is altijd welkom. Ik weet ook niet alles.

Veel leesplezier. En een beheersbare storm.

01 Executive Summary

Nederlandse en Europese organisaties staan voor een ingrijpende compliance-situatie. In de periode 2024-2027 worden meer dan twintig Europese en nationale wetgevingskaders van kracht, gelijktijdig, met overlappende deadlines en brede sectorale reikwijdte. Dit is geen reguliere update van bestaande regels. Het is een fundamentele verandering van het compliance-landschap.

De wetten die nu van kracht worden, raken elke laag van uw organisatie: uw ICT-infrastructuur (NIS2/Cbw, DORA, CRA), uw data (AVG), uw medewerkers (AI Act geletterdheidsplicht), uw leveranciers (DORA art. 28, NIS2 supply chain), uw bestuurders persoonlijk (aansprakelijkheid onder Cbw en Wwke) en uw operationele continuïteit (CER/Wwke).

Wat al van kracht is — en wat velen niet weten

✓ DORA	17 januari 2025 — financiële sector, GEEN overgangsperiode
✓ AI Act geletterdheidsplicht	2 februari 2025 — geldt voor ALLE organisaties die AI inzetten
✓ NEN 7510:2024	16 december 2024 gepubliceerd — zorgsector in transitie
✓ BIO2	september 2025 — verplicht voor Rijk, provincies, waterschappen
✓ CRA (inwerking)	10 december 2024 — software-aanbieders, deadline sept. 2026

Het gevaar van de Perfect Storm zit niet in de zwaarte van één wet, maar in de combinatie. Een organisatie die te maken krijgt met een cyberincident waarbij ook persoonsgegevens betrokken zijn, moet tegelijkertijd melden bij NCSC (24 uur), AP (72 uur), en mogelijk IGJ of DNB, elk met eigen vereisten, eigen formats en eigen handhavingsbevoegdheden. Tegelijk moet het bestuur aantoonbaar toezicht hebben gehouden, anders riskeren bestuurders persoonlijke aansprakelijkheid.

Dit whitepaper geeft u een geïntegreerd overzicht van alle relevante kaders, de kritieke overlappingen, en de prioriteiten voor uw organisatie.

De Vierde Kracht — Economische Onzekerheid

De compliance-golf treft organisaties in een periode van structurele economische tegenwind:

- Eurozone BBP 2024: +0,9% — de laagste groei in tien jaar buiten crisisjaren (IMF, april 2025)
- EU PMI Maakindustrie: >24 maanden onder de contractiedrempel van 50 (S&P Global PMI 2023–2025)
- ECB rente-effect: financieringskosten zijn pas recentelijk van 4% historisch hoog niveau gedaald, met een vertraagd effect op investeringsbereidheid bij MKB en mid-market
- Nederland: CBS Q4 2024 — BBP-groei 0,2%, nagenoeg stagnatie
- Investeringsparadox: compliance-investeringen zijn verplicht en niet uitstelbaar, terwijl budgetdruk bij precies die bedrijven het hoogst is

Gevolg: de 'perfect storm' treft organisaties niet in een periode van economische kracht, maar in een periode van verhoogde kwetsbaarheid. Wie nu investeert in geïntegreerde compliance bouwt tegelijkertijd operationele weerbaarheid die ook in economisch moeilijkere tijden rendeeft.

02 Sector Urgentie Heatmap — 13 Sectoren

Onderstaande matrix dekt alle sectoren die onder NIS2 (essentiële en belangrijke entiteiten), CER/Wwke (kritieke infrastructuur) en overige EU-regelgeving vallen. Rood = directe actie vereist (wet van kracht of deadline <6 maanden). Oranje = voorbereiding lopend jaar noodzakelijk. Geel = in kaart brengen. Groen = relatief beperkte impact. De laatste vijf sectoren (gemarkeerd) zijn aanvulling op de acht eerder gedefinieerde HCI-kernscenario's.

KRITIEK — Actie NU

HOOG — Dit jaar

MIDDEL — Monitoren

LAAG / N.v.t.

Sector	NIS2 Cbw	DORA	AVG	AI Act	BIO2	NEN 7510	CER Wwke	CRA
Overheid / Gemeente	KRITIEK	LAAG	KRITIEK	HOOG	KRITIEK	LAAG	HOOG	MIDDEL
Ziekenhuis / Zorg	KRITIEK	LAAG	KRITIEK	HOOG	LAAG	KRITIEK	HOOG	MIDDEL
Financieel / Bank	KRITIEK	KRITIEK	KRITIEK	HOOG	LAAG	LAAG	HOOG	MIDDEL
Energie / Nuts	KRITIEK	LAAG	HOOG	MIDDEL	LAAG	LAAG	KRITIEK	MIDDEL
Onderwijs	HOOG	LAAG	KRITIEK	HOOG	HOOG	LAAG	MIDDEL	MIDDEL
Software / SaaS	HOOG	LAAG	HOOG	KRITIEK	LAAG	LAAG	MIDDEL	KRITIEK
Logistiek & SC	HOOG	LAAG	HOOG	MIDDEL	LAAG	LAAG	HOOG	HOOG
Legal / LegalTech	HOOG	MIDDEL	HOOG	KRITIEK	LAAG	LAAG	MIDDEL	MIDDEL
Farma & Life Sciences	KRITIEK	LAAG	KRITIEK	KRITIEK	LAAG	HOOG	HOOG	HOOG
Telecom & ICT-diensten	KRITIEK	MIDDEL	HOOG	HOOG	LAAG	LAAG	HOOG	KRITIEK
Maakindustrie / OEM	HOOG	LAAG	MIDDEL	HOOG	LAAG	LAAG	MIDDEL	KRITIEK
Pensioenfondsen & Verz.	HOOG	KRITIEK	HOOG	HOOG	LAAG	LAAG	MIDDEL	LAAG
Detailhandel (groot)	MIDDEL	LAAG	KRITIEK	HOOG	LAAG	LAAG	LAAG	MIDDEL

NIS2/Cbw: verwachte inwerkingtreding 1 juli 2026. DORA: van kracht per 17 jan 2025. CRA: volledig van kracht 11 dec 2027 (rapportageplicht al sept. 2026). BIO2: verplicht voor overheid sept. 2025.

03 Financiële Impact — Wat staat er op het spel?

Boetes zijn geen theoretisch risico meer. In 2023 legde de EDPB meer dan €2,1 miljard aan GDPR-boetes op in de EU. In Nederland beboette de AP Netflix €4,75 miljoen (2024). DORA introduceert eigen boetekaders boven op de bestaande AVG-structuur. De tabel hieronder geeft de maximale blootstelling per wetgevingskader.

Kader	Max. boete	Grondslag	Toezichthouder NL	Van kracht
AVG / GDPR	€20M of 4% wereldwijde omzet	Ernstige overtredingen	Autoriteit Persoonsgegevens	Mei 2018 ✓
AVG / GDPR	€10M of 2% wereldwijde omzet	Technische/org. verplichtingen	Autoriteit Persoonsgegevens	Mei 2018 ✓
DORA	2% jaaromzet	Niet-naleving financiële sector	DNB + AFM	Jan. 2025 ✓
NIS2 / Cbw	€10M of 2% wereldwijde omzet	Essentiële entiteiten	NCSC / RDI / vakdepartement	Q2 2026
CRA	€15M of 2,5% wereldwijde omzet	Software/hardware-aanbieders	Aangewezen markttoezichthouder	Dec. 2024 ✓
EU AI Act (hoog)	€30M of 6% wereldwijde omzet	Hoog-risico AI-systemen	Nog aan te wijzen NL	Aug. 2026
EU AI Act (overig)	€15M of 3% wereldwijde omzet	Overige overtredingen	Nog aan te wijzen NL	Feb. 2025 ✓
CER / Wwke	Bestuurdersaansprakelijkheid	Kritieke entiteiten	NCTV / vakdepartement	Q2 2026

Rekenvoorbeeld: Ziekenhuis met ransomware-incident

Stel: een middelgroot ziekenhuis (250 bedden, jaaromzet €120M) wordt getroffen door ransomware. Patiëntgegevens lekken. NIS2 én AVG zijn van toepassing. De instelling heeft geen ISMS, geen meldproces.

Mogelijke blootstelling:

- AVG art. 32 (onvoldoende beveiliging): tot €10M of 2% omzet → max. €2,4M
- AVG art. 33 (niet tijdig gemeld): tot €10M of 2% omzet → max. €2,4M
- NIS2/Cbw (geen risicobeheer, geen meldplicht nageleefd): tot €10M of 2% omzet → max. €2,4M
- NEN 7510 (IGJ handhaving): bestuurlijke boete + aanwijzing + publieke verklaring
- Herstelkosten, reputatieschade, aanbestedingsuitsluiting: €0,5M – €5M+

Theoretisch cumulatief maximum: >€7M + reputatieschade + mogelijke IGJ-aanwijzing
→ Vergelijk dit met de investeringskosten van een adequaat ISMS: €80K–€250K.

04 De Acht Kernkaders — Kort & Concreet

4.1 NIS2 / Cyberbeveiligingswet (Cbw) — verwacht 1 juli 2026

De NIS2-richtlijn (Richtlijn EU 2022/2555) verplicht essentiële en belangrijke entiteiten tot een breed pakket aan cyberbeveiligingsmaatregelen. Nederland miste de EU-implementatiedeadline van 17 oktober 2024. Het wetsvoorstel Cbw (36.764) is ingediend op 4 juni 2025; parlementaire behandeling loopt.

Kernverplichtingen: risicobeheer, supply chain security, incidentbeheer, MFA, encryptie, trainingsplicht bestuurders. **Meldplicht significant incident:** 24u waarschuwing → 72u vervolgmelding → 1 maand eindverslag bij NCSC.

Drempel 'significant incident': financiële schade >€500.000 of >5% jaaromzet.

Bestuurdersaansprakelijkheid: bestuurders moeten maatregelen goedkeuren én aantoonbaar kennis hebben (trainingsplicht).

4.2 DORA — van kracht 17 januari 2025

DORA (Verordening EU 2022/2554) is rechtstreeks toepasselijk in de financiële sector. Geen implementatiewet nodig, geen overgangperiode. DNB vervangt per 17 januari 2025 de Good Practice Informatiebeveiliging 2023.

Vijf pijlers: ICT-risicobeheer, incidentrapportage, TLPT (penetratietests voor grote instellingen), third-party ICT-register (art. 28, verplicht per 17 januari 2026), informatie-uitwisseling. **Boete:** tot 2% jaaromzet. DORA is lex specialis t.o.v. NIS2 voor de financiële sector.

4.3 AVG / GDPR — van kracht mei 2018, handhaving intensiveert

De AVG blijft de basiswet voor persoonsgegevensverwerking. De AP intensiveert handhaving: 20.000–30.000 klachten per jaar, actief optreden ook bij lichtere overtredingen. Het nieuwe boetebeleid (AP 2023, Staatscourant nr. 34541) laat hoge boetes toe zonder vaste drempels.

In december 2025 bevestigde het kabinet dat de US CLOUD Act van toepassing is op Microsoft 365, Teams en Zivver. Dit is geen reden om morgen over te stappen, dat gelooft niemand. Maar het is wel een aanleiding om te kijken naar iets wat bijna iedere organisatie contractueel heeft maar zelden onderhoudt: het exit-scenario voor kritieke leveranciers. Dat scenario is verplicht, maar in de praktijk staat het ergens in een la en is het nooit getest. De CLOUD Act maakt dit een actueel governance-vraagstuk, geen IT-vraagstuk.

4.4 EU AI Act — gefaseerde inwerkingtreding 2025–2027

Datum	Verplichting
2 feb 2025 ✓	Verbod onaanvaardbaar-risico AI + AI-geletterdheidsplicht (art. 4) — AL VAN KRACHT
2 aug 2025 ✓	Verplichtingen GPAI-modellen (grote taalmodellen zoals GPT-klasse)
2 aug 2026	Volledige verplichtingen hoog-risico AI-systemen (Bijlage III)
2 aug 2027	Gereguleerde producten met ingebouwde AI (incl. medische toepassingen)

Hoog-risico AI omvat o.a.: biometrische identificatie, AI in werving/selectie, kredietbeoordelings-AI, AI in rechtshandhaving, AI in essentiële dienstverlening. Artikel 6(3) biedt ontsnappingsroute voor systemen zonder significant besluitvormingsrisico.

4.5 BIO2 — verplicht voor overheid per 5 maart 2026

De Baseline Informatiebeveiliging Overheid versie 2 (BIO2 v1.3, gepubliceerd 5 maart 2026) vervangt BIO 1.04 voor het Rijk, provincies en waterschappen. Gemeenten passen BIO 1.04zv nog toe maar moeten BIO2 als richtinggevend kader hanteren.

BIO2 vereist een ISMS op basis van ISO 27001, sluit aan op NIS2 (art. 21 Cbw) en reduceert het aantal maatregelen met ~60% ten opzichte van BIO 1.04 door een risicogestuurde aanpak.

4.6 NEN 7510:2024 — zorgsector

De herziene NEN 7510:2024 (gepubliceerd 16 december 2024) introduceert 93 algemene en 8 zorgspecifieke beheersmaatregelen. Verplichte encryptie van patiëntgegevens is nieuw. Gecertificeerde organisaties moeten uiterlijk 20 februari 2027 getransitioneerd zijn.

Wettelijke verankering via Wabvpz en Besluit elektronische gegevensverwerking. IGJ eist aantoonbare voldoening van ziekenhuizen. NEN 7510 vult de NIS2-zorgplicht in maar dekt niet de meldplicht en registratieplicht volledig.

4.7 CER / Wwke — verwacht 1 juli 2026

De Wet Weerbaarheid Kritieke Entiteiten implementeert de CER-richtlijn (EU 2022/2557). Complementair aan NIS2/Cbw: Cbw = digitale weerbaarheid, Wwke = fysieke weerbaarheid. Van toepassing op elf sectoren kritieke infrastructuur. Na aanwijzing als kritieke entiteit: 10 maanden om te voldoen.

4.8 CRA (Cyber Resilience Act) — van kracht 10 december 2024 [AANVULLING]

Nieuw ten opzichte van het draft document

De Cyber Resilience Act (Verordening EU 2024/2847) ontbrak in de originele versie van dit document.

Dit kader is essentieel voor software-aanbieders, SaaS-platforms met embedded componenten en IoT-leveranciers.

Tijdslijn CRA:

- 10 december 2024: Verordening in werking getreden
- 11 september 2026: Rapportageverplichting actief (kwetsbaarheden melden aan ENISA)
- 11 december 2027: Volledige toepassing (conformiteitsbeoordeling, CE-markering vereist)

Boete: €15M of 2,5% van de wereldwijde jaaromzet — hoger dan NIS2.

Pure SaaS en PaaS vallen NIET onder CRA. Embedded software/firmware WEL.

90% van producten kan zichzelf certificeren (self-assessment). 10% vereist notified body.

4.9 Aanvullende Sectoren — Buiten de Kernacht

De volgende vijf sectoren vallen eveneens onder de reikwijdte van de beschreven wetgeving maar werden niet behandeld in de acht eerder gedefinieerde kernscenario's.

Farma & Life Sciences

De farmaceutische en life sciences sector valt als essentiële entiteit onder NIS2 (gezondheidszorg-categorie). Bijzondere aandacht verdient de AI Act: medische AI-toepassingen (diagnose-ondersteuning, geneesmiddelenonderzoek) vallen onder de hoog-risico categorie Bijlage III §5 en zijn per 2 augustus 2027 onderworpen aan de zwaarste conformiteitseisen.

Gelijktijdig valt medische hulpmiddelen-software onder MDR (Medical Device Regulation) én CRA zodra er een netwerkverbinding aanwezig is. Het voldoen aan MDR artikel 17 (cybersecurity-eisen) en CRA zal naar verwachting aanzienlijk overlappen, maar vereist afzonderlijke documentatie en conformiteitsprocedures.

Telecom & ICT-dienstverleners

Telecomaanbieders en aanbieders van digitale infrastructuur, zoals datacenters, CDN's, DNS-diensten en cloudproviders, vallen als essentiële entiteit onder NIS2/Cbw, in sommige gevallen met de hoogste meldplicht-drempels in de sector. De NIS2-richtlijn onderscheidt expliciet 'aanbieders van openbare elektronische communicatienetwerken' (art. 3 lid 1 sub b).

CRA-impact is hoog: elke software, firmware of dienst met digitale componenten die aan klanten wordt geleverd valt potentieel onder de CRA-definitie. Kritieke ICT-derde partijen die systeemdiensten leveren aan financiële instellingen vallen bovendien onder DORA-toezicht via hun financiële klanten.

Maakindustrie / OEM (Originaliteitsproducenten)

De maakindustrie staat voor de zwaarste CRA-impact van alle sectoren. Elk product met een digitale component, van een industriële machine tot een connected sensor, valt na 11 december 2027 onder de CRA. Fabrikanten moeten een Software Bill of Materials (SBOM) bijhouden, kwetsbaarheden melden aan ENISA (per september 2026) en producten voorzien van een CE-markering op basis van CRA-conformiteit.

Tegelijkertijd valt operationele technologie (OT/ICS) in de industrie onder NIS2 als 'belangrijke entiteit'. De combinatie CRA (productcertificering) + NIS2 (operationele beveiliging) vereist een geïntegreerde aanpak die in de praktijk zelden gesynchroniseerd is.

Pensioenfondsen & Verzekeraars

Pensioenfondsen en verzekeraars vallen onder DORA (van kracht 17 januari 2025) via de EIOPA-regulering, naast DNB- en AFM-toezicht. Voor verzekeringsgroepen met meer dan €500M aan activa gelden de strengste TLPT-vereisten (Threat-Led Penetration Testing). Solvency II-vereisten op het gebied van operationeel risicobeheer overlappen significant met DORA's ICT-risicobeheer-pijler.

AI Act-impact: kredietscoring, risicoclassificatie en schade-afhandeling via AI vallen onder Bijlage III §5 (essentiële diensten). Gebruik van AI in levensverzekeringen of gezondheidsproducten raakt bovendien bijzondere categorieën in de AVG.

Detailhandel (groot / e-commerce)

Grote retailers en e-commerce platformen zijn met name blootgesteld via AVG (klantprofiling, loyaltyprogramma's, targeted advertising) en AI Act. Automatische prijsoptimalisatie en productaanbevelingen vallen onder 'beperkt risico' AI (transparantieplicht). Gezichtsherkenning in winkels is per 2 februari 2025 verboden als 'onaanvaardbaar risico' AI tenzij strikte uitzonderingen van toepassing zijn.

Retailers met meer dan 50 fte of €10M omzet die digitale diensten aanbieden (webshop als 'online marktplaats') kunnen als 'belangrijke entiteit' onder NIS2 vallen. De AP heeft detailhandel aangemerkt als prioriteitssector voor handhaving in 2025–2026 vanwege tracking en profilering.

05 Volledig Wetgevingslandschap — Alle Kaders

Waarom doet de EU dit eigenlijk? — De Drie Echte Motivaties

1. BURGERBESCHERMING: de primaire legitimatie

Privacy (AVG), digitale veiligheid (NIS2), eerlijk AI (AI Act), veerkrachtige infrastructuur (CER). De EU reageert op gedocumenteerde schade: >€2,1 miljard GDPR-boetes in 2023 (EDPB) en duizenden datalekken, hacks en AI-discriminatiezaken die de noodzaak bewezen.

2. DIGITALE SOEVEREINITEIT: de geopolitieke drijver
95% van EU-Cloud capaciteit zit bij niet-EU providers (EC 2023). De US CLOUD Act en Chinese Wetgeving op nationale veiligheid raken data van EU-burgers zonder EU-toestemming.
Regelgeving is het instrument om technologische afhankelijkheid te doorbreken.

3. HET 'BRUSSELS EFFECT': de strategische ambitie
EU-regelgeving wordt wereldstandaard. De AVG is inmiddels op 6 continenten het privacy referentiekader. De AI Act wordt dat voor kunstmatige intelligentie.
Door eerder en scherper te reguleren dan de VS of China, exporteert de EU-normen en daarmee marktmacht.

Bron: Anu Bradford, 'The Brussels Effect' (Columbia Law School).

De acht kaders in sectie 04 zijn de directe compliance-verplichtingen voor de meeste Nederlandse organisaties. Onderstaand overzicht brengt het complete EU- en NL-regelgevingslandschap in kaart, inclusief kaders die dit whitepaper aanvullen, kaders in implementatie, en normen die als invulling van wettelijke verplichtingen dienen.

Kernboodschap

De 'Perfect Storm' beslaat meer dan 8 wetten. Wie het volledige landschap overziet, telt 20+ actieve kaders en 6+ in voorbereiding — naast een set ISO-normen die als bewijslast dienen bij toezichthoudercontroles. Niet alle kaders zijn even zwaar, maar ze werken wel allemaal tegelijkertijd.

A — Reeds behandeld in dit whitepaper (kernacht)

Kader	Type	Van kracht	Sectie
NIS2 / Cyberbeveiligingswet (Cbw)	EU richtlijn → NL wet	Q2 2026 (verwacht)	4.1
DORA	EU verordening	17 jan 2025 ✓	4.2
AVG / GDPR	EU verordening	25 mei 2018 ✓	4.3
EU AI Act	EU verordening	Gefaseerd 2025–2030	4.4
BIO2	NL norm (zelfregulering)	Sept 2025 ✓	4.5
NEN 7510:2024	NL norm (wettelijk)	16 dec 2024 ✓	4.6
CER / Wwke	EU richtlijn → NL wet	Q2 2026 (verwacht)	4.7
CRA	EU verordening	10 dec 2024 ✓	4.8

B — Aanvullende EU-verordeningen (rechtstreeks werkend)

Kader	Verordening	Van toepassing	Kern	Impact
Data Act	EU 2023/2854	12 sept 2025 ✓	Toegang tot en gebruik van data van connected devices en diensten. Rechten van gebruikers op hun machinedata. Verplichte datadeling met overheid bij noodgevallen.	Hoog voor IoT, industrie, smart devices, overheid. Raakt supply chains en vendor-lock-in.

Kader	Verordening	Van toepassing	Kern	Impact
Data Governance Act (DGA)	EU 2022/868	24 sept 2023 ✓	Kader voor data-intermediairs, data-altruïsme en Europese dataruimtes (Health Data Space, Agri-Food, etc.). Vergunningplicht voor data-intermediairs.	Middel voor zorg (EHDS-voorbereiding), overheid en datadeling-initiatieven.
Digital Markets Act (DMA)	EU 2022/1925	2 mei 2023 ✓	Verplichtingen voor 'gatekeepers' (Alphabet, Apple, Meta, Microsoft, Amazon, ByteDance). Interoperabiliteit, dataportabiliteit, verbod self-preferencing.	Hoog voor tech-vendors; indirect voor alle organisaties die gatekeeper-diensten afnemen.
Digital Services Act (DSA)	EU 2022/2065	17 feb 2024 ✓	Aansprakelijkheid online platforms voor illegale content, aanbevelingsalgoritmen, advertentietransparantie. Zwaarste eisen voor Very Large Online Platforms (VLOP).	Hoog voor platforms, media, e-commerce. Moderate impact voor overige organisaties.
eIDAS 2.0	EU 2024/1183	20 mei 2024 ✓ (impl. 2026)	Europese digitale identiteitsportemonnee (EU Digital Identity Wallet). Verplichte acceptatie door publieke diensten en bepaalde private sectoren (banken, telecom) uiterlijk 2026.	Hoog voor overheid, financieel, zorg. Technische implementatie vereist voor acceptatie wallet.
MiCA	EU 2023/1114	30 dec 2024 ✓	Regulering crypto-activa (stablecoins, utility tokens, e-money tokens). Vergunningplicht voor aanbieders van cryptodiensten (CASPs). Toezicht AFM/DNB.	Hoog voor FinTech, crypto-platforms. Moderate voor banken met crypto-diensten.
Interoperable Europe Act	EU 2024/903	12 sept 2024 ✓	Verplichte interoperabiliteitsbeoordeling voor overheidssystemen die grensoverschrijdend data uitwisselen. Europese interoperabiliteitsruimte.	Middel voor overheid; lage directe impact voor private sector.
Product Liability Directive (herzien)	EU 2024/2853	Aangenomen 9 nov 2024 (impl. 2026)	Uitbreiding aansprakelijkheid naar software, AI-systemen en digitale diensten. Vermoeden van defect bij niet-compliance met veiligheidsregels. Bewijslastomkering.	Hoog voor software-aanbieders, AI-ontwikkelaars, IoT-fabrikanten. Raakt CRA en AI Act.

C — EU-richtlijnen in nationale implementatie

Kader	Richtlijn	NL- implementatie	Kern
CSRD	2022/2464	Gefaseerd 2024–2028; grote bedrijven FY2024 (rapportage 2025)	Duurzaamheidsrapportage (ESG) voor grote en beursgenoteerde bedrijven. Digitale aspecten: energie-impact ICT, due diligence digitale toeleveringsketen. ESRS E1/S1/G1 standaarden.
PSD3 + PSR	In voorbereiding	Verwacht 2025/2026; van toepassing 2027	Herziening betaalrichtlijn. Sterkere fraude-bescherming, open banking uitbreiding, API-verplichtingen. Vervangt PSD2 voor betaalinstellingen.

Kader	Richtlijn	NL- implementatie	Kern
Omnibus-pakket (CSRD+CSDDD herziening)	COM/2025/87	Herziening gepubliceerd feb 2025; procedure loopt	Vereenvoudiging CSRD en CSDDD voor MKB. Drempels verhoogd. Relevantie: scope compliance verplichtingen wijzigt voor mid-market bedrijven.

D — In voorbereiding / onderhandeling (komende 2–4 jaar)

Kader	Status april 2026	Verwacht	Kern
ePrivacy Regulation	AI >8 jaar in onderhandeling — geblokkeerd in Raad	Onbekend — mogelijk 2027+	Vervangt e-Privacy Richtlijn (cookies, metadata, machine-to-machine). Zwaarder dan AVG op communicatieprivacy.
AI Liability Directive	Commissievoorstel teruggetrokken sept 2024; herziening verwacht	Onzeker — 2027+	Aansprakelijkheid voor schade door AI-systemen. Bewijslastomkering voor hoog-risico AI. Samenhang met herziene PLD.
European Health Data Space (EHDS)	Politiek akkoord dec 2023; formele goedkeuring 2024	Gefaseerde toepassing 2027–2030	Grensoverschrijdende uitwisseling gezondheidsdata. Secundair gebruik van gezondheidsdata voor onderzoek. Zwaar voor zorg, farma, life sciences.
EUCS (EU Cloud Cert. Scheme)	Conceptversie 2023; goedkeuring doorgeschoven	2026–2027 (verwacht)	Vrijwillig certificeringschema voor cloudproviders (ENISA). Drie assurance-niveaus. Relevant voor overheidscontracten.
Cyber Solidarity Act	Aangenomen april 2024	Implementatie 2025–2026	EU cyberveiligheidsnoodmechanisme: gezamenlijke SOC-capaciteit, incidentrespons en wederzijdse bijstand. Versterkt NIS2-samenwerking.

E — Nederlandse Specifieke Kaders (aanvullend)

Kader	Van kracht	Kern	Toezicht
Wet digitale overheid (Wdo)	1 juli 2023	Verplicht gebruik erkende inlogmiddelen (DigiD, eHerkenning) voor publieke diensten. Grondslag voor eIDAS 2.0-implementatie in NL.	RDI / Logius
UAVG (Uitvoeringswet AVG)	25 mei 2018	NL-uitvoeringsbepalingen AVG: uitzonderingen, leeftijdsgrenzen, verwerkingen bijzondere data, DPO-register.	AP
Wiv 2017 / Evaluatiewet 2023	2017 / mei 2023	Bevoegdheden AIVD/MIVD incl. bulk-interceptie. Relevant voor organisaties met nationale veiligheidsaspecten en bij staatsacteur-dreigingen.	CTIVD / TIB
Algoritmeregister Overheid	Verplicht per 2024	Overheidsinstanties moeten impactvolle algoritmen publiceren. Implementatie via Digitale Overheid / BZK.	BZK / ADR
ENSIA (Eenduidige Normatiek Single Information Audit)	Jaarlijks	Gecombineerde zelfevaluatie voor gemeenten: DigiD, Suwinet, BRP, BIG/BIO-status. Vervangt aparte audits.	BZK / Logius
Wet bescherming bedrijfsgeheimen (Wbb)	23 okt 2018	Implementatie EU Trade Secrets Directive. Bescherming knowhow en bedrijfsinformatie. Relevant voor IP-bescherming in cybersecurity-context.	Rechtbank

Kader	Van kracht	Kern	Toezicht
Besluit cloud computing (Rijksdienst)	Intern rijksbeleid	Kader voor cloudgebruik door Rijksoverheid. Soevereiniteitseis voor hoog-vertrouwelijke data. Actueel door CLOUD Act-problematiek.	BZK / CIO Rijk

F — ISO/NEN Normen als Compliance-Instrumenten

ISO-normen zijn geen wettelijke verplichtingen maar fungeren als erkende invulling van wettelijke zorgplichten. Toezichthouders (IGJ, DNB, AP) accepteren ISO-certificering als bewijs van compliance. Onderstaande normen zijn direct relevant voor de wetgeving in dit whitepaper.

Norm	Gepubliceerd	Relatie tot wetgeving	Toelichting
ISO/IEC 27001:2022	2022 (rev.)	NIS2 ✓ BIO2 ✓ DORA ✓ NEN 7510 ✓	Information Security Management System (ISMS). Grondslag voor BIO2, NEN 7510 en erkend als NIS2-zorgplicht-invulling. Meest brede dekking.
ISO/IEC 27002:2022	2022 (rev.)	NIS2 ✓ BIO2 ✓ NEN 7510 ✓	Uitwerking beveiligingsmaatregelen bij 27001. 93 controls in 4 thema's. Basis voor BIO2 v1.3 en NEN 7510:2024 structuur.
ISO/IEC 42001:2023	Dec 2023 — NIEUW	EU AI Act ✓ AVG DPIA ✓	AI Management System Standard — de '27001 voor AI'. Biedt structuur voor AI governance, risicomanagement en verantwoorde AI-inzet. Relevant voor AI Act compliance per aug 2026.
ISO/IEC 27701:2019	2019	AVG ✓ DORA (data) ✓	Privacy Information Management System (PIMS). Uitbreiding op 27001 voor persoonsgegevensverwerking. Erkend door AP als aantoonbare AVG-compliance.
ISO/IEC 62443	Serie 2018–2023	CRA ✓ NIS2 (OT) ✓ CER ✓	Industriële cybersecurity voor OT/ICS-systemen (SCADA, productie-automatisering). Essentieel voor maakindustrie, energie, water. Basis voor CRA-conformiteit embedded systemen.
ISO/IEC 27400:2022	2022	CRA ✓ NIS2 ✓	IoT-specifieke beveiligingsrichtlijnen. Raakt direct de CRA-vereisten voor connected devices. Referentienorm bij CRA self-assessment.
ISO/IEC 23894:2023	2023	EU AI Act ✓	AI Risk Management. Basis voor ISO 42001. Geeft invulling aan AI Act-vereiste voor risicomanagementsysteem (art. 9) bij hoog-risico AI.
ISO/IEC 27017:2015	2015	AVG ✓ DORA (cloud) ✓	Cloudspecifieke beveiligingsmaatregelen (uitbreiding 27001/27002). Relevant voor DORA third-party ICT-risicobeheer bij cloudproviders.
ISO 22301:2019	2019	NIS2 ✓ DORA ✓ CER ✓	Business Continuity Management System (BCMS). Invulling van de continuïteitseisen in NIS2 (art. 21 sub c), DORA en CER/Wwke.
NEN-EN-ISO/IEC 27018:2020	2020	AVG ✓ DORA (cloud) ✓	Bescherming PII in publieke clouddiensten. Erkend als aanvullende bewijs voor AVG-compliant cloudverwerking.

06 Samenloop in de Praktijk — Vier Scenario's

Scenario 1 — Ransomware in een ziekenhuis (NIS2 + AVG + NEN 7510 + WGBO)

Een aanvaller versleutelt het EPD-systeem. Patiëntgegevens zijn tijdelijk niet beschikbaar en er is een vermoeden van dataexfiltratie. Wat moet u doen , en wanneer?

Uur/dag	Verplichting	Grondslag	Richting
0–24 uur	Vroegtijdige waarschuwing sturen	NIS2 art. 23 / Cbw art. 24	NCSC
0–72 uur	Datalek melden als hoog risico	AVG art. 33	Autoriteit Persoonsgegevens
0–72 uur	Betrokkenen informeren (patiënten)	AVG art. 34	Betrokkenen direct
72 uur	Vervolgmelding cyberincident	NIS2 art. 23(4)	NCSC
Zo snel mogelijk	Incident documenteren in NEN 7510-log	NEN 7510:2024 maatregel 5.25	Intern dossier
1 maand	Eindverslag cyberincident	NIS2 art. 23(5)	NCSC

Vier parallelle processen, vier formats, vier deadlines, tegelijkertijd. Organisaties zonder voorbereid incidentresponsproces zullen dit niet tijdig en correct kunnen uitvoeren.

Scenario 2 — AI-gestuurde sollicitatiescreening (AI Act + AVG)

Een HR-afdeling zet een AI-tool in voor het filteren van sollicitanten. Dit valt onder Bijlage III AI Act (werkgelegenheid, art. 6 jo. Annex III §3): hoog-risico AI-systeem.

Verplichtingen per 2 augustus 2026: conformiteitsbeoordeling, risicomanagementsysteem, datakwaliteitseisen, transparantie naar sollicitanten, menselijk toezicht, registratie in EU AI-databank. Bovenop de reeds geldende AVG-verplichtingen (DPIA verplicht, art. 22 profilering).

Actie nu: inventariseer alle AI-tools die betrokken zijn bij besluitvorming over personen. AI-geletterdheidsplicht geldt al per 2 februari 2025. Medewerkers en bestuurders moeten kunnen aantonen dat zij de AI-tools die zij inzetten begrijpen.

Scenario 3 — Bank met cloud-leverancier als kritieke ICT-derde (DORA + AVG)

Een middelgrote bank maakt gebruik van een US-based cloud provider (bijv. Azure/AWS) voor kernbankieren-functionaliteit. DORA art. 28 vereist een uitgebreid ICT-derdepartijregister en contractvereisten per 17 januari 2026.

Gelijktijdig bevestigde het kabinet in december 2025 dat de US CLOUD Act van toepassing is op Microsoft 365 en Teams. Niemand verwacht dat banken morgen massaal migreren, maar de vraag die hier echt gesteld moet worden is anders: wanneer heeft uw organisatie voor het laatst het exit-scenario voor uw cloud-leveranciers geactualiseerd en getest? Dat is de verplichting die er al lag en nu urgent is geworden.

Scenario 4 — Software-aanbieder met IoT-component (CRA + NIS2 + AVG)

Een Nederlandse SaaS-aanbieder biedt een platform aan met een hardware-gateway (IoT-device). De gateway valt onder CRA. Deadlines: rapportageplicht kwetsbaarheden per 11 september 2026, CE-markering per 11 december 2027. Tegelijk kan het platform onder NIS2 vallen als het als 'digitale infrastructuur' kwalificeert.

Pure SaaS zonder embedded componenten valt niet onder CRA. Zodra er een hardwarecomponent, firmware of embedded OS in het product zit, is CRA van toepassing.

07 Bestuurdersaansprakelijkheid — Persoonlijk Risico

Een van de meest onderschatte aspecten van de Perfect Storm is de verschuiving naar persoonlijke aansprakelijkheid van bestuurders. Meerdere kaders leggen nu expliciet verplichtingen bij het bestuur neer, niet alleen bij de CISO of IT-afdeling.

Wat de wetgeving van bestuurders vereist

NIS2 / Cbw:	Bestuurders moeten cyberbeveiligingsmaatregelen goedkeuren, toezicht houden en aantoonbaar voldoende kennis hebben (trainingsplicht). Persoonlijke aansprak.
CER / Wwke:	Bestuurdersaansprakelijkheid bij ernstige niet-naleving. Sancties in wet opgenomen.
AVG:	Organisaties (en feitelijk leidinggevend) kunnen aansprakelijk worden gesteld. Boetes zijn niet aftrekbaar van belasting (NL beleid).
DORA:	Bestuur is eindverantwoordelijk voor ICT-risicobeheer. Jaarlijkse evaluatie vereist. DNB kan bestuurders persoonlijk aanspreken bij systematisch falen.
AI Act:	Organisaties (lees: bestuurders) die verboden AI inzetten riskeren de hoogste boetes. Geen 'wist niet'-verweer na feb. 2025 — geletterdheidsplicht geldt.

Drie concrete acties voor het bestuur — nu

- Laat een formeel besluit nemen in de RvB/MT dat het cyberbeveiligingsbeleid is goedgekeurd — dit is een NIS2-verplichting die al vóór inwerkingtreding van de Cbw best practice is.
- Volg of organiseer een aantoonbare AI-geletterdheidsmodule voor bestuurders en management de AI Act-verplichting geldt al per 2 februari 2025.
- Zorg dat uw CISO of externe compliance-adviseur periodiek aan het bestuur rapporteert over compliance status en leg dit vast in de notulen.

08 Kritieke Deadlines 2024–2027

Datum	Mijlpaal	Kader	Wie
17 jan 2025 ✓	DORA van kracht — geen overgangperiode	DORA	Financiële sector
2 feb 2025 ✓	AI-geletterdheidsplicht + verbod onaanvaardbaar-risico AI	EU AI Act	Alle organisaties
16 dec 2024 ✓	NEN 7510:2024 gepubliceerd	NEN 7510	Zorgsector
17 jan 2026	DORA ICT-derdepartijregister (art. 28) verplicht	DORA	Financiële sector
5 mrt 2026 ✓	BIO2 v1.3 verplicht (Rijk, provincies, waterschappen)	BIO2	Overheid
1 jul 2026	Cyberbeveiligingswet + Wwke verwacht inwerking	NIS2 / CER	Alle sectoren
17 jul 2026	Aanwijzing kritieke entiteiten Wwke (uiterlijk)	CER / Wwke	11 sectoren
2 aug 2026	Volledige AI Act hoog-risico AI-systemen	EU AI Act	Hoog-risico AI-gebruikers
11 sep 2026	CRA rapportageverplichting kwetsbaarheden (ENISA)	CRA	Software/hardware-aanb.
20 feb 2027	NEN 7510:2024 transitie — deadline gecertificeerde org.	NEN 7510	Gecertificeerde zorgorgan.
2 aug 2027	AI Act: gereguleerde producten met AI (incl. medisch)	EU AI Act	Medische toepassingen
11 dec 2027	CRA volledig van toepassing (conformiteitsbeoordeling)	CRA	Software/hardware-aanb.

10 Acht Prioriteiten — Waar te Beginnen

Na dertig jaar in de ICT-sector zie ik steeds dezelfde patronen terugkomen als organisaties met grote veranderingen te maken krijgen. Onderstaand geen checklist van wat u moet doen, maar de fouten die ik het vaakst zie en die het meeste tijd en geld kosten.

Fout 1 — Per wet een aparte projectgroep opzetten

Wie voor NIS2, DORA en AI Act drie losse trajecten opzet, betaalt driemaal voor dezelfde oplossing en raakt drie keer uitgeput.

Een ISMS op basis van ISO 27001 is de gemeenschappelijke basis voor NIS2, DORA, NEN 7510 en BIO2 tegelijk. Integratie is de hefboom, niet de uitzondering.

Fout 2 — Compliance als IT-verantwoordelijkheid behandelen

Bestuurders die dit volledig delegeren aan de IT-afdeling of CISO, lopen persoonlijk risico. NIS2 en DORA leggen verplichtingen expliciet bij het bestuur neer: goedkeuring van beleid, trainingsplicht, jaarlijkse evaluatie.

De vraag 'heeft onze CISO dit geregeld?' is niet langer voldoende.

Fout 3 — Meldprocessen per wet apart inregelen

Bij een ransomware-incident waarbij persoonsgegevens betrokken zijn, lopen vier meldplichten tegelijk: NCSC (24u), AP (72u), en mogelijk IGJ of DNB.

Wie dit per wet apart heeft geregeld, loopt vast op het moment dat het telt. Één gecombineerd incidentresponsproces is de enige werkbare aanpak.

Fout 4 — AI-tools inzetten zonder governance

Veel organisaties zetten AI-tools in voor besluitvorming over mensen zonder te weten dat dit hoog-risico AI is onder de AI Act.

De AI-geletterdheidsplicht geldt al per 2 februari 2025. Bestuurders en medewerkers moeten aantoonbaar begrijpen welke AI-tools ze inzetten en waarom.

Fout 5 — Leveranciers vertrouwen zonder te toetsen

NIS2 en DORA stellen beide eisen aan uw ICT-toeleveringsketen, niet alleen aan uw eigen organisatie. Een datalek of uitval bij een kritieke leverancier is ook uw probleem.

DORA art. 28 verplicht financiële instellingen per januari 2026 tot een ICT-derdepartijregister. Wie dat nog niet heeft, loopt achter.

Maak een register van kritieke ICT-leveranciers en beoordeel hun compliance-positie.

Fout 6 — Exit-scenario op papier laten liggen

Vrijwel elke organisatie heeft contractueel een exit-scenario voor kritieke leveranciers. Vrijwel niemand actualiseert of test het.

De US CLOUD Act heeft dit van een juridische formaliteit tot een actueel governance-vraagstuk gemaakt. Wanneer heeft u voor het laatst uw exit-scenario voor uw cloudleverancier doorgelopen?

Overweeg een Transfer Impact Assessment voor US-gebaseerde cloudservices.

Fout 7 — CRA pas in 2027 op de agenda zetten

De CRA-rapportageverplichting voor kwetsbaarheden bij ENISA geldt al per 11 september 2026. Wie embedded software of IoT-componenten levert en pas in 2027 begint, mist die deadline.

Self-assessment volstaat voor 90% van de producten, maar dat proces kost tijd.

Rapportageverplichting kwetsbaarheden aan ENISA geldt per 11 september 2026.

Wat wel werkt — vroeg registreren bij NCSC

NCSC biedt dreigingsinformatie, indicatoren en kennisdeling aan geregistreerde entiteiten. Vrijwillige registratie is mogelijk vóór inwerkingtreding van de Cbw.

Geen verplichting, wel direct voordeel: u ontvangt informatie over actieve dreigingen die uw sector raken.

10 De Stille Storm — IT Talentschaarste in West-Europa

Er is een dimensie van de Perfect Storm die zelden in compliance-documenten wordt besproken: zelfs als uw organisatie bereid is te investeren en het bestuur de urgentie begrijpt, er zijn simpelweg niet genoeg mensen om alle wetgeving tegelijkertijd te implementeren. De schaarste aan IT- en cybersecurityspecialisten in West-Europa is structureel, en wordt door de nieuwe regelgolf dramatisch verergerd.



10.1 De Nederlandse Situatie — Structureel Overspannen

De Nederlandse IT-arbeidsmarkt bevindt zich in een staat van structurele overspanning. CBS-data over Q4 2024 toont 18.700+ openstaande ICT-vacatures — een stijging van 39% ten opzichte van de pre-pandemieperiode. Cruciaal: dit is geen juniorentekort. Het gaat om een senior specialist-tekort, geconcentreerd in precies de rollen die organisaties nodig hebben voor NIS2, DORA en AI Act compliance.

ICT-categorie	% van vacatures	Geschat aantal	Compliance-relevantie
Software / Development / Engineering	~35%	~6.500	CRA, AI Act
IT Management / Architecture / Consulting	~15%	~2.800	NIS2, DORA
Data / AI / Machine Learning	~10%	~1.900	AI Act, AVG
DevOps / SRE / Infrastructure	~8%	~1.500	NIS2, CRA
Security / Cybersecurity / Compliance	~7%	~1.300	NIS2, DORA, CRA, AI Act
Overige ICT	~23%	~4.700	Divers

Bron: CBS ICT-vacatures 2024–2025, analyse HCI EU Market Entry Guide 2026.

Het is vissen in een lege vijver. Al het senior NL IT-talent is volledig ingezet. Headhunting betekent het wegkappen van elkaars mensen, het lost niets op. TNO onderzoek laat zien dat 34% van NL werknemers werkdruk en werkstress als reden voor verzuim opgeeft; in de IT-sector ligt dit percentage nog hoger door de structureel hoge werkdruk op bestaande teams.

10.2 West-Europa — Een Structureel Gat

Het probleem overstijgt Nederland. De Europese Commissie heeft in de Digital Decade-doelstelling vastgelegd dat de EU 20 miljoen ICT-specialisten nodig heeft tegen 2030. Het huidige tekort op EU-schaal staat op circa 9 miljoen professionals. ENISA schat dat Europa specifiek 500.000 extra cybersecurityprofessionals nodig heeft. De ISC² Cybersecurity Workforce Study 2024 rapporteert een wereldwijd gat van 4,8 miljoen cybersecurityprofessionals.

Land / Regio	Open ICT-vacatures (2024)	Cybersec. tekort (schatting)	Bron
Nederland	18.700+	~1.300+	CBS Q4 2024
Duitsland	149.000+	~12.000+	Bitkom Research 2024
Verenigd Koninkrijk	170.000+	~14.000+	UK Gov. / DCMS 2024
EU totaal	>900.000	~500.000	EC Digital Decade / ENISA 2024
Wereldwijd	>5 miljoen	4,8 miljoen	ISC² Workforce Study 2024

10.3 De Compliance-Talent Paradox — Wat dit Betekent

De kern van het probleem

Organisaties die willen voldoen aan NIS2, DORA en AI Act hebben het volgende nodig:

- NIS2 vereist: CISO of gelijkwaardig, incident response team, security engineers, supply chain security officers, trainers (bestuurders moeten opgeleid worden)
- DORA vereist: ICT-risicomanager, TLPT-specialisten (externe pen-testers, schaarste), third-party auditcapaciteit, informatieuitwisselingsfunctionaris
- AI Act vereist: AI governance officer, AI auditors, bias/fairness testers, model documentatie specialisten, ISO 42001-gecertificeerde assessors
- CRA vereist: Product security engineers, SBOM-specialisten, kwetsbaarheidsbeheerders, ENISA-rapportagecoördinatoren

Al deze rollen zijn schaars. Al deze rollen zijn nodig tegelijkertijd.

Gartner voorspelt dat organisaties die compliance-implementaties plannen voor 2026, in meer dan 50% van de gevallen vertraging zullen oplopen — niet door budget, maar door het ontbreken van gekwalificeerde interne of externe resources. In de NL praktijk leidt dit al tot een premium op cybersecurity-consultants van 40–70% boven normale tarieven voor NIS2-trajecten.

10.4 Vier Strategische Reacties

Strategie 1 — Geïntegreerde aanpak (hoogste ROI)

Eén ISMS-implementatie (ISO 27001) dekt NIS2, DORA, NEN 7510 en BIO2 tegelijk.
 Eén AI-governance framework (ISO 42001) dekt AI Act en AVG-DPIA gelijktijdig.
 Dit halveert de benodigde specialisten-uren en verdubbelt de compliance-output per fte.

Strategie 2 — Managed compliance services

Externe specialisten als managed service: vCISO (virtual CISO), managed SOC, compliance-as-a-service. Voorkomt recruitment-problematiek en biedt directe senioriteit.
 Kosten: €3.000–€8.000/maand afhankelijk van scope — lager dan één inhouse senior CISO (€120K–€160K/jaar).

Strategie 3 — Nearshore / offshore IT teams

Polen, Roemenië, Portugal, Noord-Macedonië: ruime beschikbaarheid van senior IT-talent.
Remote Experts (Bas ter Heurne): nearshore delivery centers <300 fte, op- en afschalen binnen 4 weken.
Compliance-relevantie: NIS2/DORA stellen eisen aan security van remote/nearshore werkplekken.
AVG-check vereist: nearshore locatie in EU = geen extra doorgifte-problematiek.

Strategie 4 — AI-ondersteunde compliance tooling

GRC-platforms (ServiceNow GRC, Vanta, Drata, OneTrust) automatiseren evidence-verzameling en controles — reduceren benodigde mensuren met 30–50% bij gestandaardiseerde frameworks.
Caveat: tooling vervangt expertise niet — gespecialiseerde setup en onderhoud blijft vereist.

11 Geopolitieke Risicocontext — De Storm Achter de Storm

Compliance is niet alleen een juridische verplichting — het is ook een reactie op een veranderend dreigingslandschap. De geopolitieke spanningen van 2022–2026 zijn de directe aanleiding voor een groot deel van de nieuwe Europese wetgeving (NIS2, CRA, CER, Data Act, digitale soevereiniteit). Organisaties die de geopolitieke context begrijpen, begrijpen ook waarom toezichthouders nu daadwerkelijk handhaven.

Waarom geopolitiek uw compliance-risico verhoogt

- 1. Dreigingsniveau stijgt: staatsacteurs (Rusland, Iran, China, Noord-Korea) zijn actiever dan ooit. Een significante NIS2-melding is aannemelijker als u onder actieve nation-state targeting valt.
- 2. Soevereiniteitsagenda versnelt: geopolitieke druk versnelt de EU-regelgeving rondom data en digitale autonomie — wat leidt tot méér verplichtingen, sneller.
- 3. Supply chain risico wordt wetgevingsrisico: een leverancier getroffen door sancties of statelijke acteur = uw NIS2/DORA supply chain verplichting die direct geactiveerd wordt.
- 4. Bestuursaansprakelijkheid raakt internationale context: als uw bestuur geen inzicht heeft in geopolitieke dreigingen die uw sector raken, is dat een governance-tekort onder NIS2 (trainingsplicht).

9.1 Oekraïne — Rusland: Cyber als Wapen

Het gewapend conflict in Oekraïne (februari 2022 – heden) heeft de Europese cyberdreiging structureel veranderd. Russische statelijke acteurs — met name APT28 (Fancy Bear / GRU), Sandworm (GRU Unit 74455) en Cozy Bear (SVR) — zijn actief buiten het directe conflictgebied gericht op Europese energie-, transport- en overheidsinfrastructuur.

Dimensie	Bevinding	Relevantie NL organisaties
Cyberaanvallen	NCSC CSBN 2024: Rusland verantwoordelijk voor het merendeel van bekende statelijke cyberoperaties tegen EU. Sandworm verantwoordelijk voor aanvallen op Oekraïens energie-netwerk (2022/2023).	NIS2-meldplicht: nation-state aanvallen zijn per definitie 'significant incident'. Energiebedrijven, overheid en telecom zijn primaire doelwitten.
Sabotage & hybride	Sabotage Nord Stream pijplijnen (sept 2022), verstoring Viasat satellietnetwerk (feb 2022), aanvallen	CER/Wwke: fysieke sabotage kritieke infrastructuur is nu een wettelijke planningsvereiste. Bedrijven in de 11 CER-

Dimensie	Bevinding	Relevantie NL organisaties
	op Europese spoorinfrastructuur. AIVD: Rusland voert 'hybride operaties' uit op NL bodem.	sectoren moeten sabotage-scenario's opnemen in continuïteitsplannen.
Desinformatie	Russische desinformatiecampagnes (o.a. via Telegram, RT) gericht op EU-publieke opinie, verkiezingen en steun voor Oekraïne. DSA-handhaving tegen RT actief.	DSA: platforms moeten systematische desinformatierisico's beoordelen. Indirect: reputatieschade en vertrouwenscrises als gevolg van desinformatie beïnvloeden operationele continuïteit.
Economische sancties	EU-sanctiepakket 14 (aug 2024) omvat >2.200 entiteiten. Sanctienaleving vereist due diligence op leveranciers, technologiepartners en indirect ook IT-toeleveranciers.	NIS2 supply chain + AVG: sanctie-compliance raakt vendor management processen. Gebruik van Russische software (o.a. Kaspersky — NCSC-advies: vervangen) is officieel afgeraden.

NCSC-advies april 2026

Het Nationaal Cyber Security Centrum (NCSC) handhaaft het dreigingsniveau voor statelijke cyberoperaties op 'hoog' voor de volgende sectoren: energie, water, overheid, telecom, financieel, havens. Specifiek advies: vervang Russische software en diensten (incl. Kaspersky-antivirussoftware) in kritieke processen. Bron: ncsc.nl/actueel — zie ook CSBN 2024.

9.2 Israel / USA — Iran: Energie, Cyber en Bredere Midden-Oosten Instabiliteit

De escalatie tussen Iran enerzijds en Israel en de VS anderzijds (2023–2026) heeft directe gevolgen voor Europese organisaties via drie kanalen: cyberdreigingen van Iraanse statelijke acteurs, energiemarkt-volatiliteit en verstoring van scheepvaartroutes.

Dimensie	Bevinding	Relevantie NL organisaties
Iraanse cyber-operations	APT34 (OilRig / MOIS), MuddyWater, APT33 (Elfin/Refined Kitten) richten zich op energie, financieel en overheid. CISA/NCSC-UK-NCSC NL joint advisory (2024): Iraanse groepen actief in kritieke infrastructuur EU.	NIS2: energie- en financiële entiteiten moeten Iraanse TTPs (Tactics, Techniques, Procedures) opnemen in dreigingsmodellen. Relevantie voor TLPT (DORA) en penetratietests.
Energie & scheepvaart	Aanvallen op tankers Rode Zee (Houthi's, gesteund door Iran) verstoorden ~30% van Suezkanaal-transport nov 2023 – heden. Energieprijsvolatiliteit als gevolg van geopolitieke escalatie.	Logistiek & supply chain: CER/Wwke en NIS2 supply chain-eis. Energiebedrijven: scenario-planning bij leveringsonderbrekingen (CER art. 13).
Regionale escalatie	Directe militaire confrontatie Iran-Israel (april/okt 2024). VS-Iran diplomatiek klimaat fragiel. Risico op verdere Midden-Oosten-escalatie met energiegevolgen voor EU.	Business continuïteit en crisisplannen: BCMS (ISO 22301) en CER continuïteitsplannen moeten energie- en supply chain-scenario's bevatten voor Midden-Oosten-escalatie.

9.3 USA — Europa: Soevereiniteit, NAVO en Digitale Autonomie

De relatie tussen de VS en de EU staat onder structurele spanning. De terugkeer van de Trump-administratie (jan 2025) heeft de geopolitieke onzekerheid vergroot met directe gevolgen voor Europese organisaties op het gebied van digitale soevereiniteit, defensieautonomie en handelspolitiek.

Spanningslijn	Feitelijke ontwikkeling	Directe compliance-relevantie
NAVO-onzekerheid	Trump (jan 2025): twijfels over art. 5-commitment, eis van 5% BNP defensie-uitgaven. Europese NAVO-leden versnellen defensie-investeringen. EU lanceert ReArm Europe / Veiligheidsunie.	Toename van defensie-budgetten → versnelde IT-modernisering → hogere NIS2/CER-urgentie voor defensiegerelateerde sectoren. Supply chain: meer Europese defensie-inkoop = CRA-impact op Europese hardware-industrie.
Groenland / Canada dreigingen	Trump: herhaalde claims op Groenland (jan-mrt 2025), dreiging Canada-annexatie. EU verklaarde collectieve respons bij aanval op EU-bondgenoot.	Soevereiniteitsagenda versnelt: EU Digital Sovereignty Package, Data Act, EUCS en migratie weg van US-cloudleveranciers worden politiek urgent. Overheidscontracten: US cloud-afhankelijkheid nu actief politiek risico.
US CLOUD Act	Kabinet dec 2025: bevestigt dat US CLOUD Act van toepassing is op Microsoft 365, Teams en Zivver. AVG-doorgifte rechtsgrondslagen onder druk. Tweede Kamer moties (mrt 2025): verminder afhankelijkheid US cloud.	Kabinet dec 2025: US CLOUD Act van toepassing op M365 en Teams. Niemand verwacht massale migratie, maar het exit-scenario voor cloud-leveranciers is nu een actueel governance-vraagstuk. Wanneer heeft uw organisatie dat scenario voor het laatst getest?
Handelstarieven	Trump kondigt 25% importtarieven aan op EU-goederen (mrt 2025). EU-vergeldingsmaatregelen in voorbereiding. Technologie-sector: risico op US-export controls uitbreiding naar software.	Supply chain en CRA: Europese hardware- en software-aanbestedingen worden politiek gestuurd richting EU-alternatieven. CRA-certificering voor niet-EU aanbieders wordt zwaarder getoetst.

EU Digitale Soevereiniteit — Direct wetgevingsgevolg

De geopolitieke spanningen met de VS zijn de directe aanleiding voor het EU Digital Sovereignty Package:

- Data Act (sept 2025): recht op dataportabiliteit weg van US-cloudleveranciers
- EUCS: Europees cloudcertificeringschema — voorkeur voor EU-gehoste diensten bij overheidscontracten
- eIDAS 2.0: Europese identiteitsportemonnee als alternatief voor US Big Tech inlog (Google, Apple ID)
- Tweede Kamer-motie: uitfasering AWS/Azure voor nationale domeinen als langetermijndoel

Bron: EC Digital Compass 2030, Rijksoverheid cloudbeleid, Tweede Kamer mrt 2025

9.4 USA — China: Chips, Supply Chain en Cyberespionage

De technologische ontkoppeling tussen de VS en China heeft directe gevolgen voor de Europese en Nederlandse technologie-supply chain, met name op het gebied van halfgeleiders, telecom-infrastructuur en kritieke hardware. Tegelijkertijd voeren Chinese statelijke acteurs gerichte cyberoperaties uit op Europese organisaties.

Dimensie	Bevinding	Relevantie NL organisaties
Halfgeleiders & ASML	VS export controls halfgeleiders (okt 2022, verstrengd 2023/2024) raken NL bedrijven zoals ASML. NL exportvergunning vereist voor DUV-machines naar China. Geopolitieke druk op NL-beleid.	CRA + NIS2: supply chain risico voor organisaties met Chinese hardwarecomponenten. Continuïteitsrisico als Chinese leverancier wegvalt door sancties.
Huawei / ZTE 5G-ban	NL volgt EU-aanbeveling: Huawei en ZTE uitgesloten van 5G-kernnetwerken. KPN en Odido verwijderen Huawei-apparatuur. Kosten €1–2 miljard (schattingen sector).	Telecom-sector: NIS2 supply chain-eis en CER. Organisaties die van telecominfrastructuur afhankelijk zijn: informeer naar uw provider over Huawei-uitfaseringstijdlijn.

Dimensie	Bevinding	Relevantie NL organisaties
Chinese cyberespionage	AIVD Jaarverslag 2024: China meest actieve statelijke actor gericht op NL economische spionage. Volt Typhoon (US CISA advisory): pre-positioning in kritieke infrastructuur EU. APT40 (MSS): gericht op maritiem, overheid, tech.	NIS2/CER: high-tech bedrijven, havens, overheid en waterbeheer zijn primaire targets. NCSC: versterk detectie-capaciteiten (EDR/SIEM) — dit is een NIS2-maatregel (art. 21 sub g).
TikTok / ByteDance	VS TikTok-ban (jan 2025, deels opgeschort). EU DSA-onderzoek TikTok lopend. NL: Rijksoverheid adviseert geen TikTok op zakelijke apparaten.	AVG + DSA: gebruik van TikTok voor communicatie raakt AVG-grondslagen (doorgifte China). Organisaties die social media-beleid voeren: expliciet TikTok-beleid documenteren.

9.5 Rusland — Europa: Hybride Oorlogsvoering en Kritieke Infrastructuur

Rusland voert naast militaire operaties in Oekraïne ook een brede hybride campagne uit gericht op Europese samenlevingen en infrastructuur. De EU en NAVO kwalificeren dit als systematische destabilisering. Voor Nederlandse organisaties — met name in de 11 CER-sectoren — is dit de meest directe dreigingscontext.

Type operatie	Voorbeeld	Implicatie
Sabotage kritieke infra	Nord Stream (sept 2022), Baltische zeetelekabelschade (nov 2024), GPS-verstoring Balticum/Polen.	CER/Wwke: fysieke weerbaarheidseisen zijn direct respons hierop. Continuïteitsplannen moeten sabotage-scenario's bevatten.
Cyberaanvallen overheid	DDoS op NL overheidswebsites (2022-2024 meerdere episoden, Killnet). Datalekken bij EU-instellingen.	NIS2: overheid is essentiële entiteit. Aanvalssimulaties en detectiecapaciteit verplicht.
Desinformatie	Pro-Russische campagnes op Telegram, nep-accounts op X/Facebook gericht op NL politiek.	DSA-compliance voor platforms. Organisaties: mediatraining medewerkers (onderdeel AI-geletterdheidsplicht).
Economische druk	Gasafpersingsstrategie 2022 (Nordgaz). Ondanks afbouw NL-Russische energieafhankelijkheid: indirecte prijsimpact via EU-markt.	CER: energiebedrijven moeten alternatieve leveringsscenario's documenteren. NIS2: OT-beveiliging energiesector.

9.6 Geopolitiek Risicoveld — Samenvattende Impactmatrix

Geopolitieke Factor	Cyberdreiging	Supply Chain	Soevereiniteit	Wetg.-urgentie
Rusland-Oekraïne oorlog	KRITIEK	HOOG	MIDDEL	NIS2, CER
Israel/USA-Iran conflict	HOOG	HOOG	LAAG	NIS2, CER
USA-Europa spanningen	LAAG	MIDDEL	KRITIEK	Data Act, eIDAS 2, AVG
USA-China tech-oorlog	HOOG	KRITIEK	HOOG	CRA, NIS2, DSA
Rusland-Europa hybride	KRITIEK	MIDDEL	MIDDEL	NIS2, CER, DSA

11 Bronnen & Referenties

Alle feiten, boetebedragen en deadlines in dit whitepaper zijn gebaseerd op onderstaande primaire bronnen. De URL's zijn geldig per peildatum april 2026.

A — EU Wetgeving (Official Journal)

Ref.	Document	Publicatie / Link
[1]	Verordening (EU) 2016/679 — AVG/GDPR	OJ L 119, 04.05.2016 eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016R0679
[2]	Richtlijn (EU) 2022/2555 — NIS2	OJ L 333/80, 27.12.2022 eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32022L2555
[3]	Verordening (EU) 2022/2554 — DORA	OJ L 333/1, 27.12.2022 eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32022R2554
[4]	Richtlijn (EU) 2022/2557 — CER	OJ L 333/164, 27.12.2022 eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32022L2557
[5]	Verordening (EU) 2024/1689 — AI Act	OJ L 1689, 12.07.2024 eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L_202401689
[6]	Verordening (EU) 2024/2847 — CRA	OJ L 2847, 23.10.2024 eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L_202402847

B — Nederlandse Wetgeving & Overheid

Ref.	Document	Publicatie / Link
[7]	Kamerstuk 36.764 — Wetsvoorstel Cyberbeveiligingswet	Ingediend 4 juni 2025 tweedekamer.nl/kamerstukken — zoek op 36764
[8]	Kamerstuk 36.765 — Wetsvoorstel Wwke	Ingediend 4 juni 2025 eerstekamer.nl/wetsvoorstel/36765_wet_weerbaarheid_kritieke
[9]	BIO2 v1.3 — Baseline Informatiebeveiliging Overheid	Gepubliceerd 5 maart 2026 bio-overheid.nl/category/producten/bio
[10]	Boetebeleidsregels AP 2023	Staatscourant 2023, nr. 34541 officielebekendmakingen.nl
[11]	Besluit elektronische gegevensverwerking zorgaanbieders	Stb. 2013, 167 — grondslag NEN 7510-verplichting wetten.overheid.nl
[12]	Rijksoverheid — Implementatie NIS2/CER vertraagd	23 okt 2024 rijksoverheid.nl/actueel/nieuws/2024/10/23/implementatie-nis2-en-cer-in-nederland-vertraagd

C — Toezichthouders

Ref.	Organisatie	Document / Link
[13]	DNB	DORA toezicht dnb.nl/voor-de-sector/open-boek-toezicht/wet-regelgeving/dora/
[14]	DNB	DORA toezicht per 17 jan 2025 dnb.nl/nieuws-voor-de-sector/toezicht-2024/dora-het-toezicht-van-dnb-per-17-januari-2025/
[15]	AP	Boetes en sancties autoriteitpersoonsgegevens.nl/boetes-en-andere-sancties
[16]	AP	Jaarverslag 2024 (gepubl. maart 2025) autoriteitpersoonsgegevens.nl

Ref.	Organisatie	Document / Link
[17]	NCTV	FAQ Cyberbeveiligingswet nctv.nl/onderwerpen/c/cyberbeveiligingswet/vragen-en-antwoorden
[18]	NCTV	Wwke — veelgestelde vragen nctv.nl/onderwerpen/w/wet-weerbaarheid-kritieke-entiteiten
[19]	NCSC	Cybersecuritybeeld Nederland (CSBN) 2024 ncsc.nl/actueel/nieuws/2024/juni/24/csbn-2024
[20]	IGJ	Vragen over NEN 7510 igj.nl/vraag-en-antwoord/vragen-over-nen-7510
[21]	NEN	NEN 7510:2024 informatiebeveiliging zorg nen.nl/zorg-welzijn/ict-in-de-zorg/informatiebeveiliging-in-de-zorg
[22]	EDPB	Guidelines 04/2022 — berekening administratieve boetes edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative-fines

D — Europese Commissie & ENISA

Ref.	Organisatie	Document / Link
[23]	EC	AI Act — regulatory framework digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
[24]	EC	CRA — draft guidance maart 2026 digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[25]	EC	DORA Level 2 — technische standaarden (RTS/ITS Set 2) eba.europa.eu/regulation-and-policy/operational-resilience/digital-operational-resilience-act-dora
[26]	ENISA	ENISA Threat Landscape 2024 enisa.europa.eu/publications/enisa-threat-landscape-2024
[27]	ENISA	NIS Investments Report 2023 enisa.europa.eu/publications/nis-investments-2023
[28]	ENISA	CRA — Guidelines for manufacturers enisa.europa.eu (verwacht Q3 2026)

E — Onderzoeksrapporten & Marktdata

Ref.	Bron	Document / Bevinding
[29]	KPMG NL	Cyber Security Report 2024 Nederland — 72% NL-bedrijven verwacht NIS2-impact. kpmg.com/nl/nl/home/insights/2024/01/kpmg-cyber-security-report-2024.html
[30]	KPMG EU	EU Digital Regulation Readiness Survey 2025 — 61% organisaties niet klaar voor NIS2. kpmg.com/eu
[31]	IBM Security	Cost of a Data Breach Report 2024 — Gemiddelde kosten datalek: €4,45M (globaal); €5,97M (financieel). ibm.com/reports/data-breach
[32]	Gartner	Forecast: Information Security Spending — Worldwide \$215B in 2024 (+14,3% YoY). gartner.com/en/newsroom/press-releases/2024-05-13
[33]	Gartner	Hype Cycle for Cybersecurity 2024 — AI-augmented security, digital sovereignty as top trends. gartner.com
[34]	McKinsey	The State of AI 2024 — 65% organisaties zet generatieve AI in, nog geen AI-governance bij 67%. mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai
[35]	CBS NL	ICT-gebruik bedrijven 2024 — 83% NL-bedrijven maakt gebruik van clouddiensten. cbs.nl/nl-nl/publicatie/2024/34/ict-gebruik-bedrijven-2024
[36]	EDPB	GDPR Enforcement Report 2023 — >€2,1 miljard aan boetes opgelegd in EU in 2023. edpb.europa.eu/news/news/2024/edpb-publishes-coordinated-enforcement-framework-statistics_en

Ref.	Bron	Document / Bevinding
[37]	NEN	Transitiedocument NCS 7510:2025 (certificatieschema) — gepubl. 20 feb 2025. nen.nl
[38]	Ponemon/IBM	2024 Global AI Risk Report — 54% AI-implementaties mist governance framework. ibm.com/thought-leadership/institute-business-value

F — Sectorspecifieke Bronnen

Ref.	Bron	Document / Link
[39]	PubliekIT	Digitale Volwassenheid Nederlandse Gemeenten 2022-2025 (118 gemeenten) — gem. score 3,23/5. publiekit.nl
[40]	Logius	DigiD-beveiligingsrichtlijnen — jaarlijks geactualiseerd. logius.nl/domeinen/toegang/digid
[41]	IBD	BIO2 voor gemeenten informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid-versie-2-bio2/
[42]	DNB	Statistisch Bulletin — activa NL pensioenfondsen >€1.500 miljard (Q3 2024). dnb.nl/statistieken
[43]	TÜV NORD	NEN 7510:2024 — wat is er veranderd? tuv.nl/nl/kennisbank/blogs/nieuwen-7510
[44]	EY NL	Strategische blik op de Wet Weerbaarheid Kritieke Entiteiten ey.com/nl_nl/services/risk/een-strategische-blik-op-de-wet-weerbaarheid-kritieke-entiteiten
[45]	OpenSSF	Software Bill of Materials (SBOM) best practices (rel. CRA) openssf.org/blog/2024

12 Over HES Consultancy International

HES Consultancy International (HCI) begeleidt Nederlandse en Europese organisaties van strategie naar eerste klant, en van compliance-verplichting naar werkende implementatie. Met 30+ jaar ervaring in business development, compliance en go-to-market in de EU helpt HCI u de perfect storm te navigeren zonder in silodenken te vervallen.

HCI werkt samen met specialistische partners op het gebied van NIS2-compliant e-mailcommunicatie (MailSPEC/JACE/Pulse), cryptografische databeveiliging (Chunk Works), digitale soevereiniteit (S23K) en fysieke cyberbescherming (Triple Defence). Elke aanbeveling is gebaseerd op geverifieerde wetgeving — nooit op productpromotie.

Gratis Compliance Scan — 15 minuten, gepersonaliseerd rapport

Beantwoord 9 vragen over uw sector, uw rol en uw huidige compliancestatus.

Ontvang binnen 2 minuten een gepersonaliseerd PDF-rapport met:

- Uw specifieke risicosignalen (met wetsartikelen en boetebedragen)
- De voor uw sector relevante deadlines
- Concrete aanbevolen volgende stap

hes-consultancy.nl/scan

Mike Hes neemt binnen 24 uur contact op voor een vrijblijvend gesprek.
Calendly: calendly.com/mbhes1970/30min | +31 (0)6 1475 6834

Bronnen en Verantwoording

Dit whitepaper is gebaseerd op publiek beschikbare bronnen (Rijksoverheid, DNB, AP, NEN, Europese Commissie, Eerste Kamer) en geverifieerde regelgevingsteksten. Peildatum: april 2026. Dit document heeft een informatief karakter en is geen juridisch advies. Raadpleeg voor uw specifieke situatie altijd de meest recente officiële bronnen en juridische adviseurs.

Zie sectie 09 voor volledig bronnenregister met 45 referenties: EU Official Journal, Rijksoverheid, DNB, AP, NCSC, NEN, ENISA, KPMG, IBM, Gartner, McKinsey, CBS en overige primaire bronnen.

DISCLAIMER & COLOFON

Dit whitepaper is uitsluitend bedoeld voor algemene informatiedoeleinden en vormt geen juridisch, financieel, fiscaal of andersoortig professioneel advies. De inhoud is gebaseerd op publiek beschikbare informatie en geverifieerde bronnen per peildatum april 2026. HES Consultancy International aanvaardt geen aansprakelijkheid voor beslissingen die op basis van dit document worden genomen. De wet- en regelgeving beschreven in dit document kan na publicatie wijzigen; raadpleeg altijd actuele officiële bronnen en gekwalificeerde adviseurs voor uw specifieke situatie.

De meningen en analyses in dit document zijn die van de auteur en weerspiegelen niet noodzakelijkerwijs de standpunten van enige toezichthouder, overheidsinstantie of derde partij waarnaar wordt verwezen. Verwijzingen naar specifieke wet- en regelgeving, onderzoeksrapporten of marktdata zijn uitsluitend illustratief bedoeld en vormen geen aanbeveling van specifieke producten, diensten of organisaties.

© 2026 HES Consultancy International, Arnhem. Alle rechten voorbehouden. Gehele of gedeeltelijke reproductie is uitsluitend toegestaan met voorafgaande schriftelijke toestemming van de auteur. Citeren met bronvermelding is toegestaan.

HES Consultancy International | mbhes@hes-consultancy-international.com | +31 (0)6 1475 6834 | hes-consultancy.nl